Legrand PDU

User Guide

Xerus™ Firmware v3.4.11

legrand®

Safety Guidelines

WARNING! Read and understand all sections in this guide before installing or operating this product.

WARNING! Connect this product to an AC power source whose voltage is within the range specified on the product's nameplate. Operating this product outside the nameplate voltage range may result in electric shock, fire, personal injury and death.

WARNING! Connect this product to an AC power source that is current limited by a suitably rated fuse or circuit breaker in accordance with national and local electrical codes. Operating this product without proper current limiting may result in electric shock, fire, personal injury and death.

WARNING! Connect this product to a protective earth ground. Never use a "ground lift adaptor" between the product's plug and the wall receptacle. Failure to connect to a protective earth ground may result in electric shock, fire, personal injury and death.

WARNING! This product contains no user serviceable parts. Do not open, alter or disassemble this product. All servicing must be performed by qualified personnel. Disconnect power before servicing this product. Failure to comply with this warning may result in electric shock, personal injury and death.

WARNING! Use this product in a dry location. Failure to use this product in a dry location may result in electric shock, personal injury and death.

WARNING! Do not rely on this product's receptacle lamps, receptacle relay switches or any other receptacle power on/off indicator to determine whether power is being supplied to a receptacle. Unplug a device connected to this product before performing repair, maintenance or service on the device. Failure to unplug a device before servicing it may result in electric shock, fire, personal injury and death.

WARNING! Only use this product to power information technology equipment that has a UL/IEC 60950-1 or equivalent rating. Attempting to power non-rated devices may result in electric shock, fire, personal injury and death.

WARNING! Do not use a Legrand product containing outlet relays to power large inductive loads such as motors or compressors. Attempting to power a large inductive load may result in damage to the relay.

WARNING! Do not use this product to power critical patient care equipment, fire or smoke alarm systems. Use of this product to power such equipment may result in personal injury and death.

WARNING! If this product is a model that requires assembly of its line cord or plug, all such assembly must be performed by a licensed electrician and the line cord or plugs used must be suitably rated based on the product's nameplate ratings and national and local electrical codes. Assembly by unlicensed electricians or failure to use suitably rated line cords or plugs may result in electric shock, fire, personal injury or death.

WARNING! This product contains a chemical known to the State of California to cause cancer, birth defects, or other reproductive harm.

Safety Instructions

1. Installation of this product should only be performed by a person who has knowledge and experience with electric power.
2. Make sure the line cord is disconnected from power before physically mounting or moving the location of this product.
3. This product is designed to be used within an electronic equipment rack. The metal case of this product is electrically bonded to the line cord ground wire. A threaded grounding point on the case may be used as an additional means of protectively grounding this product and the rack.
4. Examine the branch circuit receptacle that will supply electric power to this product. Make sure the receptacle's power lines, neutral and protective earth ground pins are wired correctly and are the correct voltage and phase. Make sure the branch circuit receptacle is protected by a suitably rated fuse or circuit breaker.
5. If the product is a model that contains receptacles that can be switched on/off, electric power may still be present at a receptacle even when it is switched off.

Tip 1: The outlet (socket) shall be installed near the equipment and shall be easily accessible.

Tip 2: For detailed information on any Legrand PDU's overcurrent protectors' design, refer to that model's product specification on Raritan website's **PDU Product Selector page https://www.raritan.com/product-selector***.*

FreeType Project Copyright Notice

Portions of this software are copyright © 2015 The FreeType Project (www.freetype.org). All rights reserved.

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

Legrand is not responsible for damage to this product resulting from accident, disaster, misuse, abuse, non-Legrand modification of the product, or other events outside of Legrand'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.

CE cULus 1F61 I.T.E. LISTED

Warning

This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

CAUTION:
To reduce the risk of shock — Use indoors only in a dry location. No user serviceable parts inside. Refer servicing to qualified personnel. For use with IT equipment only. Disconnect power before servicing.

Contents

Using the Command Line Interface 269

June 2018

Using SCP Commands   393

Specifications   397

Equipment Setup Worksheet   399

Configuration or Firmware Upgrade with a USB Drive   402

June 2018

Introduction

Legrand PDU is an intelligent power distribution unit (PDU) that allows you to reboot remote servers and other network devices and/or to monitor power in the data center.

The intended use of Legrand PDU is distribution of power to information technology equipment such as computers and communication equipment where such equipment is typically mounted in an equipment rack located in an information technology equipment room.

Legrand offers different types of Legrand PDU models -- some are outlet-switching capable, and some are not. With the outlet-switching function, you can recover systems remotely in the event of system failure and/or system lockup, eliminate the need to perform manual intervention or dispatch field personnel, reduce downtime and mean time to repair, and increase productivity.

In This Chapter

Available Legrand PDU Models

This User Guide mainly introduces two types of Legrand PDU models, both of which are inlet metered PDUs.

▶ **Legrand PDUs comparison in brief:**

Features	Inlet power measurement	Outlet switching	Load shedding
Legrand Metered PDUs	✅		
Legrand Switched PDUs	✅	✅	✅

Model List

Legrand PDU comes in several models that are built to stock and can be obtained almost immediately. Legrand also offers custom models that are built to order and can only be obtained on request.

Download the Legrand PDU Data Sheet from Raritan's website, visit the ***Product Selector page*** (***http://www.findmypdu.com/***) on Raritan's website, or contact your local reseller for a list of available models.

Package Contents

The following sub-topics describe the equipment and other material included in the product package.

Zero U Products

- One Legrand PDU
- 0U bracket pack and buttons for Zero U

1U Products

- One Legrand PDU
- 1U bracket pack and screws

2U Products

- One Legrand PDU
- 2U bracket pack and screws

APIPA and Link-Local Addressing

The Legrand PDU supports Automatic Private Internet Protocol Addressing (APIPA).

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

Exception: Legrand PDU in the Port Forwarding mode does not support APIPA. See **Setting the Cascading Mode** *(on page 150).*

Once the Legrand PDU 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 Legrand PDU, but no IP address is assigned to the Legrand PDU.

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

  Note: Configuration by connecting the Legrand PDU to a computer using a network cable is an application of this scenario. See **Connecting the Legrand PDU to a Computer** *(on page 30).*

- The Legrand PDU 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 Legrand PDU. See *Configuring Network Settings* (on page 140).

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

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

For retrieval of the link-local address, see ***Device Info*** (on page 70).

Before You Begin

Before beginning the installation, perform the following activities:

- Unpack the product and components
- Prepare the installation site
- Check the branch circuit rating
- Fill out the equipment setup worksheet

Unpacking the Product and Components

1. Remove the Legrand PDU and other equipment from the box in which they were shipped. See *Package Contents* (on page 15) for a complete list of the contents of the box.
2. Compare the serial number of the equipment with the number on the packing slip located on the outside of the box and make sure they match.
3. Inspect the equipment carefully. If any of the equipment is damaged or missing, contact Legrand Technical Support Department for assistance.
4. Verify that all circuit breakers on the Legrand PDU are set to ON. If not, turn them ON.

   Or make sure that all fuses are inserted and seated properly. If there are any fuse covers, ensure that they are closed.

   Note: Not all models have overcurrent protectors.

Preparing the Installation Site

1. Make sure the installation area is clean and free of extreme temperatures and humidity.

   Note: If necessary, contact Legrand Technical Support for the maximum operating temperature for your model. See **Maximum Ambient Operating Temperature** *(on page 397).*

2. Allow sufficient space around the Legrand PDU for cabling and outlet connections.
3. Review *Safety Instructions* (on page 4) listed in this User Guide.

Checking the Branch Circuit Rating

The rating of the branch circuit supplying power to the PDU shall be in accordance with national and local electrical codes.

Filling Out the Equipment Setup Worksheet

An Equipment Setup Worksheet is provided in this User Guide. See *Equipment Setup Worksheet* (on page 399). Use this worksheet to record the model, serial number, and use of each IT device connected to the PDU.

As you add and remove devices, keep the worksheet up-to-date.

Rackmount and Locking Outlets

In This Chapter

Circuit Breaker Orientation Limitation

Usually a PDU can be mounted in any orientation. However, when mounting a PDU with circuit breakers, you must obey these rules:

- Circuit breakers CANNOT face down. For example, do not horizontally mount a Zero U PDU with circuit breakers on the ceiling.
- If a rack is subject to shock in environments such as boats or airplanes, the PDU CANNOT be mounted upside down. If installed upside down, shock stress reduces the trip point by 10%.

  Note: If normally the line cord is down, upside down means the line cord is up.

Rack-Mounting the PDU

This chapter describes how to rack mount a Legrand PDU.

Rackmount Safety Guidelines

In Legrand products which require rack mounting, follow these precautions:

- Operation temperature in a closed rack environment may be greater than room temperature. Do not exceed the rated maximum ambient temperature of the Power Distribution Units. See *Specifications* (on page 397) in the User Guide.
- Ensure sufficient airflow through the rack environment.
- Mount equipment in the rack carefully to avoid uneven mechanical loading.
- Connect equipment to the supply circuit carefully to avoid overloading circuits.
- Ground all equipment properly, especially supply connections, to the branch circuit.

0U Button Mount
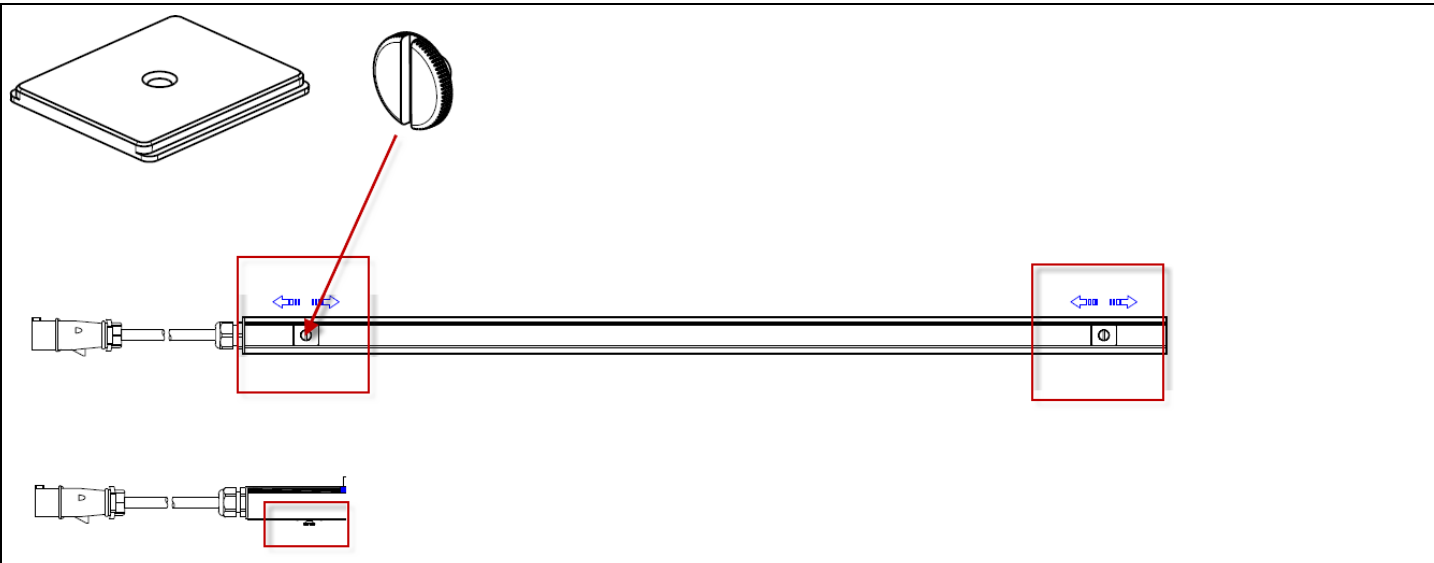
Part Numbers:

- 250-70-0140-00: button (2)
- 250-70-0141-00: bracket (2)

- Slide flat brackets onto rear of 0U model and align over holes at each end.
- Press button into bracket hole and turn with finger.
- Mount by positioning the PDU at the rack, then pressing the buttons through the holes in the cabinet and letting the PDU drop down slightly.

1U/2U Legrand Clip Mount
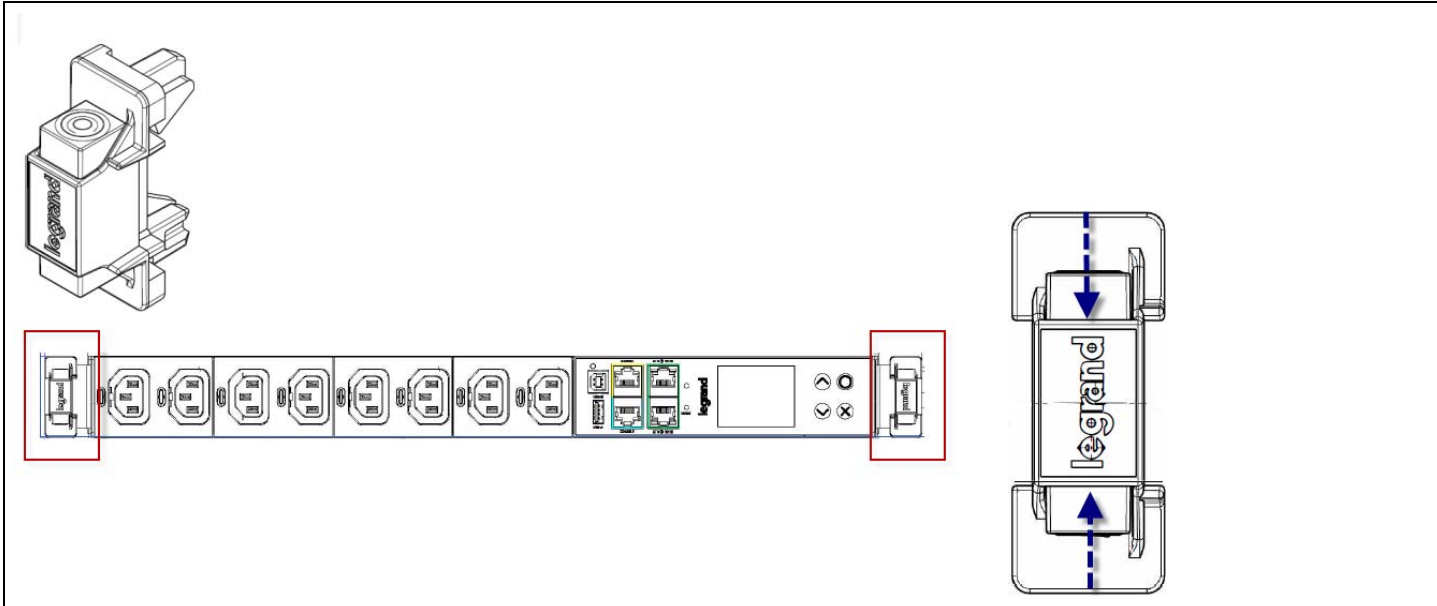
Parts:
- Legrand Soluclip (2)
- Brackets (2): 1U or 2U size

- Attach brackets to ends of 1U model with screws, then attach the Soluclip at each end by squeezing the buttons together to insert the hooks through the bracket. Release the buttons when the hooks are in position securely through the bracket.
- Mount by positioning the PDU at the rack, then tilting the PDU to press the hooks through the holes in the rack. Then set the PDU back to level to engage the hooks.

2U Bracket Mount
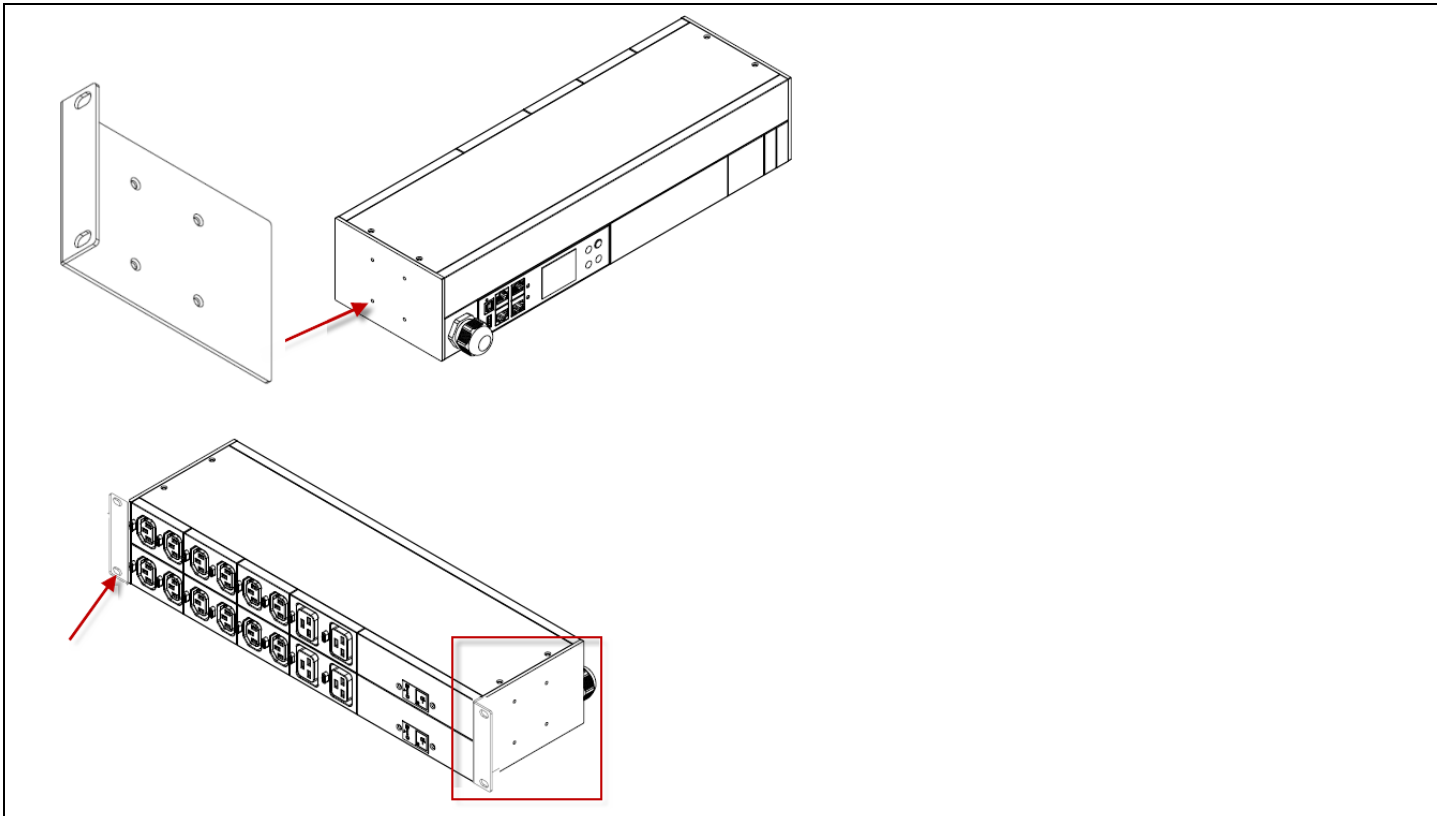
Parts: ▪ Brackets (2) and screws	▪ Attach the brackets with "ears" facing front to each end of the PDU with 4 screws. ▪ Mount by positioning the PDU at the rack, then attaching the bracket "ears" to the rack with 2 screws in holes provided on each ear.

Locking Outlets

Not every Legrand PDU is implemented with locking outlets.

Locking outlets, if available, on the Legrand PDU help secure the connection of power cords from your IT equipment to the PDU.

A locking outlet has a button on it. Such outlets do not require any special power cords to achieve the locking purpose. All you need to do is simply plug a regular power cord into the locking outlet and the outlet automatically locks the cord.

▶ **To remove a power cord from the locking outlet:**

1. Press and hold down the tiny button adjacent to the outlet.
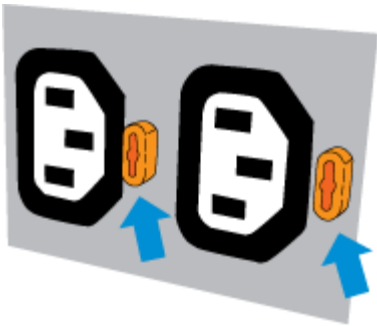
2. Unplug the power cord now.

Initial Installation and Configuration

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

In This Chapter

Connecting the PDU to a Power Source

1. Verify that all circuit breakers on the Legrand PDU are set to ON. If not, turn them ON.

    Or make sure that all fuses are inserted and seated properly. If there are any fuse covers, ensure that they are closed.

    Note: Not all models have overcurrent protectors.

2. Connect each Legrand PDU to an appropriately rated branch circuit. See the label or nameplate affixed to your Legrand PDU for appropriate input ratings or range of ratings.

    Note: When a Legrand PDU powers up, it proceeds with the power-on self test and software loading for a few moments. Note that outlet LEDs are only available on some PDU models.

3. When the software has completed loading, the outlet LEDs show a steady color and the front panel display illuminates.

Connecting the Legrand PDU to Your Network

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

Note: If your Legrand PDU will work as a master device in the bridging mode, you must make a wired connection. See **Cascading Multiple Legrand PDUs for Sharing Ethernet Connectivity** *(on page 32).*

Ethernet port of Legrand PDU must be enabled for the described connection to work properly, which has been enabled per default. See *Wired Network Settings* (on page 141).

▶ **To make a wired connection:**

1. Connect a standard network patch cable to the Ethernet port on the Legrand PDU.
2. Connect the other end of the cable to your LAN.

You can connect either Ethernet port of the Legrand PDU to the LAN -- ETH1 or ETH2.

You can also connect both Ethernet ports to the LAN. See *Dual Ethernet Connection* (on page 25).

Below illustrates the Ethernet ports on Zero U models.
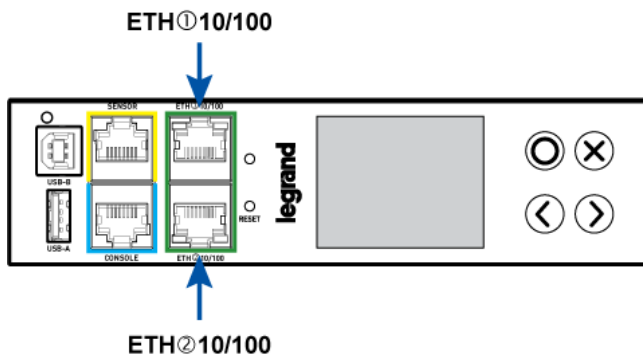
Warning: Accidentally plugging an RS-232 RJ-45 connector into the Ethernet port can cause permanent damage(s) to the Ethernet hardware.

▶ **To make a wireless connection:**

Do one of the following:

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

See *USB Wireless LAN Adapters* (on page 24) for a list of supported wireless LAN adapters.

USB Wireless LAN Adapters

The Legrand PDU 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 Legrand PDU matches the access point. The following is the wireless LAN configuration that the Legrand PDU supports.

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

Important: Supported 802.11 network protocols vary according to the wireless LAN adapter being used with the Legrand PDU. See *USB Wireless LAN Adapters* **(on page 24).**

Dual Ethernet Connection

A Legrand PDU has two Ethernet (LAN) ports. Both ports support up to 100 Mbps.

For more information on the two ports, see ***Connection Port Functions*** (on page 56).

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 Legrand master or slave device to the LAN. See **Cascading Multiple Legrand PDUs for Sharing Ethernet Connectivity** *(on page 32).*

▶ **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 70) and ***Ethernet Interface Settings*** (on page 143).
- Both Ethernet interfaces are configured with proper IPv4 and/or IPv6 settings. See ***Wired Network Settings*** (on page 141).
  - 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 150).

Configuring the Legrand PDU

You can initially configure the Legrand PDU via one of the following:

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

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

1. Connect the Legrand PDU to a DHCP IPv4 network. See ***Connecting the Legrand PDU to Your Network*** (on page 23).
2. Retrieve the DHCP-assigned IPv4 address. Use the front panel LCD display to retrieve it. See ***Device Info*** (on page 70).
3. Launch a web browser to configure the Legrand PDU. See ***Login*** (on page 79).

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

1. Download the PDView app to your mobile device. See ***Connecting a Mobile Device to Legrand PDU*** (on page 26).
2. Connect the mobile device to Legrand PDU via USB.
3. Launch PDView to configure the Legrand PDU.

▶ **Configuration via a connected computer:**

1. Connect the Legrand PDU to a computer. See ***Connecting the Legrand PDU to a Computer*** (on page 30).
2. Use the connected computer to configure the Legrand PDU via the command line or web interface.
   - Command line interface: See ***Initial Network Configuration via CLI*** (on page 486).

> - Web interface: Launch the web browser on the computer, and type the link-local IP address or *pdu.local* to access the Legrand PDU. See **Login** (on page 79).
>
>   For link-local IP address retrieval, see **Device Info** (on page 70).

Tip: To configure a number of Legrand PDUs quickly, see **Bulk Configuration Methods** *(on page 31).*

Connecting a Mobile Device to Legrand PDU

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

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

▶ **Requirements for using PDView:**

- Legrand PDU is running any 3.4.11 or later 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*

    [QR code]

    - *https://play.google.com/store/apps/details?id=com.raritan.android.pdview*

    [QR code]

2. Install PDView.

    [PDView Raritan app icon]

▶ **Step B: Connect the mobile device to Legrand PDU**

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 Legrand PDU.
    - *iOS*: USB-A port.

- *Android*: USB-B port
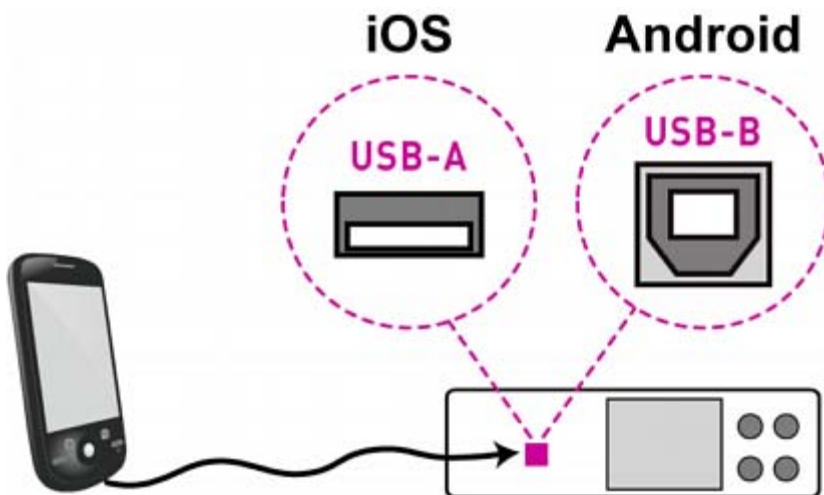
▶ **Step C: Launch PDView to access the Legrand PDU**

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 Legrand PDU yet.

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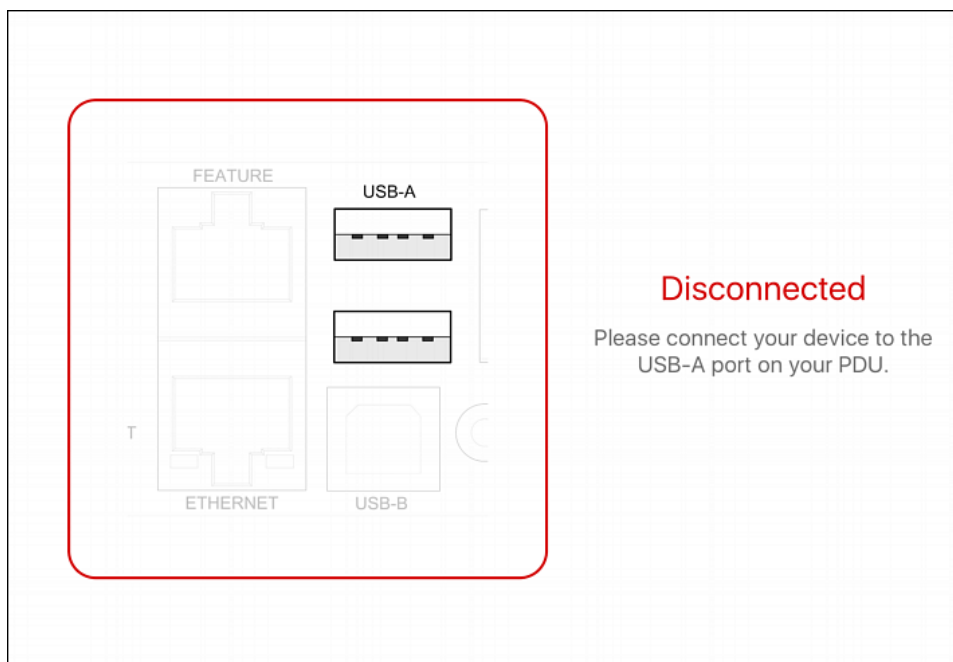
Note: PDView also shows the 'Disconnected' status during the firmware upgrade. If so, wait until the firmware upgrade finishes.

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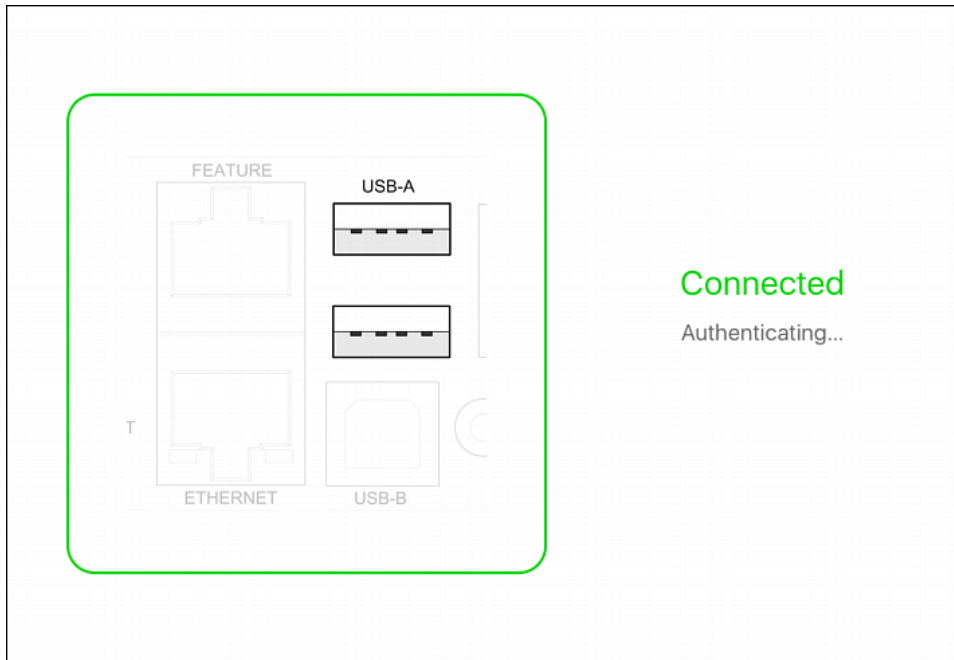
2. If the factory-default user credentials "admin/raritan" remain unchanged, PDView automatically logs in to the web interface of Legrand PDU.

   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 Legrand PDU.

   ▪ 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 Legrand PDU. See **Saving User Credentials for PDView's Automatic Login** *(on page 28).*

Saving User Credentials for PDView's Automatic Login

When PDView detects the Legrand PDU, 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 Legrand PDU 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).
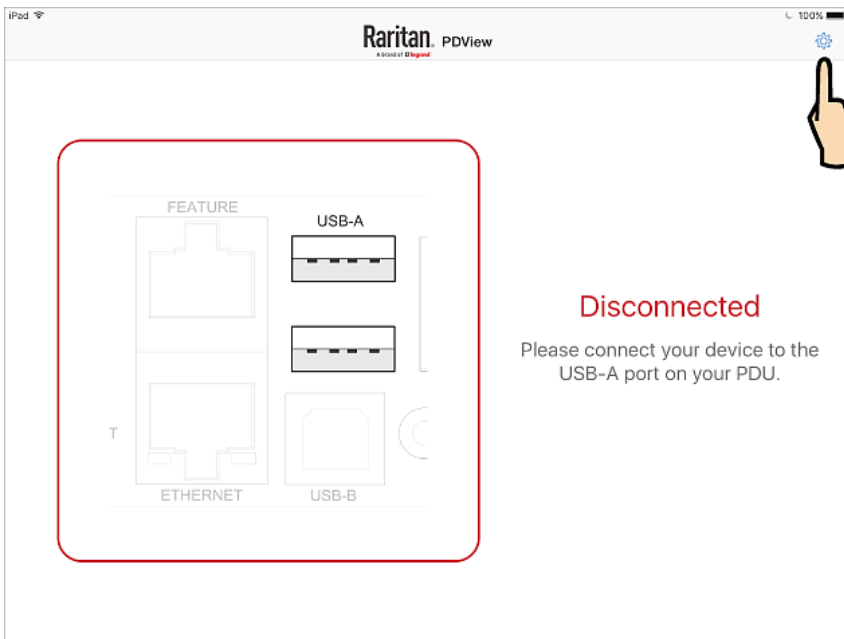
4. The user credentials setup page opens.
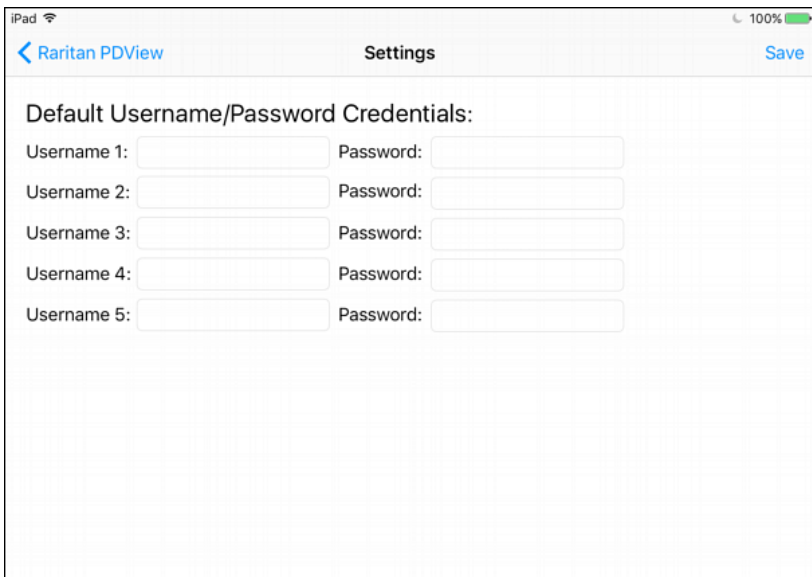
5. Type the desired user credentials, and tap Save.

June 2018

Connecting the Legrand PDU to a Computer

The Legrand PDU 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)

The following diagram illustrates a Zero U model's ports.
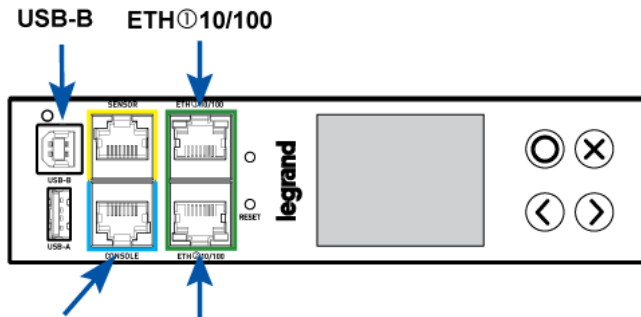
To use the command line interface (CLI) for configuration, establish an RS-232 or USB connection.

To use a web browser for configuration, make a network connection to the computer. The Legrand PDU 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 16).

Establish one of the following connections to a computer. Ethernet port of Legrand PDU 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 the Ethernet port of the Legrand PDU.
   - The Legrand PDU has dual Ethernet ports. You can connect either Ethernet port to the computer.
2. Connect the other end to a computer's Ethernet port.
3. On the connected computer, launch a web browser to access the Legrand PDU, using either link-local addressing: *pdu.local* or *169.254.x.x*. See **Login** (on page 79).

▶ **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 485).
2. Connect a USB cable between a computer's USB-A port and the USB-B port of Legrand PDU.
3. Perform **Initial Network Configuration via CLI** (on page 486).

   Note: Not all serial-to-USB converters work properly with the Legrand PDU so Legrand 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 on the Legrand PDU.
   - See **RJ45-to-DB9 Cable Requirements for Computer Connections** (on page 31).
2. Connect the DB9 end to your computer's RS-232 port (COM).
3. Perform **Initial Network Configuration via CLI** (on page 486).

June 2018

RJ45-to-DB9 Cable Requirements for Computer Connections

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

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)		

Bulk Configuration Methods

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

▶ **A bulk configuration file downloaded from Legrand PDU:**

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

  See **Bulk Configuration** (on page 239).

▶ **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 Legrand PDUs after connecting them to the network.

  See **Bulk Configuration or Firmware Upgrade via DHCP/TFTP** (on page 411).

▶ **A USB flash drive:**

- *Requirement*: A FAT32- or supperfloppy-formatted USB flash drive containing special configuration files is required.
- *Procedure*: Plug this USB drive into the Legrand PDU. 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 402).

Cascading Multiple Legrand PDUs for Sharing Ethernet Connectivity

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

- USB interface
- Ethernet interface

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

Each device in the chain is accessible over the network, with the Bridging or Port-Forwarding cascading mode activated on the master device. See **Setting the Cascading Mode** (on page 150).

- **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 Legrand PDUs in the chain must run compatible firmware versions, which are 3.4.11 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 slave devices 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 482).

▶ **Online Cascading Guide:**

For detailed information on the cascading configuration and restrictions, refer to the *Cascading Guide*, which is available from the Legrand PDU section of Raritan website's **Support page** (**http://www.raritan.com/support/**).

Cascading All Devices via USB

You must set the cascading mode before establishing the chain. See *Setting the Cascading Mode* (on page 150).

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 Legrand PDUs cascaded via USB.
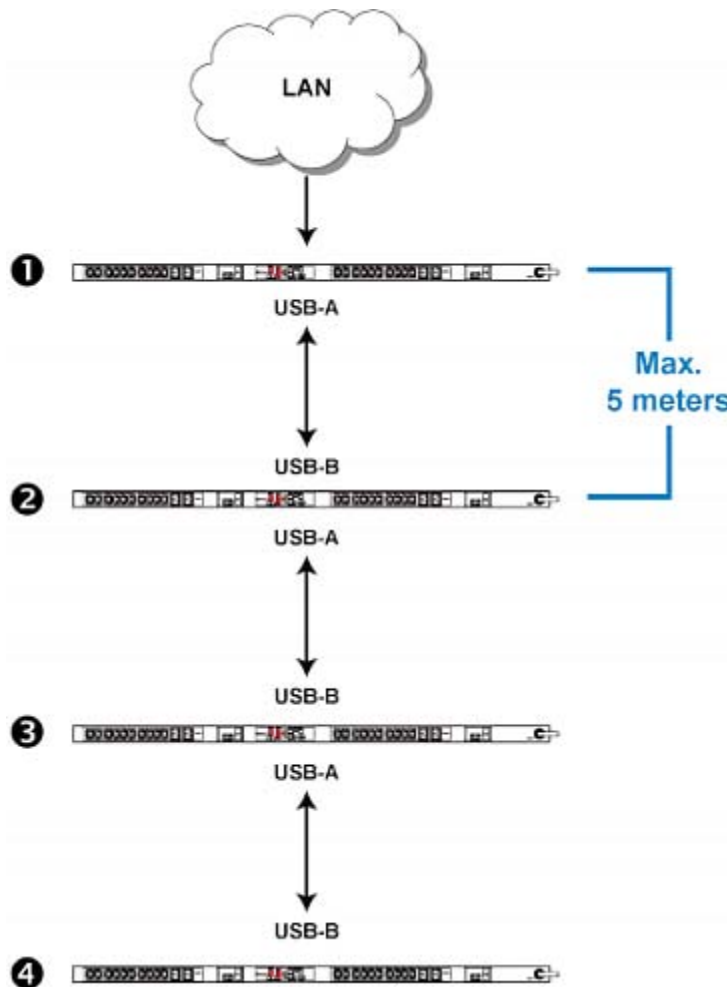
Number	Device role
❶	Master device
❷	Slave 1
❸	Slave 2
❹	Slave 3

▶ **To cascade Legrand PDUs via USB:**

1. Make sure all of Legrand PDUs are running firmware version 3.4.11 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, 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 150).

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 24).

5. Connect the USB-A port of the master device to the USB-B port of an additional Legrand PDU 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 Legrand PDU 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 140).

    - **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:**

- Legrand PDUs can be cascaded with Raritan's PX2-based products. For a list of these Raritan products, see ***Cascading with Raritan PX2-Based Products*** (on page 496).

Extended Cascading with Legrand PDUs

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

You must set the cascading mode before establishing the chain. See *Setting the Cascading Mode* (on page 150).

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 37).

You can mix Ethernet and USB cascading in the Legrand 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

![Legrand logo]
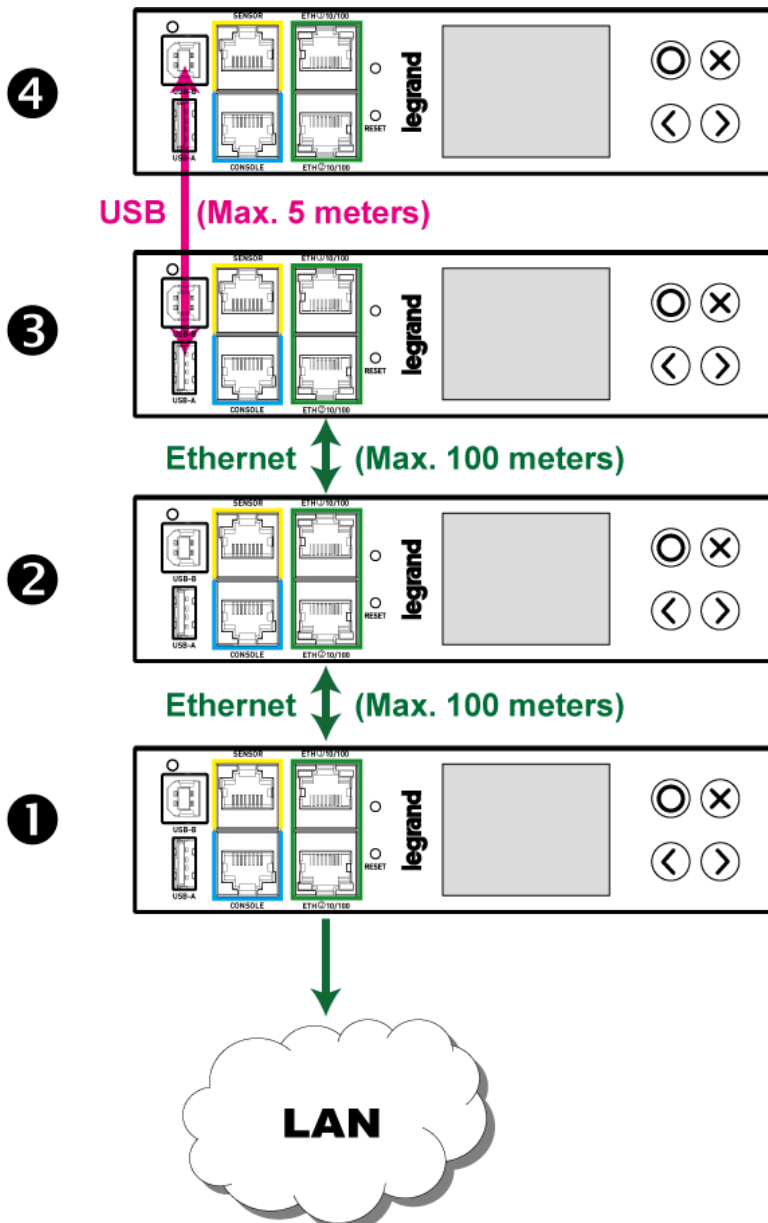
Number	Device role
❷	Slave 1
❸	Slave 2
❹	Slave 3

Ethernet cascading is recommended because of the longer distance, lower latency and more reliable connection it supports.

Note: For instructions on USB cascading, see **Cascading All Devices via USB** *(on page 33).*

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

1. Make sure all of Legrand PDUs are running firmware version 3.4.11 or later.
2. Choose one Legrand 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 150).

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 24).

5. Connect the available Ethernet port of the master device to either Ethernet port of another Legrand via a standard network patch cable. This additional Legrand device is Slave 1.

6. Connect Slave 1's available Ethernet port to either Ethernet port of another Legrand via a standard network patch cable. The second additional device is Slave 2.

7. Repeat the same step to connect more Legrand 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 140).

   ▪ **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.

▶ **Enable R/STP if a cascade loop is preferred:**

- You can "loop" a cascading chain to create network communication redundancy (Bridging mode only), but only when your network supports **R/STP** protocol.

  Make sure that your network has R/STP enabled if using a cascade loop (Bridging mode) *or else network loops may occur.*

▶ **A tip for Extended cascading:**

- Legrand PDUs can be cascaded with Raritan's PX2-based products. For a list of these Raritan products, see *Cascading with Raritan PX2-Based Products* (on page 496).

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.
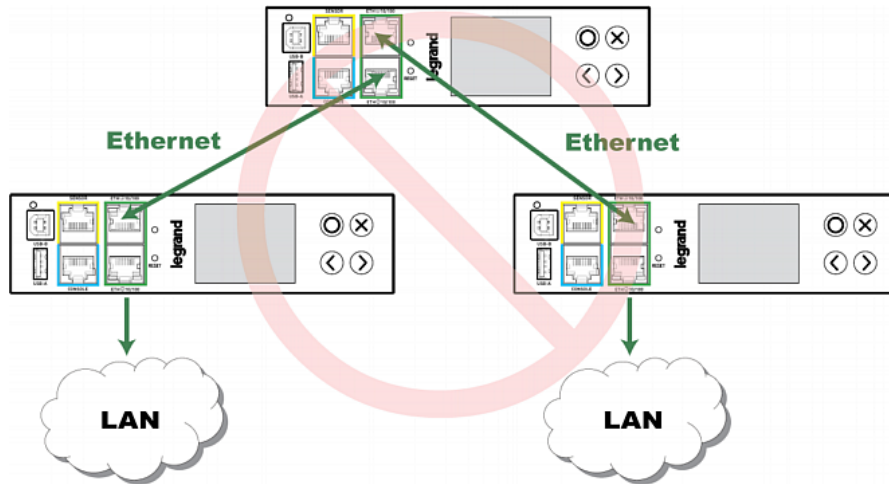
- One cascaded device has two upstream devices via Ethernet and USB cables.
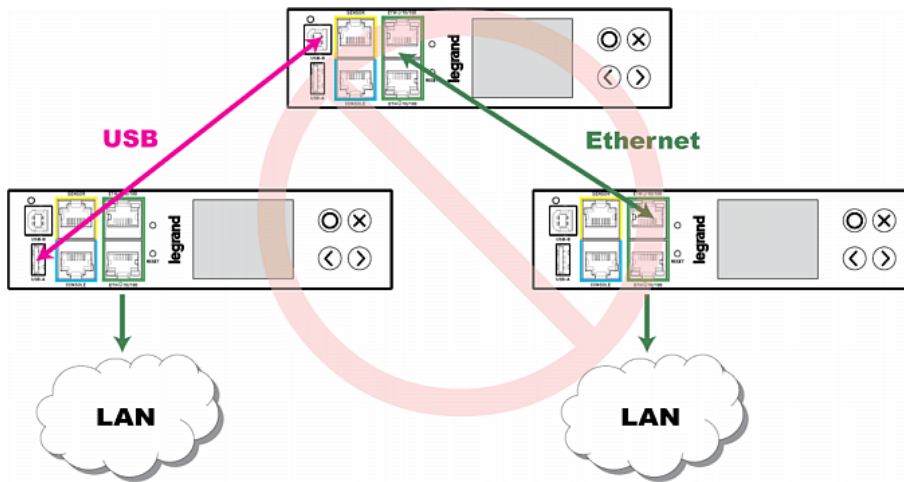
- One cascaded device has two downstream devices.
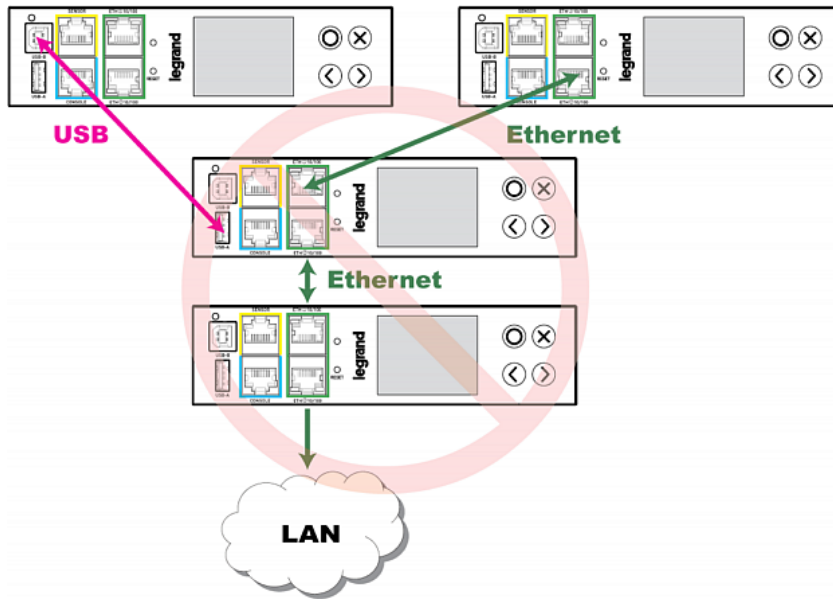
- One device is connected to another device via two cascading cables - USB and Ethernet cables.
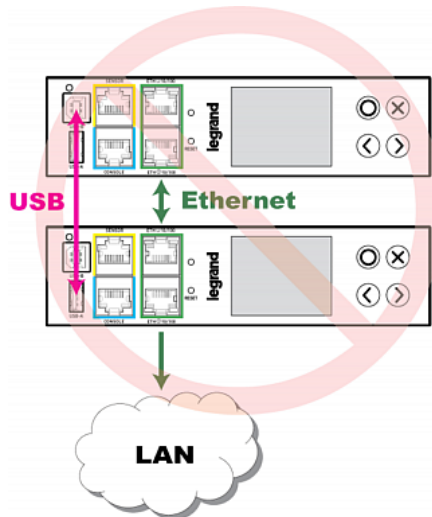
Connecting External Equipment (Optional)

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

In This Chapter

Connecting Raritan Environmental Sensor Packages

Legrand PDU supports all types of Raritan environmental sensor packages, including DPX, DPX2, DPX3, DX and DX2 sensor packages. 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/**).

An environmental sensor package may comprise sensors only or a combination of sensors and actuators.

Legrand PDU can manage a maximum of 32 sensors and/or actuators. The supported maximum cabling distance is 98 feet (30 m), except for DPX sensor packages.

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

- *DPX Sensor Packages* (on page 40)
- *DPX2 Sensor Packages* (on page 44)
- *DPX3 Sensor Packages* (on page 45)
- *DX or DX2 Sensor Packages* (on page 47)

Identifying the Sensor Port

> Warning: If you purchase Raritan's environmental sensor packages, make sure you connect them to the correct port on the Legrand PDU, or damages may be caused to the Legrand PDU 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.

![Legrand logo]

DPX Sensor Packages

Most DPX sensor packages come with a factory-installed sensor cable, whose sensor connector is RJ-12.

RJ-12
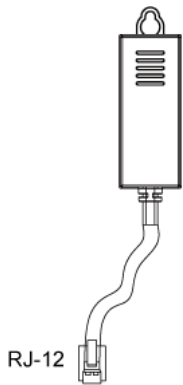
For the cabling length restrictions, see *Supported Maximum DPX Sensor Distances* (on page 43).

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

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

An RJ-12 to RJ-45 adapter is required to connect a DPX sensor package to Legrand PDU.

    a. Connect the adapter's RJ-12 connector to the DPX sensor cable.

    b. Connect the adapter's RJ-45 connector to the RJ-45 SENSOR port of the Legrand PDU.

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

1. Connect a Raritan-provided phone cable to the IN port of a differential air pressure sensor.
2. Get an RJ-12 to RJ-45 adapter. Connect the adapter's RJ-12 connector to the other end of the phone cable.
3. Connect this adapter's RJ-45 connector to the RJ-45 SENSOR port on the Legrand PDU.
4. If intended, connect one DPX sensor package to the OUT port of the differential air pressure sensor. It can be any DPX sensor package, such as a DPX-T3H1.
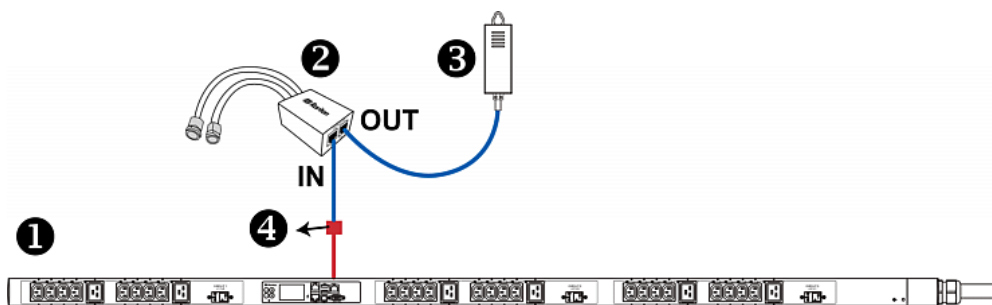
❶	The Legrand PDU
❷	Raritan differential air pressure sensors
❸	One DPX sensor package (optional)
❹	RJ-12 to RJ-45 adapter

June 2018

Using an Optional DPX-ENVHUB4 Sensor Hub

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

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

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

Tip: The Raritan sensor hub that supports ALL types of Raritan environmental sensor packages is DPX3-ENVHUB4. See **Using an Optional DPX3-ENVHUB4 Sensor Hub** *(on page 49).*

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

1. Connect the DPX-ENVHUB4 sensor hub to the Legrand PDU.

   a. Plug one end of the Raritan-provided phone cable (4-wire, 6-pin, RJ-12) into the IN port (Port 1) of the hub.

   b. Get an RJ-12 to RJ-45 adapter. Connect this adapter's RJ-12 connector to the other end of the phone cable.

   c. Connect this adapter's RJ-45 connector to the PDU's RJ-45 SENSOR port.

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

   This diagram illustrates a configuration with a sensor hub connected.
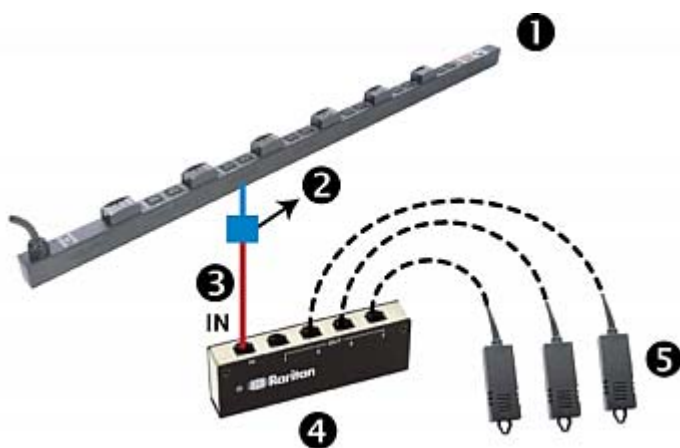
❶	Legrand PDU
❷	RJ-12 to RJ-45 adapter
❸	Raritan-provided phone cable
❹	DPX-ENVHUB4 sensor hub
❺	DPX sensor packages

Using an Optional DPX-ENVHUB2 cable

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

This cable supports DPX sensor packages only. Do NOT connect DPX2, DPX3, DX or DX2 sensor packages to it.

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

1. Use an RJ-12 to RJ-45 adapter to connect the DPX-ENVHUB2 cable to the Legrand PDU.

   a. Connect the adapter's RJ-12 connector to the cable.

     b.   Connect the adapter's RJ-45 connector to the RJ-45 SENSOR port on the Legrand PDU.

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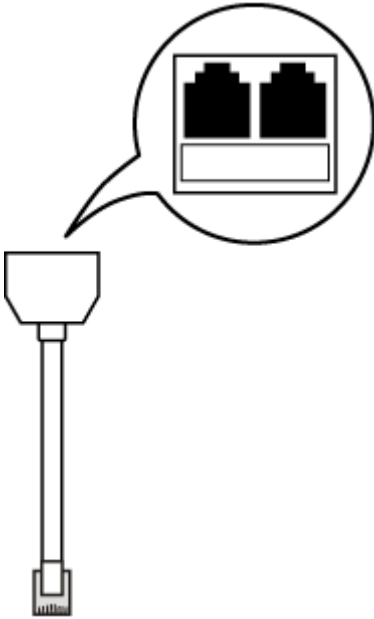
3.   Repeat the above steps if there are additional SENSOR ports on your Legrand PDU.

Supported Maximum DPX Sensor Distances

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

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

▶ **Sensor connection restrictions:**

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

▶ **Maximum distance illustration:**

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

- The sum of a DPX-T3H1 sensor cable's length is 16' (5 m).

3 m + 1 m + 1 m = 5 m
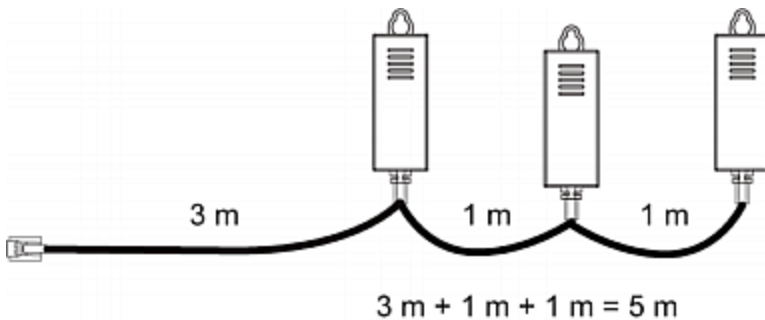
- The total cabling length between the Legrand PDU and one DPX-T3H1 is 49' (15 m) as illustrated below.

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

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

DPX2 Sensor Packages

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

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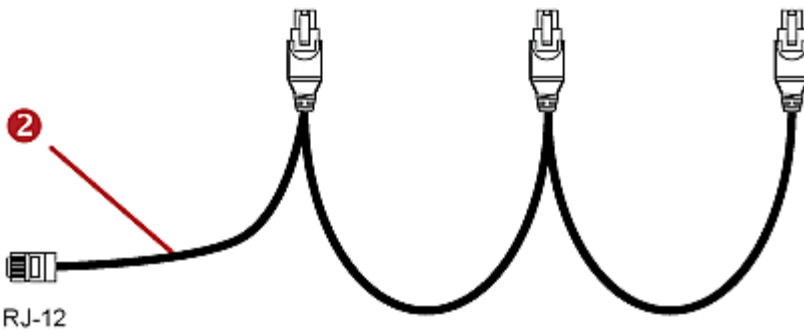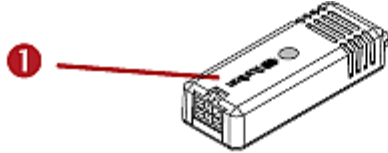
Item	
❶	DPX2 sensor package
❷	DPX2 sensor cable with one RJ-12 connector and three head connectors

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

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

▶   **To connect DPX2 sensor packages to the Legrand PDU:**

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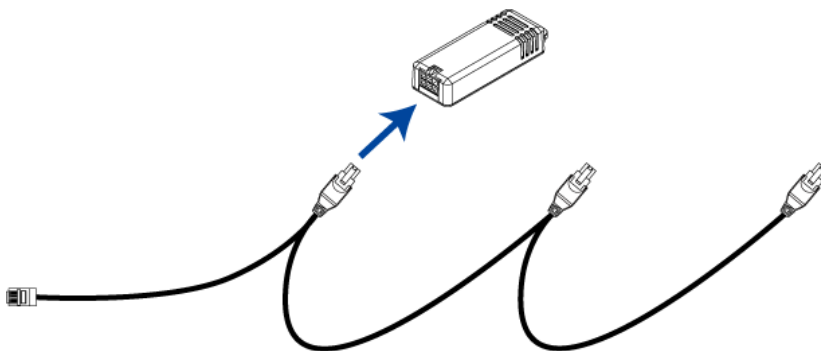
2. Connect remaining DPX2 sensor packages to the second and then the third head connector.
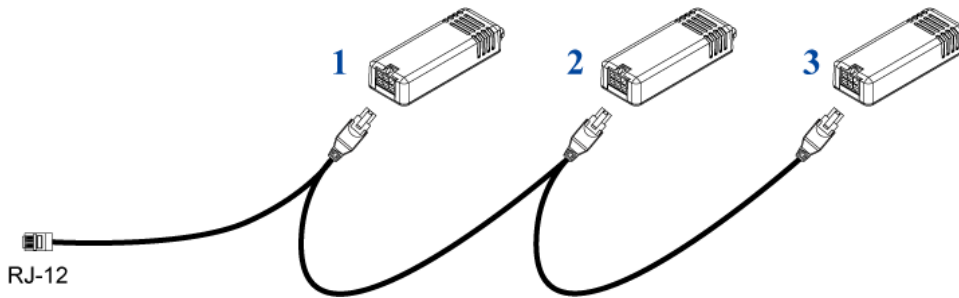
Tip: If the number of sensors you are connecting is less than the number of head connectors on your sensor cable, connect them to the first one or first two head connectors to ensure that there are NO free head connectors prior to the final DPX2 sensor package attached.

3. Use an RJ-12 to RJ-45 adapter to connect the DPX2 sensor package(s) to the Legrand PDU.
   a. Connect the adapter's RJ-12 connector to the DPX2 sensor cable.
   b. Connect the adapter's RJ-45 connector to the RJ-45 SENSOR port of the Legrand PDU.

   OR you can directly connect the DPX2 sensor package to a DX sensor chain without using any RJ-12 to RJ-45 adapter. See **Connecting a DPX2 Sensor Package to DX** (on page 48).

DPX3 Sensor Packages

A DPX3 sensor package features the following:

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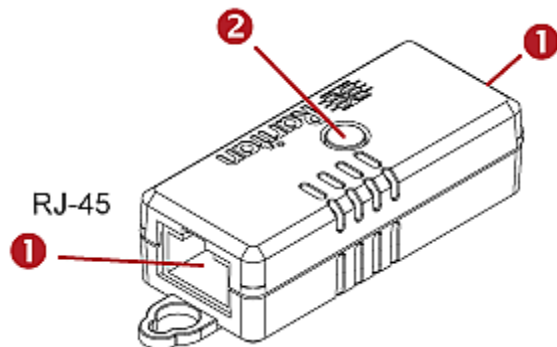
Numbers	Components
❶	RJ-45 ports, each of which is located on either end of a DPX3 sensor package.
❷	LED for indicating the sensor status.

► **To connect DPX3 sensor packages to the Legrand PDU:**

1. Connect a standard network patch cable (CAT5e or higher) to either RJ-45 port on the DPX3 sensor package.
2. If you want to cascade DPX3 sensor packages, get an additional standard network patch cable (CAT5e or higher) and then:
   a. Plug one end of the cable into the remaining RJ-45 port on the prior DPX3.
   b. Plug the other end into either RJ-45 port on an additional DPX3.

June 2018

Repeat the same steps to cascade more DPX3 sensor packages.
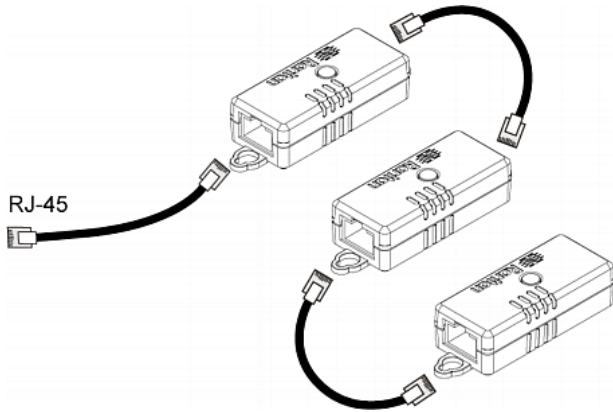
3. Connect the first DPX3 sensor package to the Legrand PDU by plugging its cable's connector into the RJ-45 SENSOR port of the Legrand PDU.

Connecting a DPX2 Sensor Package to DPX3

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

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

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

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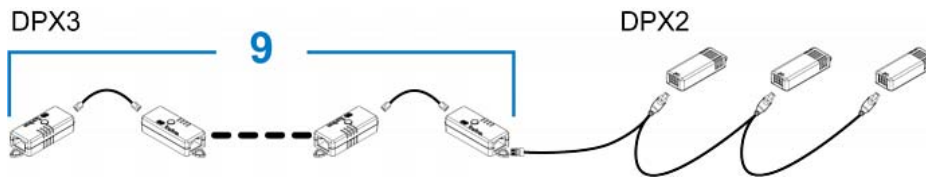
▶ **When connecting a DPX2 sensor package containing two DPX2 sensors:**

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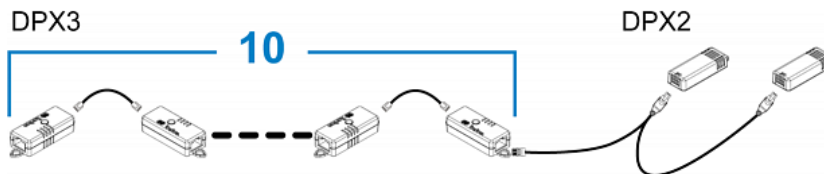
▶ **When connecting a DPX2 sensor package containing one DPX2 sensor:**

A maximum of eleven DPX3 sensor packages can be cascaded because 12-1=11.
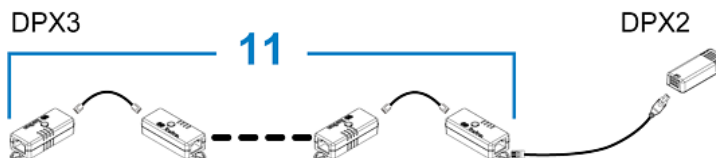
DX or DX2 Sensor Packages

DX2 sensor packages, which WILL be released one by one in 2018, are functionally similar to DX or DPX3 sensor packages. Description in this section applies to all DX and DX2 sensor packages unless otherwise specified.

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 Legrand PDU 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 Legrand PDU.

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

Tip: To manage the last 4 functions, you can release 4 "managed" sensors or actuators, and then manually bring the last 4 functions into management. See **Peripherals** *(on page 116).*
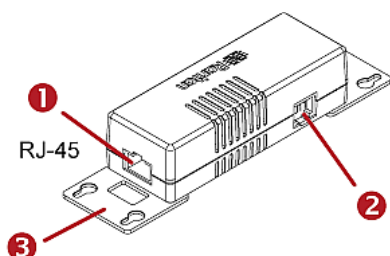
Numbers	Components
❶	RJ-45 ports, each of which is located on either end of a DX sensor package.
❷	RJ-12 port, which is reserved for future use and now blocked.
❸	Removable rackmount brackets.

Note: A DX2 sensor does not have the RJ-12 port and looks slightly different from the above image. For details, refer to the Environmental Sensors and Actuators Guide (or Online Help).

▶ **Connect DX sensor packages to the Legrand PDU:**

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. A Legrand PDU supports only one DX-PD2C5.
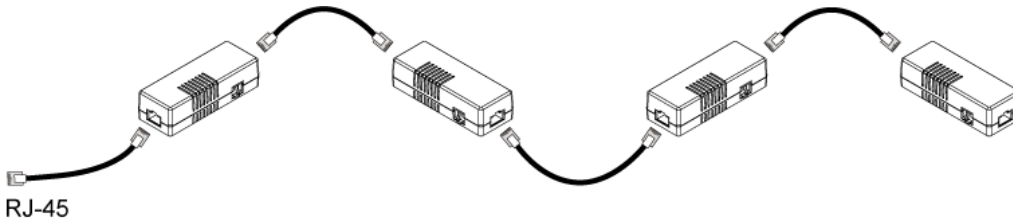
RJ-45

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

4. If needed, connect a DPX2 sensor package to the end of the DX chain. See **Connecting a DPX2 Sensor Package to DX** (on page 48).

Warning: The Legrand PDU does NOT support simultaneous connection of both DX-PD2C5 and asset management strip(s) so do NOT connect both of them at the same time.

Connecting a DPX2 Sensor Package to DX

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

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

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

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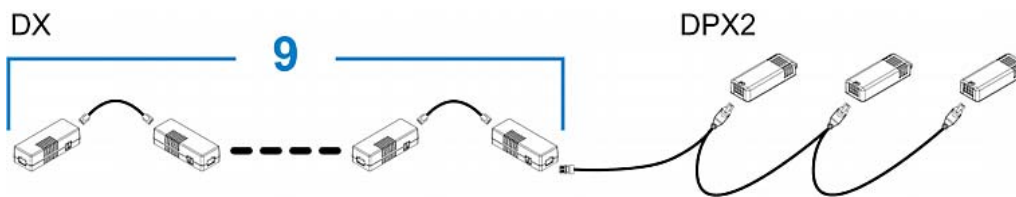
▶ **When connecting a DPX2 sensor package containing two DPX2 sensors:**

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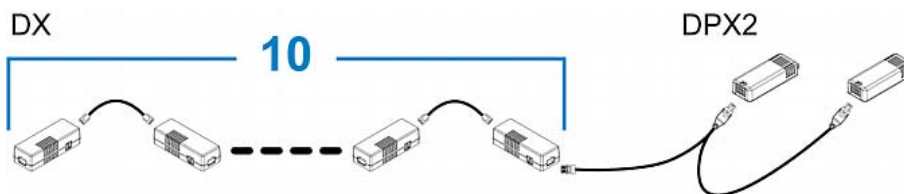
▶ **When connecting a DPX2 sensor package containing one DPX2 sensor:**

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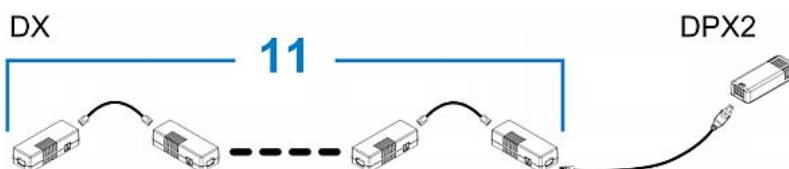
Using an Optional DPX3-ENVHUB4 Sensor Hub

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

- All ports on the DPX3-ENVHUB4 sensor hub are RJ-45 instead of RJ-12 as the DPX-ENVHUB4 sensor hub.
- The DPX3-ENVHUB4 sensor hub supports all Raritan environmental sensor packages, including DPX, DPX2, DPX3, DX and DX2 sensor packages.

To connect diverse types of sensor packages to this sensor hub, you must follow the combinations shown in the section titled ***Mixing Diverse Sensor Types*** (on page 50).

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

1. Connect the DPX3-ENVHUB4 sensor hub to the Legrand PDU 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 Legrand PDU.
2. Connect the Raritan sensor packages to any of the four OUT ports on the hub.
   - An RJ-12 to RJ-45 adapter is required for connecting a DPX or DPX2 sensor package to the hub.

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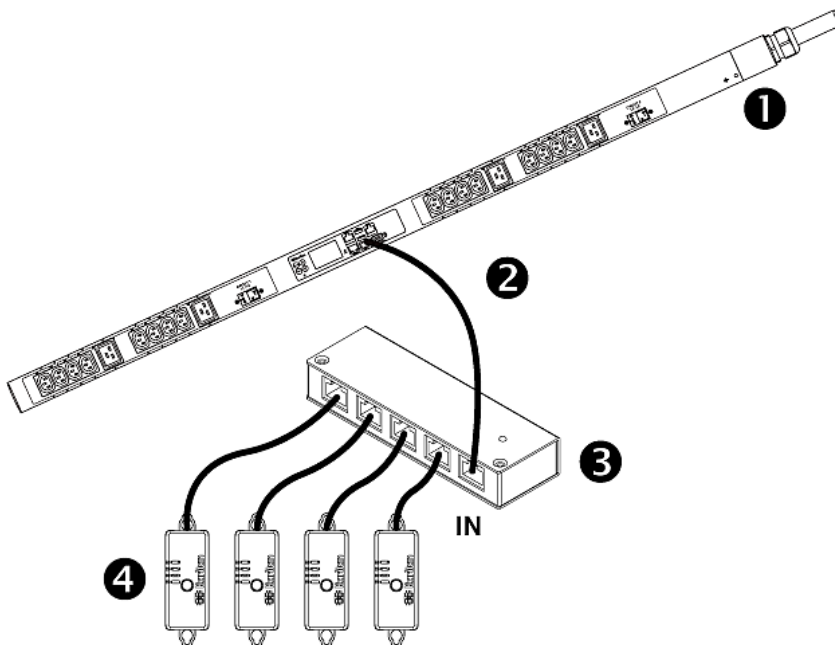
❶	Legrand PDU
❷	A standard network cable
❸	DPX3-ENVHUB4 sensor hub
❹	Any Raritan sensor packages

Mixing Diverse Sensor Types

You can mix DPX, DPX2, DPX3, DX and DX2 sensor packages on one Legrand PDU according to the following sensor combinations. In some scenarios, the DPX3-ENVHUB4 sensor hub is required.

The Legrand PDU does NOT support any other sensor-mixing combinations than those described in this section.

When mixing different sensor types, remember that the Legrand PDU supports a maximum of 32 sensors/actuators.

▶ **1 DX + 1 DPX:**

- It is strongly recommended to use an RJ-12 to RJ-45 adapter to connect the DPX sensor package to the DX sensor package.

Legrand PDU
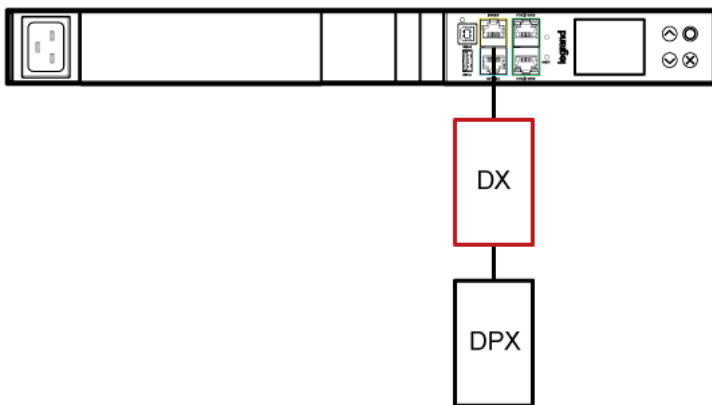
▶ **Diverse combinations via the DPX3-ENVHUB4 sensor hub:**

- You must use the **DPX3**-ENVHUB4 sensor hub instead of the old DPX-ENVHUB4 sensor hub. Each port on the hub supports any of the following:
  - A DX sensor package
  - A chain of DX sensor packages
  - A DX2 sensor package
  - A chain of DX2 sensor packages
  - A DPX3 sensor package
  - A chain of DPX3 sensor packages
  - A DPX2 sensor package
  - A DPX sensor package

- An RJ-12 to RJ-45 adapter is recommended to connect a DPX or DPX2 sensor package to DPX3-ENVHUB4.
- In the following diagrams, the sensor package in "green" can be replaced by a DPX2 sensor package. The sensor package in "blue" can be one DPX2, DPX3 or DX sensor package.

This section only illustrations the following three combinations, but actually there are tens of different combinations by using the DPX3-ENVHUB4 sensor hub.

Legrand PDU

DPX3-ENVHUB4

IN

DX

DX

DPX

DX

DX

DPX

DX /
DPX2

DX /
DPX2

Legrand PDU

IN

DPX3-ENVHUB4

DPX2 / DPX3 / DX

DPX2 / DPX3 / DX

DPX3

DPX3

DPX3 / DPX2

DPX
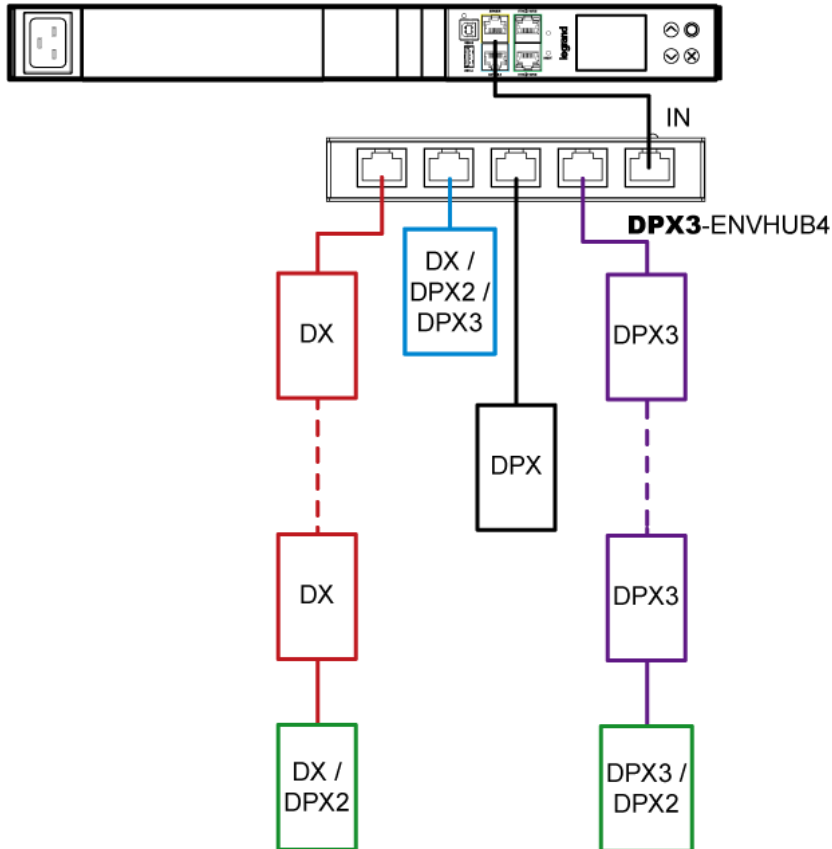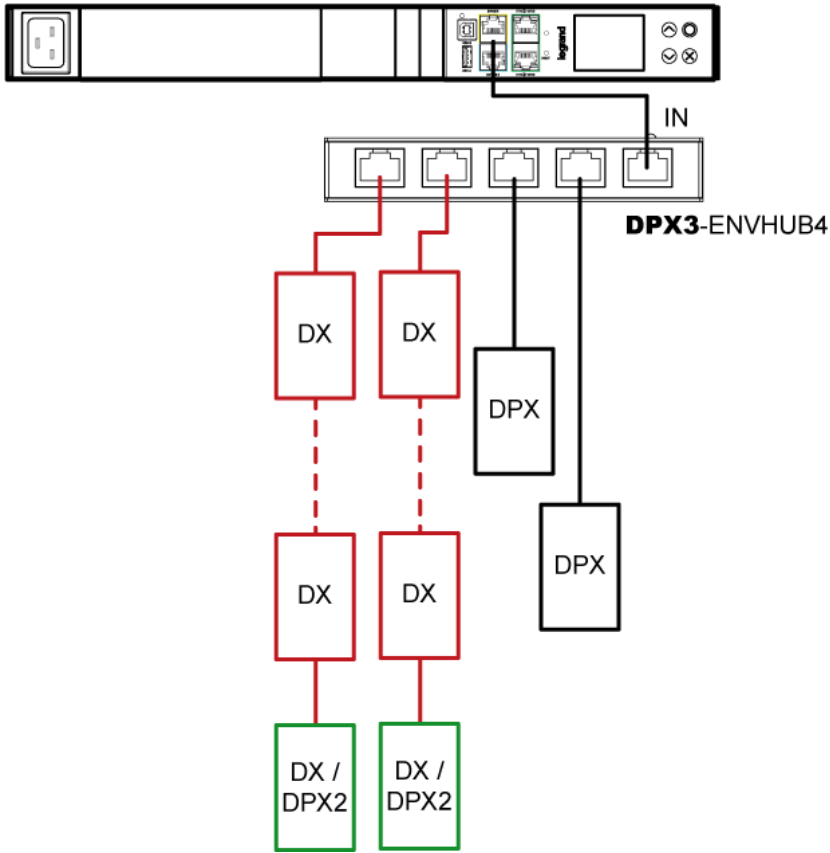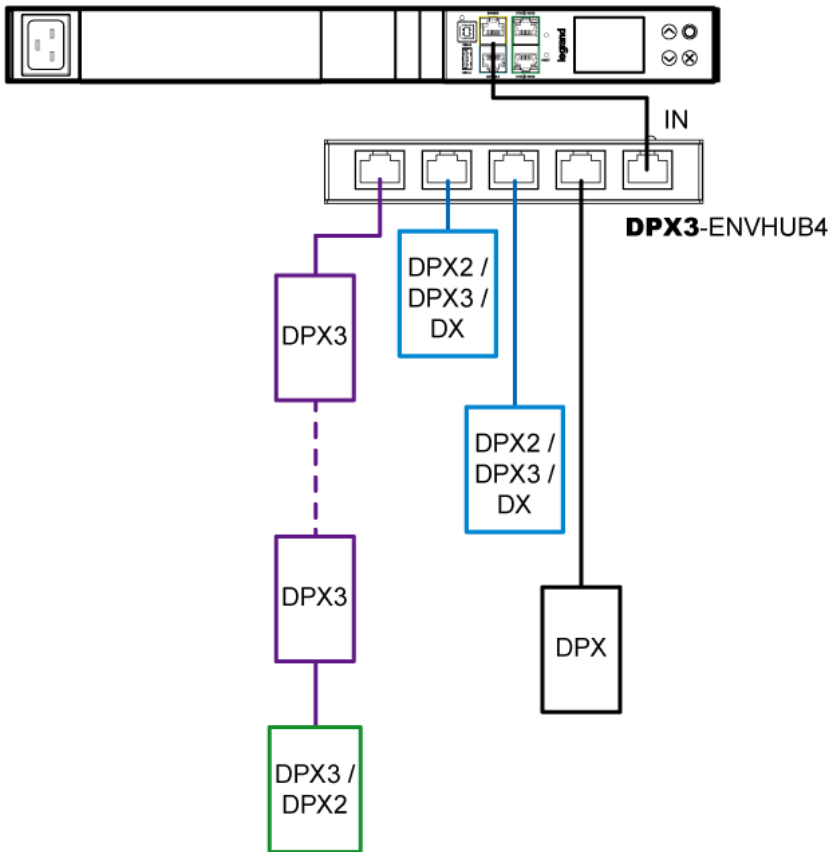
▶ **Mix DPX3 and DX or DX2 in a sensor chain:**

Any DX or DX2 sensor package in a chain can be replaced by a DPX3 sensor package, or vice versa. The total number of sensor packages in this chain cannot exceed 12.

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

You can add a DPX2 sensor package to the end of such a sensor-mixing chain if intended. See ***Connecting a DPX2 Sensor Package to DPX3*** (on page 46) or ***Connecting a DPX2 Sensor Package to DX*** (on page 48).

Connecting a Logitech Webcam

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

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

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

Other UVC-compliant webcams may also work. However, Legrand 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 Legrand PDU supports up to two webcams. You can use a "powered" USB hub to connect webcams if needed.

After connecting a webcam, you can retrieve visual information from anywhere through the Legrand PDU 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 Legrand PDU. The Legrand PDU 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 Legrand PDU web interface after the connection is complete. See ***Configuring Webcams and Viewing Live Images*** (on page 248).

June 2018

Introduction to PDU Components

This chapter explains how to use the Legrand PDU, including:

- Introduction to the LEDs and ports on the PDU
- Operation of the front panel display
- The overcurrent protector's behavior
- The reset button

In This Chapter

Panel Components

The Legrand PDU comes in Zero U, 1U, and 2U sizes. All types of models come with the following components on the outer panels.

- Inlet
- Outlets
- Connection ports
- Dot-matrix LCD display
- Reset button

Inlet

Connect each Legrand PDU to an appropriately rated branch circuit. See the label or nameplate affixed to your Legrand PDU for appropriate input ratings or range of ratings.

There is no power switch on the Legrand PDU. To power cycle the PDU, unplug it from the branch circuit, wait 10 seconds and then plug it back in.

Outlets

The total number of outlets varies from model to model.

Legrand Switched PDU

These models are outlet-switching capable. A small LED is adjacent to each outlet to indicate the state of the relay board.

LED state	Outlet status	What it means
Not lit	Powered OFF	The outlet is turned off and no power is available. OR the control circuitry's power supply is broken. OR the outlet's associated circuit breaker has tripped.
Red	ON and LIVE	LIVE power. The outlet is on and power is available.

LED state	Outlet status	What it means
	ON and NOT LIVE	The outlet is turned on but power is not available. This is probably because the outlet's relay board is damaged. Please contact Legrand Technical Service for RMA service.

Legrand Metered PDU

These models are NOT outlet-switching capable so all outlets are always in the ON state.

Outlet LEDs are not available.

Connection Port Functions

A Legrand PDU has 6 ports.

▶ **6 ports on the front panel:**
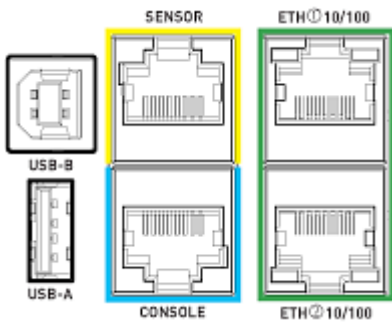
- CONSOLE port x 1 (blue)
- Sensor port x 1 (yellow)
- USB-A port x 1
- USB-B port x 1
- Ethernet port x 2 (green)

▶ **Legrand PDU models:**

The table below explains the function of each port.

Port	Used for...

USB-B	• Cascading Legrand PDUs for sharing a network connection. See *Cascading All Devices via USB* (on page 33).
	• Establishing a USB connection between a computer and the Legrand PDU for:
	  ▪ Using the command line interface.
	  ▪ Performing the disaster recovery. Contact Legrand Technical Support for instructions.
	• Connecting to an Android mobile device for viewing or configuring the Legrand PDU.
	See *Connecting a Mobile Device to Legrand PDU* (on page 26).

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 Legrand PDU. See *Connecting a Mobile Device to Legrand PDU* (on page 26).
	• Connecting a USB device, such as a Logitech® webcam or wireless LAN adapter.
	• Cascading Legrand PDUs for sharing a network connection.
CONSOLE **(RJ-45)**	Establishing a serial connection between the Legrand PDU and a computer for accessing the command line interface..
	You need a third-party RJ-45 to DB9 adapter/cable for the connection. See *RJ45-to-DB9 Cable Requirements for Computer Connections* (on page 31).
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.
ETH①10/100, ETH②10/100	Legrand PDU has two Ethernet ports, supporting up to 100 Mbps.
	Connecting the Legrand PDU to your company's network via a standard network patch cable (Cat5e/6). This connection is necessary to administer or access the Legrand PDU 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 Legrand PDUs* (on page 35).
	Note: Connection to this port is not required if wireless connection is preferred, or if the Legrand PDU is a slave device in the cascading configuration. See **Cascading Multiple Legrand PDUs for Sharing Ethernet Connectivity** *(on page 32).*

Front Panel Display

The following diagram shows the dot-matrix LCD display panel on Zero U models.
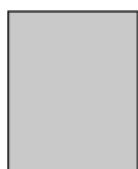
You can use the LCD display to view the Legrand PDU information and even switch an outlet. It consists of:

- A dot-matrix LCD display
- Four control buttons

Zero U models automatically adjust the orientation of the content shown on the dot-matrix LCD display after detecting the direction in which the PDU is installed. 1U and 2U models do NOT adjust the content's orientation.

Note: All dot-matrix LCD display diagrams illustrated in the User Guide are for Zero U models. Your dot-matrix LCD may look slightly different if it is on a 1U/2U model.

Automatic and Manual Modes

After powering on or resetting the Legrand PDU, the front panel LCD display first shows a dark screen, then Legrand logo and finally enters the automatic mode.

▶ **Automatic mode without alerts available:**

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

If overcurrent protectors are available on your Legrand PDU, the display cycles between both the inlet and overcurrent protector information.

Note: You can make a Legrand PDU with overcurrent protectors show the inlet information only in the automatic mode. See **Front Panel Settings** *(on page 224).*

▶ **Manual mode:**

To view more information or control outlets if your Legrand PDU is outlet-switching capable, enter the manual mode.

Press ⭕ or ✖ to enter the manual mode, where the Main Menu is first displayed. See **Main Menu** (on page 60).

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 the inlet 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 75).

  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 59).

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 Legrand PDU, built-in components, or connected peripheral devices
- Control outlets if your model supports outlet-switching
- 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 120).

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

Alerts
PDU
Inlet I1
OCPs
Outlets
Peripherals
Device Info

X Auto   9:57 PM   Select ⭘
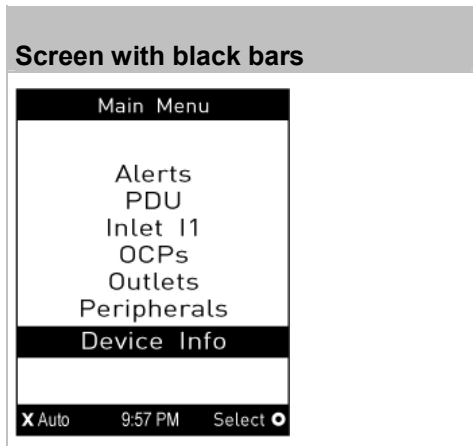
Main Menu

The Main Menu contains 5 to 7 menu commands, depending on the model.

Control buttons that can be used and the system time are shown at the bottom of the LCD display.

Main Menu

Alerts
PDU
Inlet I1
OCPs
Outlets
Peripherals
Device Info

X Auto   9:57 PM   Select ⭘
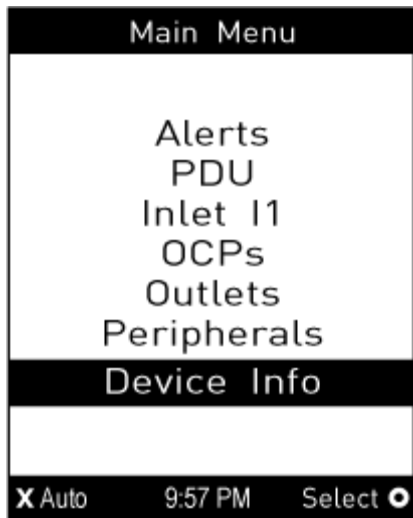
If any alerts exist, the top and bottom bars on the LCD display change the color from black to yellow or red. See **Operating the Dot-Matrix LCD Display** (on page 59).

Menu command	Function
Alerts	Indicates all alerted sensors, if any. See *Alerts* (on page 61).
PDU	Shows the internal beeper's state, and, if it is on, the reason for turning on. If your Legrand PDU has multiple inlets, this menu item also shows the total active power and total active energy. See *PDU* (on page 62).
Inlet I1	Shows the inlet I1's information. See *Inlet* (on page 63).
OCPs	Shows a list of overcurrent protector information. See *OCPs* (on page 64). Only Legrand PDU models with overcurrent protectors have this menu item.
Outlets	This menu command is available on Legrand Switched PDUs only. Shows each outlet's information. If your Legrand PDU supports outlet-switching, you can turn on, off or power cycle an outlet. See *Outlets* (on page 65).
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 67).
Device Info	Shows the device information of Legrand PDU, such as IP and MAC address. See *Device Info* (on page 70).

Note: To return to the automatic mode, press ⊗. *See* **Automatic and Manual Modes** *(on page 58).*

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
- Any tripped circuit breakers or blown fuses

Tip: The same information is available in the web interface's Dashboard. See **Dashboard - Alerted Sensors** *(on page 91).*

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 120).

- 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 59).

Number	Description
❶	Sensor names.
❷	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 121). ▪ Alarmed ▪ Lower Critical = below lower critical ▪ Lower Warning = below lower warning ▪ Upper Warning = above upper warning ▪ Upper Critical = above upper critical ▪ Open (for overcurrent protectors)

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

PDU

You can configure the following feature with the "PDU" menu command.

- Energy pulse output settings

This feature, once enabled, blinks the energy pulse LED proportional to the energy consumption. For this LED's location, see **Energy Pulse LED** (on page 76).

It can be used as a simple interface in certification labs where they use an optical sensor to count the number of pulses and compare it to the energy reading of a reference meter.

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

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

2. The Energy Pulse page opens. By default the energy pulsing is turned off. DO NOT enable this feature unless you have to use it.

```
            Energy Pulse


    LED Energy Metering Pulse
         Disabled




    ✗ Back     9:57 PM    Setup ⊙
```
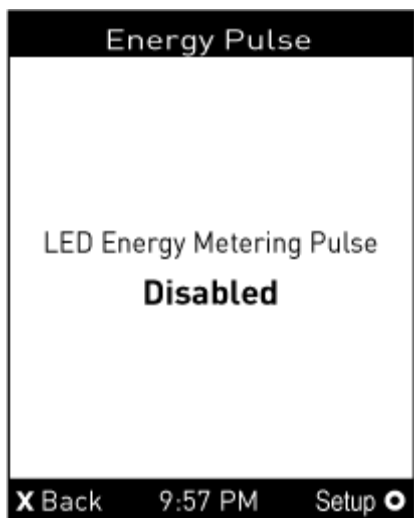
    a. To change the energy pulse settings, press ⊙.

    b. Press ⌃ or ⌄ to select an option.

    c. Press ⊙ to confirm the selection, or ⊗ to cancel.

3. To return to the Main Menu, press ⊗.

Inlet

An inlet's information is separated into two pages. Page numbers are indicated in the top-right corner of the LCD display.

▶ **To show the inlet information:**

1. Press ⌃ or ⌄ to select "Inlet I1" in the Main Menu, and press ⊙.
2. The first page shows the inlet's active power (W), apparent power (VA), power factor (PF), and active energy (Wh).

```
Inlet  I1                  1/2
            Active Power:
         4,898 w
          Apparent Power:
         4,998 VA
           Power Factor:
              0.98
           Active Energy:
              0 Wh

    ✗ Back     9:57 PM
```
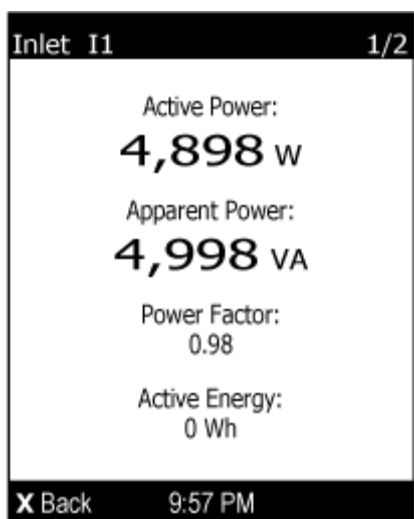
3. To go to other page(s), press ⌃ or ⌄.

■ For a single-phase model, the second page shows the inlet's voltage (V), frequency (Hz) and current (A).

```
Inlet  I1                    2/2

            Voltage:
          224 v

           Frequency:
          60.0 Hz

            Current:
          0.000 A


X Back        9:57 PM
```
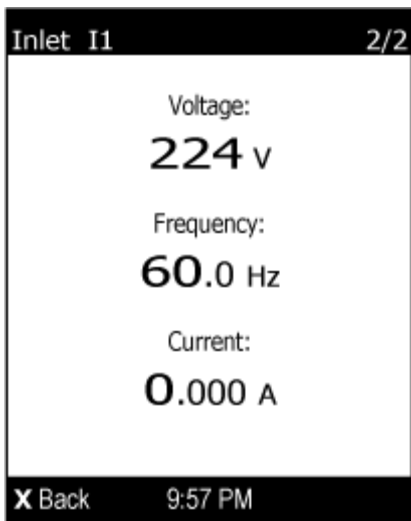
■ For a three-phase model, the next several pages respectively show unbalanced current's percentage, line frequency, and the current and voltage values of each line.

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

OCPs

If your model has more overcurrent protectors (OCPs) than the LCD display can show at a time, a page number appears in the top-right corner of the display. Otherwise, no page numbers are available.

▶ **To show the overcurrent protector information:**

1. Press ⌃ or ⌄ to select "OCPs" in the Main Menu, and press ◯.
2. The LCD display shows a list of overcurrent protectors similar to the following diagram.

```
               OCPs

Circuit Breaker C1
L1-N, 20A            0.000 A
Circuit Breaker C2
L1-N, 20A            0.000 A

❶                      ❷


X Back        9:57 PM
```
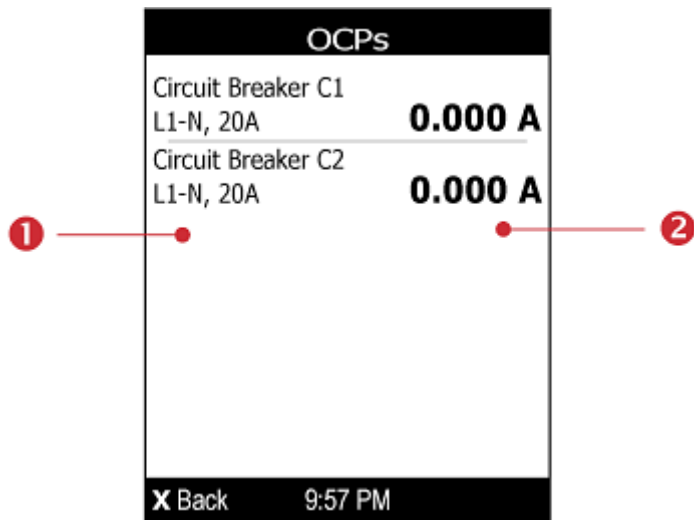
Number	Description
❶	Overcurrent protector names. Associated lines and rated current are displayed below each overcurrent protector's name.

Number	Description
❷	Current reading of the corresponding overcurrent protector.

3. If the desired overcurrent protector is not visible, press ⌃ or ⌄ to scroll up or down.

Note: If any circuit breaker trips, the list of overcurrent protectors looks slightly different from the above diagram. The tripped one will show "open" instead of a current reading.

Outlets

This outlet-related section applies to Legrand Switched PDUs only.

With the front panel display, you can do the following for outlets:

- Show each outlet's information.
- Turn on, off or power cycle an individual outlet if your Legrand PDU is outlet-switching capable. To do this, you must first enable the front panel outlet control function. See **Front Panel Settings** (on page 224).

Showing Outlets Information

Multiple outlet information can be displayed on the LCD display.

Control buttons that can be used and the system time are shown at the bottom of the LCD display.

▶ **To show outlets information:**

1. Press ⌃ or ⌄ to select "Outlets" in the Main Menu, and press ⊙.
2. The LCD display shows a list of outlets with their receptacle types, and power states which are indicated by the colors of circles.

   The currently-selected outlet number and total of outlets are indicated in the top-right corner of the display.

   ▪ A red circle indicates that this outlet is powered on.
   ▪ A green circle indicates that this outlet is powered off.

3. Press ⌃ or ⌄ to select an outlet, and press ⊙.

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

4. To return to the Main Menu, press ⊗ several times until the Main Menu is shown.

Power Control

The front panel outlet control must be enabled for performing this power control function. The default is to disable this function. See ***Front Panel Settings*** (on page 224).

Available options for power control vary, based on the power state of the selected outlet.

- For an outlet which has been turned on, the 'Switch On' option is unavailable.
- For an outlet which has been turned off, the 'Switch Off' option is unavailable.

Control buttons that can be used and the system time are shown at the bottom of the LCD display.

▶ **To power on, off or cycle an outlet using the LCD display:**

1. Press ⌃ or ⌄ to select "Outlets" in the Main Menu, and press ◎.
2. The LCD display shows a list of outlets with their receptacle types, and power states which are indicated by the colors of circles.

   The currently-selected outlet number and total of outlets are indicated in the top-right corner of the display.

   - A red circle indicates that this outlet is powered on.
   - A green circle indicates that this outlet is powered off.
   - If so, the word "Off" replaces the current value.
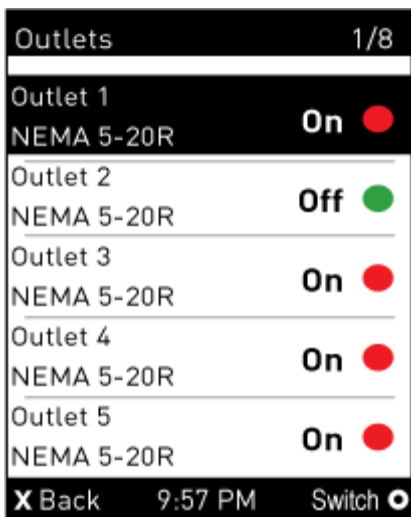
```
Outlets                    1/8
┌─────────────────────────────┐
│ Outlet 1                     │
│ NEMA 5-20R        On  ●      │
├─────────────────────────────┤
│ Outlet 2                     │
│ NEMA 5-20R        Off ●      │
├─────────────────────────────┤
│ Outlet 3                     │
│ NEMA 5-20R        On  ●      │
├─────────────────────────────┤
│ Outlet 4                     │
│ NEMA 5-20R        On  ●      │
├─────────────────────────────┤
│ Outlet 5                     │
│ NEMA 5-20R        On  ●      │
├─────────────────────────────┤
│ X Back    9:57 PM   Switch ○ │
└─────────────────────────────┘
```

3. Press ⌃ or ⌄ to select an outlet, and press ◎.

   If the desired outlet is not visible, press ⌃ or ⌄ to scroll up or down.
4. The power control page opens. A submenu similar to the following diagram appears.

   Note: The submenu is not available when the front panel outlet control is disabled. If so, a message "Front-panel outlet control is disabled" is displayed.

When the selected outlet has been turned off, 'Switch On' replaces the option of 'Switch Off'.

```
┌─────────────────────────────┐
│         Outlet  N           │
│                             │
│                             │
│                             │
│                             │
│ ▌       Switch Off          │
│          Cycle              │
│                             │
│                             │
│                             │
│                             │
│ ✕ Back    9:57 PM   Select ⬤│
└─────────────────────────────┘
```
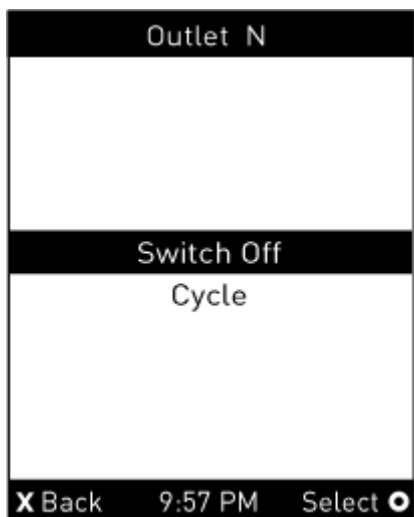
5. Press ⌃ or ⌄ to select the desired option, and press ⬤.
   - Switch Off: Turn off the outlet.
   - Switch On: Turn on the outlet.
   - Cycle: Power cycle the outlet. The outlet is turned off and then on.

6. A confirmation message appears. Press ⌃ or ⌄ to select Yes or No, and then press ⬤.
   - Yes: Confirm the operation.
   - No: Abort the operation.

7. Verify that the selected outlet is switched on or off, depending on the option you selected in the above step.
   - Check the outlet state shown on the LCD display -- red or green circles.
   - Check the outlet LED. A green LED indicates that the outlet is turned off, and a red LED indicates that the outlet is turned on.

8. To return to the Main Menu, press ✕ several times until the Main Menu is shown.

Peripherals

If there are no Raritan environmental sensor packages connected to your Legrand PDU, 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 229).

▶ **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 120).

The top and bottom bars also turn yellow or red. See **Operating the Dot-Matrix LCD Display** (on page 59).

Number	Description
❶	Sensor or actuator names.
❷	Sensor or actuator states as listed below. For further information, see **Sensor/Actuator States** (on page 121). ▪ *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* 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 ⬡. A screen similar to the following is shown.

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.
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 Legrand PDU. ▪ *Chain Pos. <n>*: <n> is the sensor or actuator's position in a sensor daisy chain. *Note: Only DX, DX2, DPX2 and DPX3 sensor packages provide the chain position information.* ▪ If this sensor or actuator is on a sensor package with multiple channels, such as DX-D2C6, 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* or *Alarmed*. ▪ 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 125).

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

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

```
┌─────────────────────────────────┐
│      Peripheral Actuator 6      │
│                                 │
│      Powered Dry Contact 1      │
│                                 │
│           QU74592507            │
│        Port 1, Chain Pos. 1     │
│            Channel 1            │
│                                 │
│             Off                 │
│                                 │
│             X: -                │
│             Y: -                │
│             Z: -                │
│                                 │
│ ✗ Back     9:57 PM    Switch ◉  │
└─────────────────────────────────┘
```
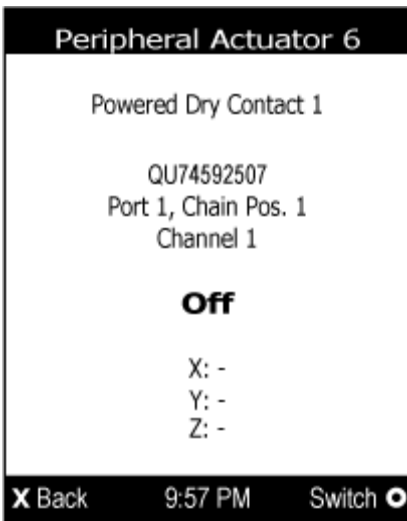
2. Press ◉ to turn on or off the actuator. A confirmation message similar to the following is shown.

```
┌─────────────────────────────────┐
│      Peripheral Actuator 6      │
│                                 │
│     Do you really want          │
│       to switch on              │
│       Powered Dry               │
│       Contact 1?                │
│                                 │
│   ┌─────────────────────────┐   │
│   │         Yes             │   │
│   ├─────────────────────────┤   │
│   │         No              │   │
│   └─────────────────────────┘   │
│                                 │
│ ✗ 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.

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 ◉.

June 2018

2. Device information similar to the following diagram displays.
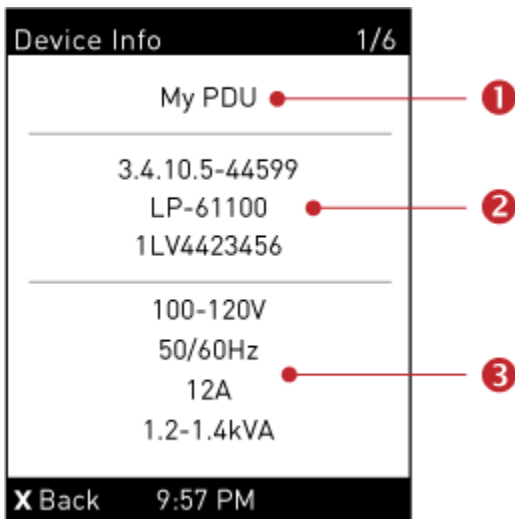
Number	Description
❶	Device name.
❷	Firmware version, model name and serial number.
❸	Device ratings, including rated voltage, frequency, current and power.

3. Press ⌄ to show the Network Common page.
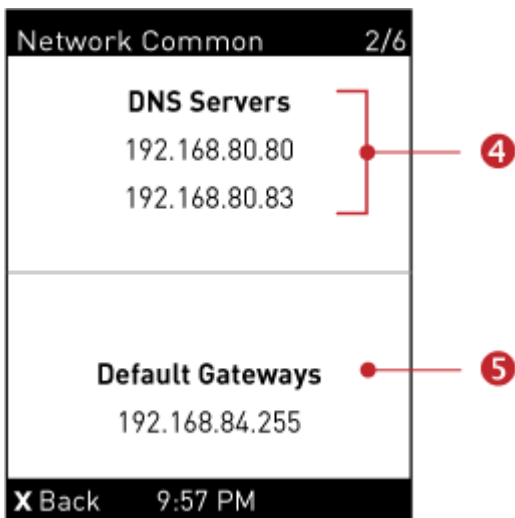
Number	Description
❹	DNS servers.
❺	Default gateways.

4. Press ⌄ to show the Network Cascading page.

```
Network Cascading      3/6



          No Cascading        ●────────── ⑥




X Back      9:57 PM
```

```
Network Cascading      3/6

  Network Bridge Enabled

        IPv4
        DHCP
   192.168.84.53/24

        IPv6
     IPv6 Disabled

X Back      9:57 PM
```

```
Network Cascading      3/6


   Port Forwarding Master




   Slave Connected: yes

X Back      9:57 PM
```

Number	Description
⑥	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 150). ▪ 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.

A Legrand PDU 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 143).*

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

6. Press ⌄ to show the WIRELESS page.

WIRELESS 6/6	WIRELESS 6/6
No Adapter Detected	00:19:70:0f:a4:33 mySSID
	IPv4 DHCP 192.168.84.30/24 ⑨
Interface Disabled	**IPv6** IPv6 Disabled
✗ Back 9:57 PM	✗ Back 9:57 PM

OR

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

7. 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, the screen's background turns red.

For color definitions, see **Yellow- or Red-Highlighted Sensors** (on page 120).

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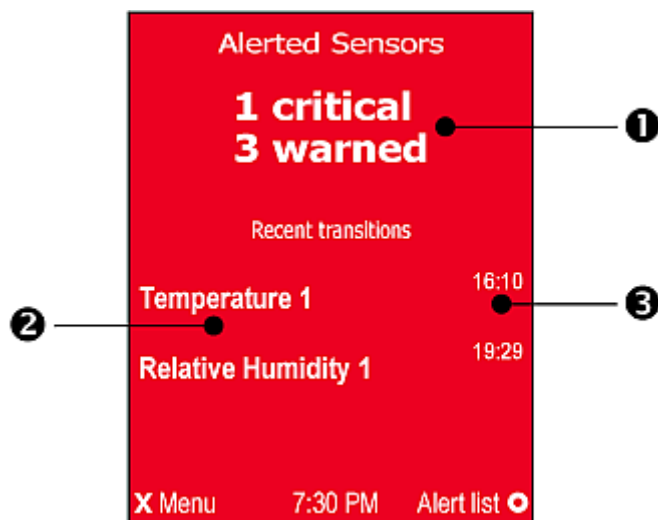
Number	Description
❶	The total of alerted sensors in critical and warning levels.
❷	A list of final alerted sensors that changed their readings or states.
❸	The final time that each alerted sensor changed its readings or states.

► **Next steps:**

- To view details of all alerted sensors, press ⭕. If the detailed information exceeds one page, press ⌃ or ⌄ to switch between pages.
- To return to the Alerts Notice screen, press ⓧ.

When upgrading the Legrand PDU, 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 near the display panel on the PDU.

Pressing this reset button restarts the software of Legrand PDU without any loss of power to outlets.

The Legrand PDU can be reset to its factory default values using this button when a serial connection is available. See *Resetting to Factory Defaults* (on page 429).

The following image illustrates the location of the reset button on Zero U models.
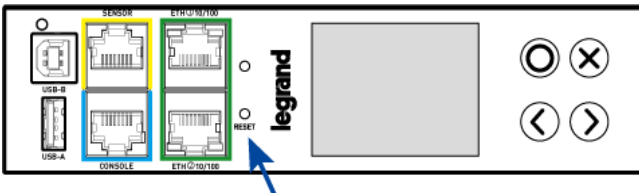
Energy Pulse LED

The energy pulse LED is located near the USB-B port on the front display panel.

The following image illustrates a Zero U model's panel.
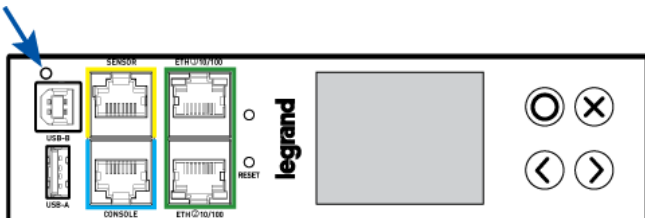
It can be used as a simple interface in certification labs where they use an optical sensor to count the number of pulses and compare it to the energy reading of a reference meter.

By default this LED is disabled. You need to enable and configure the energy pulse settings first before you can use it for verifying the pulse output. See *PDU* (on page 62).

June 2018

Circuit Breakers

Legrand PDU models rated over 20A (North American) or 16A (international) contain overcurrent protectors for outlets, which are usually branch circuit breakers. These circuit breakers automatically trip (disconnect power) when the current flowing through the circuit breaker exceeds its rating.

If a circuit breaker switches off power, the LCD display shows `open`. To find which circuit breaker is open (trips), select Alerts or OCPs in the Main Menu. See **_Operating the Dot-Matrix LCD Display_** (on page 59).

When a circuit breaker trips, power flow ceases to all outlets connected to it. You must manually reset the circuit breaker so that affected outlets can resume normal operation.

Depending on the model you purchased, the circuit breaker may use a button- or handle-reset mechanism.

Resetting the Button-Type Circuit Breaker

Your button-type circuit breakers may look slightly different from the images shown in this section, but the reset procedure remains the same.

▶ **To reset the button-type breakers:**

1. Locate the breaker whose ON button is up, indicating that the breaker has tripped.
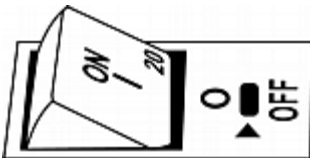
2. Examine your Legrand PDU and the connected equipment to remove or resolve the cause that results in the overload or short circuit. **This step is required, or you cannot proceed with the next step.**
3. Press the ON button until it is completely down.

Resetting the Handle-Type Circuit Breaker

Your handle-type circuit breakers may look slightly different from the images shown in this section, but the reset procedure remains the same.

▶ **To reset the handle-type breakers:**

1. Lift the hinged cover over the breaker.
2. Check if the colorful rectangle or triangle below the operating handle is GREEN, indicating that the breaker has tripped.
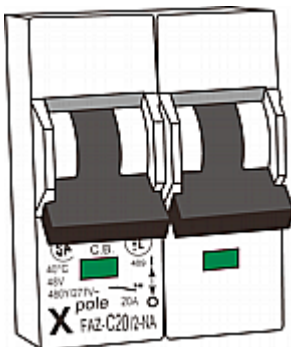
3. Examine your Legrand PDU and the connected equipment to remove or resolve the cause that results in the overload or short circuit. **This step is required, or you cannot proceed with the next step.**

4. Pull up the operating handle until the colorful rectangle or triangle turns RED.
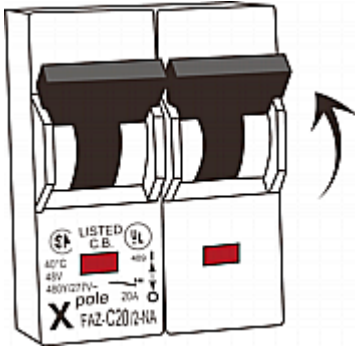
Using the Web Interface

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

In This Chapter

Supported Web Browsers

- Internet Explorer® 11
- Microsoft Edge
- 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 Legrand PDU, 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 130).

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 Legrand PDU.
   - 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 16).
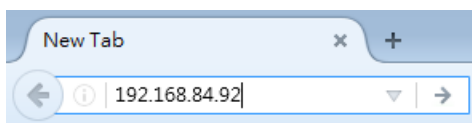
> *Tip: You can also enter the desired page's URL so that you can immediately go to that page after login. See* **Quick Access to a Specific Page** *(on page 86).*

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

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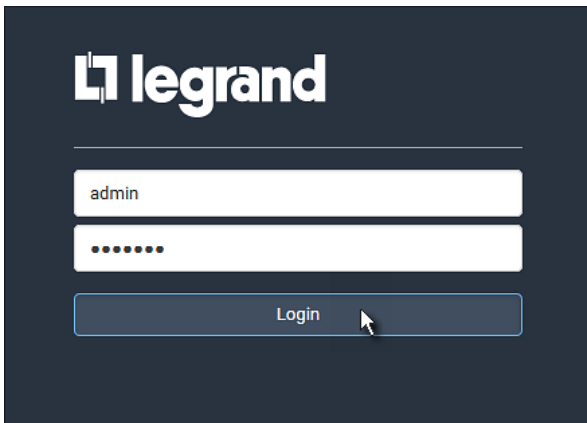
3. (Optional) If a security agreement is displayed, accept it. Otherwise, you cannot log in.

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

   Note: To configure the security agreement, see **Enabling the Restricted Service Agreement** *(on page 181).*

4. Click Login or press Enter. The web interface of Legrand PDU opens.

   Depending on your hardware configuration, your web interface shown onscreen may look slightly different from the image below.
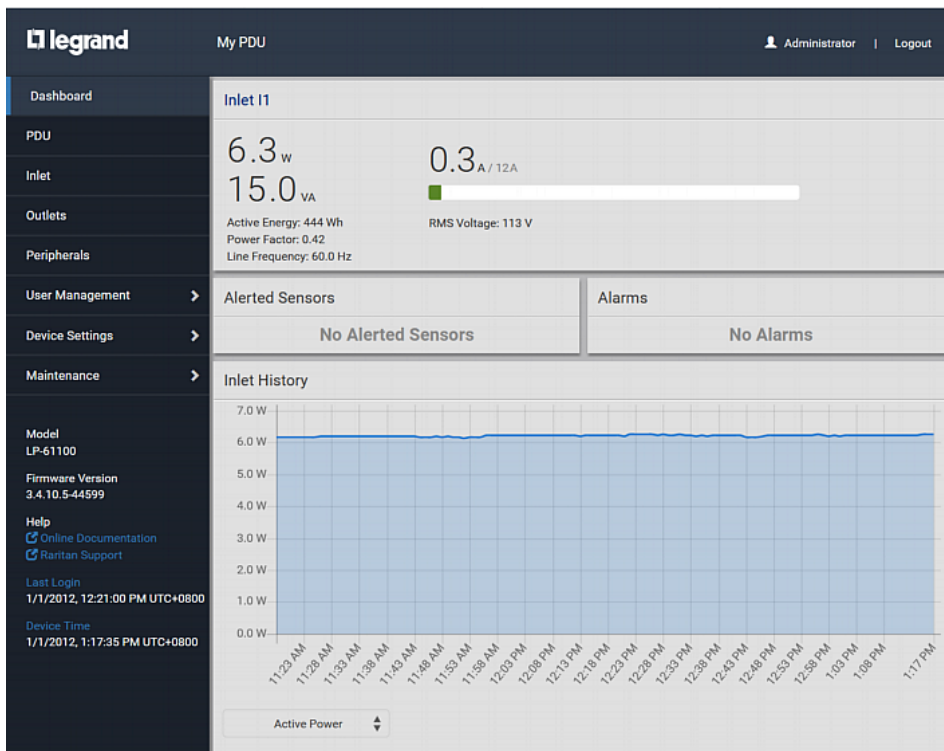
Note: The address to access a slave device in the Port Forwarding mode via non-standard ports is a combination of a protocol (http:// or https://), an IP address and a port number. See **Port Forwarding Examples** *(on page 155).*

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 133).

▶ **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 130).*

▶ **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 135).

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

Remembering User Names and Passwords

Legrand PDU 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.

Legrand PDU does NOT support other browser password managers.

Logout

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

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

- Click "Logout" on the top-right corner.
  -- OR --
- Close the tab of Legrand PDU 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 [Legrand logo] on the top-left corner.

Number	Web interface element
❶	*Menu* (on page 84)
❷	Data/setup page of the selected menu item.
❸	▪ Left side: - Legrand PDU device name. *Note: To customize the device name, see* **PDU** *(on page 94).* ▪ Right side: - Your login name, which you can click to view your user account settings. - Logout button.
❹	From top to bottom -- ▪ Your Legrand PDU model. ▪ Current firmware version. ▪ **Online Documentation**: link to the online help of Legrand PDU. - See ***Browsing through the Online Help*** (on page 494).

Number	Web interface element
	▪ **Raritan Support**: link to the Legrand PDU section of Raritan Technical Support webpage.
	▪ Date and time of your user account's last login.
	- Click **Last Login** to view your login history.
	▪ Legrand PDU 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 Legrand PDU may show all or some menu items shown below.
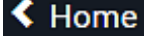
Menu	Information shown
Dashboard	Summary of the Legrand PDU status, including a list of alerted sensors and alarms, if any. See **Dashboard** (on page 87).
PDU	Device data and settings, such as the device name and MAC address. See **PDU** (on page 94).
Inlet	Inlet status and settings, such as inlet thresholds. See **Inlet** (on page 98).
Outlets	Outlet status, settings and outlet control if your model is outlet-switching capable. See **Outlets** (on page 100).

Menu	Information shown
OCPs	The OCPs menu item displays only when there are overcurrent protectors implemented on your model.
	OCP status and settings, such as OCP thresholds. See **OCPs** (on page 110).
Peripherals	Status and settings of Raritan environmental sensor packages, if connected. See **Peripherals** (on page 116).
Webcams	The 'Webcams' menu item appears when there is any webcam(s) connected to the Legrand PDU, or when there are snapshots saved onto the Legrand PDU already.
	Webcam live snapshots/video and webcam settings. See **Webcam Management** (on page 247).
SmartLock -- *and/or* -- Card Readers	Either or both menu items appear when you connect the equipment included in a Raritan's SmartLock kit to Legrand PDU. For details, refer to the user documentation accompanying the SmartLock kit or download it from Legrand's **Support page** (*http://www.raritan.com/support/*).
	▪ **SmartLock**: Configures and controls the door handles connected to Legrand PDU 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 Legrand PDU directly or indirectly. See **SmartLock and Card Reader** (on page 257).
User Management	Data and settings of user accounts and groups, such as password change. See **User Management** (on page 130).
Device Settings	Device-related settings, including network, security, system time, event rules and more. See **Device Settings** (on page 139).
Maintenance	Device information and maintenance commands, such as firmware upgrade, device backup and reset. See **Maintenance** (on page 230).

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

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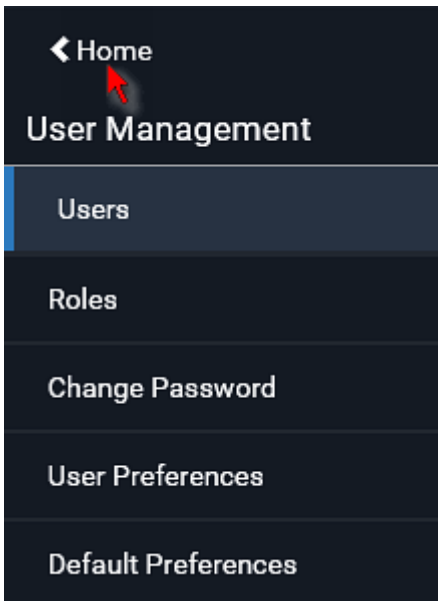
- Click **legrand** on the top-left corner to return to the main menu.

Quick Access to a Specific Page

If you often visit a specific page in the Legrand PDU 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 Legrand PDU 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 Legrand PDU 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 four to five sections, depending on your model.
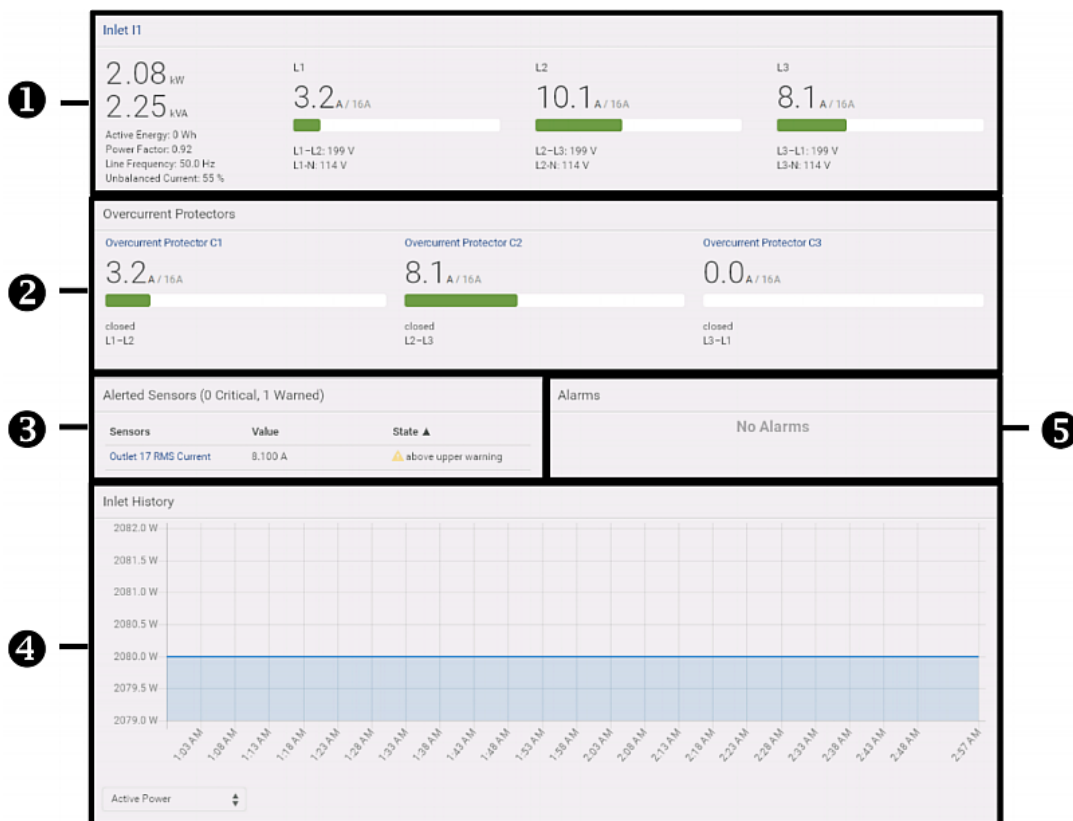
Number	Section	Information shown

❶	**Inlet I1**	▪ Overview of inlet power data
		▪ A current bar per phase, which changes colors to indicate the RMS current state
		  - green: normal
		  - yellow: warning
		  - red: critical
		See ***Dashboard - Inlet I1*** (on page 89).

❷	**Overcurrent Protectors**	This section is available only when your Legrand PDU contains overcurrent protectors (OCPs).
		
		▪ Overview of each OCP's status
		▪ A current bar per OCP, which changes colors to indicate the RMS current state
		  - green: normal
		  - yellow: warning
		  - red: critical
		See ***Dashboard - OCP*** (on page 90).

❸	**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 91).
❹	**Inlet History**	The chart of the inlet's active power history is displayed by default. You can make it show a different data type. See ***Dashboard - Inlet History*** (on page 92).
❺	**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 93).

Dashboard - Inlet I1

The number of phases shown in the Inlet section is model dependent.

▶ **Link to the Inlet page:**

To view more information or configure the inlet(s), click this section's title 'Inlet I1' to go to the Inlet page. See *Inlet* (on page 98).

Inlet I1			
4.44 kW	L1	L2	L3
5.13 kVA	**7.5** A / 16A	**7.0** A / 16A	**4.9** A / 16A
Active Energy: 0 Wh			
Power Factor: 0.86	L1–L2: 398 V	L2–L3: 399 V	L3–L1: 398 V
Line Frequency: 50.0 Hz	L1-N: 229 V	L2-N: 230 V	L3-N: 230 V
Unbalanced Current: 25 %			
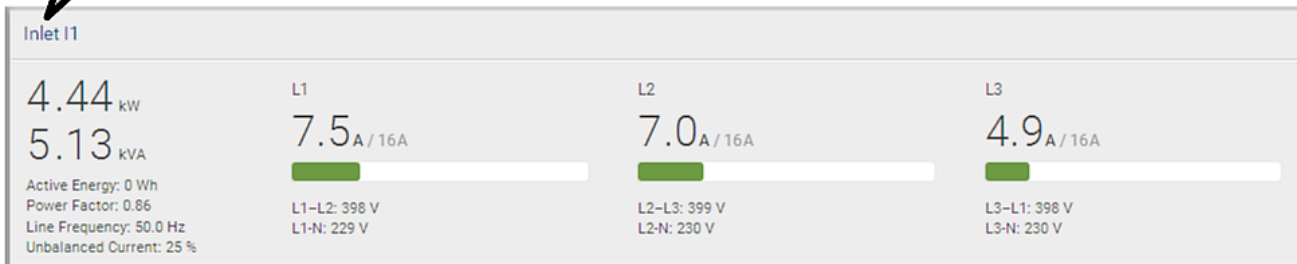
▶ **Left side - generic inlet power data:**

4.44 kW
5.13 kVA

Active Energy: 0 Wh
Power Factor: 0.86
Line Frequency: 50.0 Hz
Unbalanced Current: 25 %
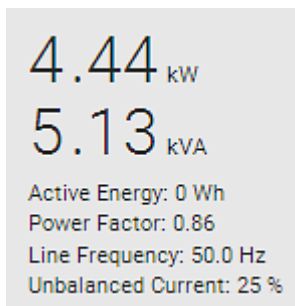
The left side lists all or some of the following data. Available data is model dependent.

- **Active power (kW or W)**
- **Apparent power (kVA or VA)**
- Active energy (kWh or Wh)
- Power factor
- Line frequency (Hz)
- Unbalanced current (%) - *model dependent*

▶ **Right side - inlet's current and voltage:**

L1
7.5 A / 16A

L1–L2: 398 V
L1-N: 229 V
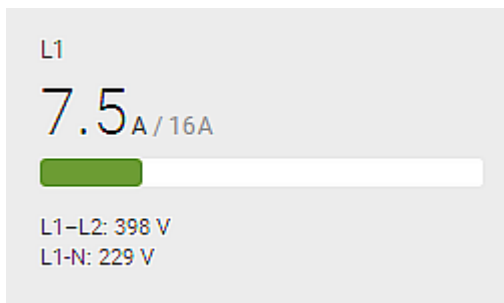
The right side shows the current and voltage data per phase. For a single-phase device, it shows only one line, but for a three-phase device, it shows three lines (L1, L2 and L3).

Inlet data from top to bottom includes:

- RMS current (A) and rated current
  - The smaller, gray text adjacent to RMS current is the rated current.
- A bar showing the RMS current level
- RMS voltage (V)

The RMS current bars automatically change colors to indicate the current status if the thresholds have been enabled. To configure thresholds, see **_Inlet_** (on page 98).

Status	Bar colors
normal	▮
above upper warning	▮
above upper critical	▮

Note: The "below lower warning" and "below lower critical" states also show yellow and red colors respectively. However, it is not meaningful to enable the two thresholds for current levels.

Dashboard - OCP

Availability and total number of OCPs depend on the models.

▶ **Each OCP's link:**

To view more information or configure individual OCPs, click the desired OCP's index number, which is C1, C2 and the like, to go to its setup page.
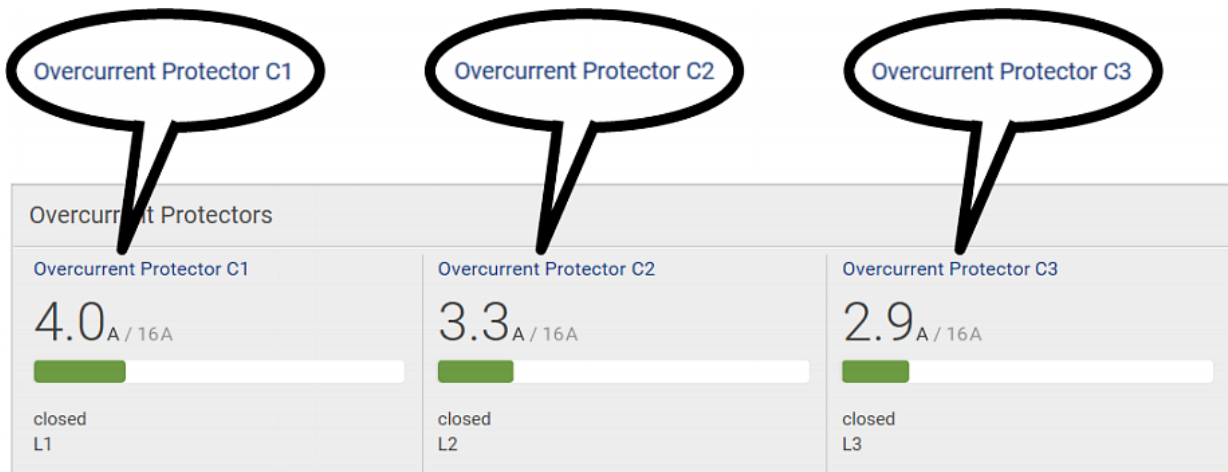
▶ **Each OCP's power data:**

OCP data from top to bottom includes:

- RMS current (A), and rated current
  - Smaller gray text adjacent to RMS current is each OCP's rated current, such as "16A" shown in the above diagram.

- A bar showing OCP current levels
- OCP status -- open or closed
- Associated line pair

The RMS current bars automatically change colors to indicate the current status if OCP thresholds have been enabled. To configure thresholds, see *OCPs* (on page 110).

Status	Bar colors
normal	
above upper warning	
above upper critical	

Note: The "below lower warning" and "below lower critical" states also show yellow and red colors respectively. However, it is not meaningful to enable the two thresholds for current levels.

Dashboard - Alerted Sensors

When any internal sensors or environmental sensor packages connected to the Legrand PDU enter an abnormal state, the Alerted Sensors section in the Dashboard show them for alerting users. This section also lists tripped circuit breakers or blown fuses, if available.

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 125).

If wanted, you can resort the list by clicking the desired column header. See *Sorting a List* (on page 86).

▶   **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.

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 121).

Dashboard - Inlet History

The inlet's power chart helps you observe whether there were abnormal events within the past tens of minutes. The default is to show the inlet's active power data.

You can have it show the chart of other inlet power data. Simply select a different data type by clicking the selector 🔼🔽 below the diagram. Available data types include:

- RMS current
- RMS voltage
- Active power
- Apparent power

June 2018
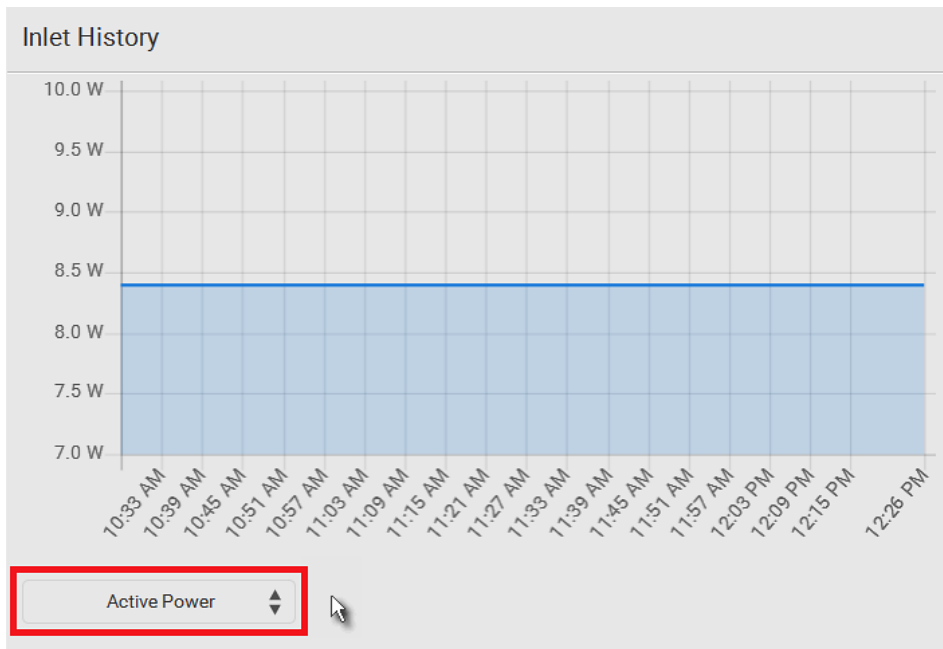
- To retrieve the exact data at a particular time, hover your mouse over the data line in the chart. Both the time and data are displayed as illustrated below.
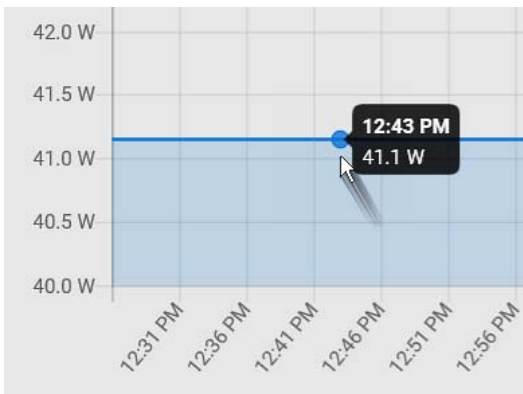
Dashboard - Alarms

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 184).*

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.

Field	Description
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.

Tip: The date and time shown on the Legrand PDU web interface are automatically converted to your computer's time zone. To avoid any time confusion, you can apply the same time zone settings as those of Legrand PDU to your computer.

PDU

The Legrand PDU device's generic information and PDU-level global settings are available on the PDU page.

To open the PDU page, click 'PDU' in the *Menu* (on page 84).

▶ **Device information shown:**

- Firmware version
- Serial number
- MAC address
- Rating

▶ **To configure global settings:**

1. Click Edit Settings.

Settings		
		Edit Settings
Name	My PDU	
Outlet state on device startup	last known	
Outlet initialization delay on device startup	3 s	
Power off period during power cycle	10 s	
Inrush Guard Delay	200 ms	
Peripheral Device Z Coordinate Format	Rack-Units	
Peripheral Device Auto Management	enabled	
Altitude	0 m	
Active Powered Dry Contact Limit	1	
Reset All Active Energy Counters	Reset Active Energy	

2. Now you can configure the fields.

   - Click [⯅⯆] to select an option.
   - Select or deselect the checkbox.
   - Adjust the numeric values.

▪ For time-related fields, if you do not prefer the option selection using [⏶⏷], you can type a value manually which must include a time unit, such as '50 s'. See **Time Units** (on page 98).

*In the following table, those fields marked with * are available on an outlet-switching capable model only.*That is, Legrand Switched PDUs.

Field	Function	Note
Name	Customizes the device name.	
*Outlet state on device startup	Determines the initial power state of ALL outlets after the Legrand PDU powers up. ▪ *Options: on, off, and last known* See **Options for Outlet State on Startup** (on page 96).	▪ After removing power from the PDU, you must wait for a minimum of 10 seconds before powering it up again. Otherwise, the default outlet state settings may not work properly. ▪ You can override the global outlet state setting on a per-outlet basis so specific outlets behave differently on startup. See **Individual Outlet Pages** (on page 107).
*Outlet initialization delay on device startup	Determines how long the Legrand PDU waits before providing power to all outlets during power cycling or after recovering from a temporary power loss. ▪ *Range: 1 second to 1 hour*	See **Initialization Delay Use Cases** (on page 97).
*Power off period during power cycle	Determines the power-off period after the outlet is switched OFF during a power cycle. ▪ *Range: 1 second to 1 hour*	▪ Power cycling the outlet(s) turns the outlet(s) off and then back on. ▪ You can override this global power cycle setting on a per-outlet basis so specific outlets' power-off period is different. See **Individual Outlet Pages** (on page 107).
*Inrush Guard Delay	Prevents a circuit breaker trip due to inrush current when many devices connected to the PDU are turned on. ▪ *Range: 100 milliseconds to 10 seconds*	See **Inrush Current and Inrush Guard Delay** (on page 97).
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 97).	To specify the location of any sensor/actuators in the data center, see **Individual Sensor/Actuator Pages** (on page 125).
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 98).

Field	Function	Note
Altitude	Specifies the altitude of Legrand PDU above sea level when a Raritan's DPX 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 480). ▪ The default altitude measurement unit is meter. See **Setting Default Measurement Units** (on page 137). ▪ You can have the measurement unit vary between meter and foot according to user credentials. See **Setting Your Preferred Measurement Units** (on page 137).
Active Powered Dry Contact Limit	Determines the maximum number of "active" powered dry contact actuators that is permitted. ▪ *Range: 0 to 24*	▪ An "active" actuator is the one that is turned ON. ▪ This setting only applies to "powered dry contact" (PD) actuators rather than normal "dry contact" actuators. ▪ To turn on/off the connected actuators, see **Peripherals** (on page 116).

3. Click Save.

▶ **To reset ALL active energy counters:**

An active energy reading is a value of total accumulated energy, which is never reset, even if the power fails or the Legrand PDU is rebooted. However, you can manually reset this reading to restart the energy accumulation process.

Only users with the "Admin" role assigned can reset active energy readings.

1. Click [Reset Active Energy] .
2. Click Reset on the confirmation message.
    ▪ All active energy readings on this Legrand PDU are reset to zero.

Options for Outlet State on Startup

The following are available options for initial power states of outlets after powering up the Legrand PDU device.

Option	Function
on	Turns on the outlet(s).
off	Turns off the outlet(s).
last known	Restores the outlet(s) to the previous power state(s) before the Legrand PDU was powered off.

If you are configuring an individual outlet on **Individual Outlet Pages** (on page 107), there is one more outlet state option.

Additional option	Function
PDU defined (xxx)	Follows the global outlet state setting, which is set on **PDU** (on page 94). The value xxx in parentheses is the currently-selected global option - *on*, *off*, or *last known*.

Initialization Delay Use Cases

Apply the initialization delay in either of the following scenarios.

- When power may not initially be stable after being restored
- When UPS batteries may be charging

Tip: When there are a large number of outlets, set the value to a smaller number to avoid a long wait before all outlets are available.

Inrush Current and Inrush Guard Delay

▶ **Inrush current:**

When electrical devices are turned on, they can initially draw a very large current known as inrush current. Inrush current typically lasts for 20-40 milliseconds.

▶ **Inrush guard delay:**

The inrush guard delay feature helps prevent a circuit breaker trip due to the combined inrush current of many devices turned on at the same time.

For example, if the inrush guard delay is set to 100 milliseconds and two or more outlets are turned on at the same time, the PDU will sequentially turn the outlets on with a 100 millisecond delay occurring between each one.

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 129).

▶ **To configure Z coordinates:**

1. Determine the Z coordinate format on **PDU** (on page 94). 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.
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 125).

How the Automatic Management Function Works

This setting is configured on **PDU** (on page 94).

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

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

Legrand PDU can manage up to 32 sensors/actuators.

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

Legrand PDU 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 116).

Time Units

If you choose to type a new value in the time-related fields, such as the Inrush Guard Delay field, you must add a time unit after the numeric value. For example, you can type '15 s' for 15 seconds.

Note that different fields have different range of valid values.

▶ **Time units:**

Unit	Time
ms	millisecond(s)
s	second(s)
min	minute(s)
h	hour(s)
d	day(s)

Inlet

You can view all inlet information, configure inlet-related settings, or reset the inlet active energy on the Inlet page. To open this page, click 'Inlet' in the **Menu** (on page 84).

Inlet thresholds, once enabled, help you identify whether the inlet enters the warning or critical level. In addition, you can have Legrand PDU automatically generate alert notifications for any warning or critical status. See **Event Rules and Actions** (on page 184).

▶ **Generic inlet information shown:**

- Inlet power overview, which is the same as **Dashboard - Inlet I1** (on page 89).
- A list of inlet sensors with more details. Number of available inlet sensors depends on the model.
  - Sensors show both readings and states.
  - Sensors in warning or critical states are highlighted in yellow or red.

  See **Yellow- or Red-Highlighted Sensors** (on page 120).

- Inlet's power chart, which is the same as *Dashboard - Inlet History* (on page 92)

▶ **To customize the inlet's name:**

1. Click Edit Settings.

Settings		▲
		Edit Settings
Label	I1	
Name		
Reset Active Energy	Reset Energy	
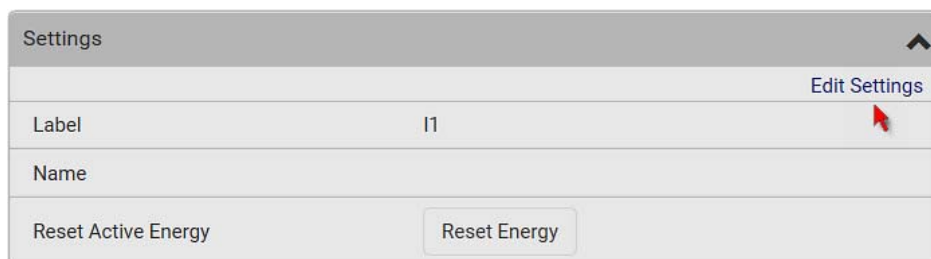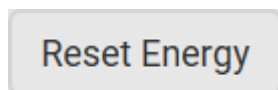
2. Type a name for the inlet.
   - For example, you can name it to identify the power source.
3. Click Save.
4. The inlet's custom name is displayed on the Inlet or Dashboard page, followed by its label in parentheses.

▶ **To reset the inlet's active energy counter:**

Only users with the "Admin" role assigned can reset active energy readings.
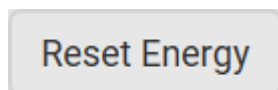
1. Click **Reset Energy**.
2. Click Reset on the confirmation message.

   This inlet's active energy reading is then reset to zero.

▶ **To configure inlet thresholds:**

Per default, there are pre-defined RMS voltage and current threshold values in related fields. See *Default Voltage and Current Thresholds* (on page 479). You can modify them to meet your needs.

1. Click the Thresholds title bar at the bottom of the page to display inlet thresholds.

Thresholds	▼

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

Thresholds				∧
				Edit Thresholds
Sensor ▲	**Lower Critical**	**Lower Warning**	**Upper Warning**	**Upper Critical**
Active Energy	—	---	---	---
Active Power	—	---	---	---
Apparent Power	—	---	---	---
Displacement Power Factor	—	---	---	---
Line Frequency	—	---	---	---
Peak Current	—	---	---	---
Phase Angle	—	---	---	---
Power Factor	—	---	---	---
Reactive Power	—	---	---	---
RMS Current	—	---	7.8 A	9.6 A
RMS Voltage	94 V	97 V	124 V	127 V

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

Lower Critical	✔	94	V
Lower Warning	✔	97	V
Upper Warning	✔	247	V
Upper Critical	✔	254	V
Deassertion Hysteresis		2	V
Assertion Timeout		0	Samples

For concepts of thresholds, deassertion hysteresis and assertion timeout, see ***Sensor Threshold Settings*** (on page 473).

4. Click Save.

Outlets

The Outlets page shows a list of all outlets and the overview of outlet status and data. To open this page, click 'Outlets' in the ***Menu*** (on page 84).

On this page, you can:

- **View all outlets' status.**

  Each outlet's data is displayed, such as receptacle type and outlet lines. On an outlet-switching capable model, each outlet's power state is also shown.

- **Perform actions on all or multiple outlets simultaneously with setup/power-control commands on the top-right corner.**

  Note that only outlet-switching capable models show the power-control buttons, and you must have the Switch Outlet permission to perform outlet-switching operations.

- **Go to an individual outlet's data/setup page by clicking an outlet's name.** See *Individual Outlet Pages* (on page 107).

If wanted, you can resort the list by clicking the desired column header. See *Sorting a List* (on page 86).

▶ **To show or hide specific columns on the outlets overview page:**

1. Click ⊞ to show a list of outlet data types.
2. Select those you want to show, and deselect those you want to hide. See *Available Data of the Outlets Overview Page* (on page 103).

Only Legrand Switched PDUs support all of the following features while Legrand Metered PDUs do NOT support them.

▶ **To configure global outlet settings or perform the load-shedding command:**

1. Click ⋮ to show a list of commands.
2. Select the desired command.

Command	Refer to
Sequence Setup	*Setting Outlet Power-On Sequence and Delay* (on page 104)

Command	Refer to
Load Shedding Setup	**Setting Non-Critical Outlets** (on page 104)
Activate Load Shedding -- OR-- Deactivate Load Shedding	**Load Shedding Mode** (on page 105)

▶ **To power control multiple outlets:**

You can switch any outlet regardless of its current power state. That is, you can turn on any outlet that is already turned on, or turn off any outlet that is already turned off.

1. Click ☑ to make checkboxes appear in front of outlets.

   Tip: To perform the desired action on only one outlet, you can simply click that outlet without making the checkboxes appear.

2. Select multiple outlets.
   - To select ALL outlets, select the topmost checkbox in the header row.

3. Click or select the desired button or command.

Button/command	Action
⏻ On	Power ON.
⏻ Off	Power OFF.
⟳ Cycle	Power cycle. - Power cycling the outlet(s) turns the outlet(s) off and then back on.

4. Confirm the operation on the confirmation message.

   *Tip: You can also power control an outlet from **Individual Outlet Pages** (on page 107).*

5. When performing any outlet-switching operation, a 'Sequence running' message similar to the following displays before the outlet-switching process finishes.
   - It indicates how many selected outlets are NOT switched on/off or cycled yet.

- If needed, click **✖ Cancel** to stop the outlet-switching operation.
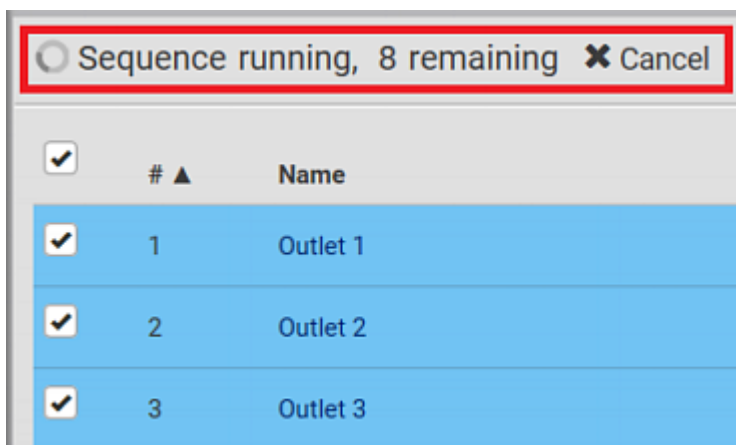
Available Data of the Outlets Overview Page

All of the following outlet data is displayed on the outlets overview page based on your selection.

All or some of the following outlet data is displayed on the outlets overview page based on your model and

selection. To show or hide specific data, click [icon]. See **Outlets** (on page 100).

- Outlet status, which is marked with either icon below. This information is available on outlet-switching capable models only.

Icon	Outlet status
⏻	Outlet turned on
⏻	Outlet turned off

- Non-critical setting for indicating whether the outlet is a non-critical outlet. This information is available on outlet-switching capable models only.

Non-critical setting	Description
true	The outlet is a non-critical outlet, which will be turned OFF in the load shedding mode. See **Load Shedding Mode** (on page 105).
false	The outlet is a critical outlet, which will remain unchanged in the load shedding mode.

Note: To set critical and non-critical outlets, go to **Outlets** *(on page 100).*

- Receptacle type
- Lines associated with each outlet

Setting Outlet Power-On Sequence and Delay

By default, outlets are sequentially powered on in the ascending order from outlet 1 to the final when turning ON or power cycling all outlets on the Legrand PDU. You can change the order in which the outlets power ON. This is useful when there is a specific order in which some IT equipment should be powered up first.

In addition, you can make a delay occur between two outlets that are turned on consecutively. For example, if the power-on sequence is Outlet 1 through Outlet 8, and you want the Legrand PDU to wait for 5 seconds before turning on Outlet 4, after Outlet 3 is turned on, assign a delay of 5 seconds to Outlet 3.

▶ **To set the outlet power-on sequence:**

1. On the Outlets page, click ⋮ > Sequence Setup.
2. Select one or multiple outlets by clicking them one by one in the 'Outlet' column.
3. Click the arrow buttons to change the outlet positions.

Button	Function
⯭	Top
↑	Up
↓	Down
⯯	Bottom
⟳	Restores to the default sequence

Next time when power cycling the Legrand PDU, it will turn on all outlets based on the new outlet order.

The new order also applies when performing the power-on or power-cycling operation on partial outlets.

▶ **To set a power-on delay for any outlet:**

1. On the same outlets list, click the 'Delay' column of the outlet that requires a wait after it is turned on.
2. Type a new value in seconds.
3. Click Save.

Legrand PDU will insert a power-on delay between the configured outlet and the one following it during the power-on process.

Setting Non-Critical Outlets

Outlets that are turned off when load shedding is activated are called non-critical outlets. Outlets that are not affected by load shedding are called critical outlets. See *Load Shedding Mode* (on page 105).

Per default, all outlets are configured as critical.

▶ **To determine critical and non-critical outlets:**

1. On the Outlets page, click ⋮ > Load Shedding Setup.
2. To set non-critical outlets, select the checkboxes of those you want.

■ To select ALL outlets, select the topmost checkbox in the header row.

Load Shedding

☑ Non Critical	Outlets ▲
☐	Outlet 1
☐	Outlet 2
☐	Outlet 3
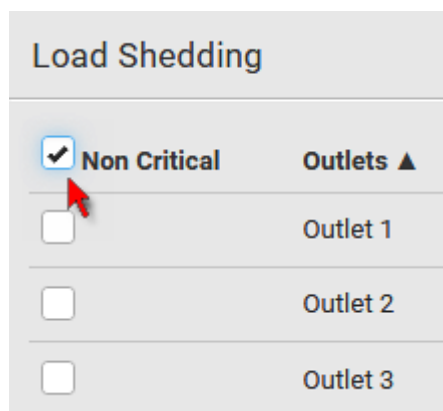
3. To turn non-critical outlets into critical ones, deselect their checkboxes.

■ To deselect ALL outlets, deselect the topmost checkbox in the header row.

4. Click Save.

Tip: You can also set up non-critical outlet setting by configuring outlets one by one. See **Individual Outlet Pages** *(on page 107).*

Load Shedding Mode

When a UPS supplying power to Legrand PDU switches into battery backup operation, it may be desirable to switch off non-critical outlets to conserve UPS battery life. This feature is known as load shedding.

Outlets that are turned off when load shedding is activated are called non-critical outlets. Outlets that are not affected by load shedding are called critical outlets. By default, all outlets are critical. To set non-critical ones, see ***Setting Non-Critical Outlets*** (on page 104).

When load shedding is activated, the Legrand PDU turns off all non-critical outlets. When load shedding is deactivated, the Legrand PDU turns back on all non-critical outlets that were ON before entering the load shedding mode.

Exception: If you once manually perform switch-off operation on any non-critical outlets during the load shedding mode, those outlets will NOT be turned back on when exiting the load shedding mode.

Activation of load shedding can be accomplished using the web interface, SNMP or CLI, or triggered by the contact closure sensors.

Tip: It is better to check non-critical outlets prior to manually entering the load shedding mode. The non-critical information can be retrieved from the Outlets page. See **Outlets** *(on page 100) or* **Available Data of the Outlets Overview Page** *(on page 103).*

You must have the following two permissions to perform the load shedding commands.

- 'Change Pdu, Inlet, Outlet & Overcurrent Protector Configuration'
- 'Switch Outlet' permission for all **non-critical** outlets

▶ **To enter the load shedding mode:**

1. On the Outlets page, click ⋮ > Activate Load Shedding.

   Note: In case Legrand PDU prevents you from performing this command, check your permissions, especially whether you have the Switch Outlet permission for ALL non-critical outlets.

2. Click Activate on the confirmation message.

   In the load shedding mode:

   ■ You CANNOT power on any "non-critical" outlets.

- The lock icon 🔒 appears for "non-critical" outlets that WILL be automatically powered on when deactivating the load shedding mode.

- The off icon ⏻ appears for outlets, critical or non-critical, that WILL NOT be automatically powered on when deactivating the load shedding mode.

*Tip: The above two icons are switched if you manually perform any power operations on non-critical outlets during the load shedding mode. See **Off and Lock Icons for Outlets** (on page 106).*

- The message "Load Shedding Active" appears next to the 'Outlets' title.
- The Non Critical column, if not shown prior to the load shedding mode, automatically displays on the Outlets page.

# ▲	Name	Status	Non Critical	Receptacle Type	Lines	
1	Outlet 1	🔒 off	true	NEMA 5-20R	L1−NEUTRAL	
2	Outlet 2	🔒 off	true	NEMA 5-20R	L1−NEUTRAL	
3	Outlet 3	⏻ on	false	NEMA 5-20R	L1−NEUTRAL	
4	Outlet 4	⏻ off	true	NEMA 5-20R	L1−NEUTRAL	
5	Outlet 5	⏻ on	false	NEMA 5-20R	L1−NEUTRAL	
6	Outlet 6	⏻ on	false	NEMA 5-20R	L1−NEUTRAL	

*Tip: To make the Non Critical column appear when the load shedding mode is not activated yet. See **Outlets** (on page 100) or **Available Data of the Outlets Overview Page** (on page 103).*

▶ **To exit from the load shedding mode:**

1. On the Outlets page, click ⋮ > Deactivate Load Shedding.
2. Click Deactivate on the confirmation message.

Now you can turn on/off any outlets.

▶ **TIP -- automatic load shedding via contact closure sensors:**

If you have connected a Raritan contact closure sensor to Legrand PDU, you can set up an event rule in a manner that this sensor's status change automatically activates or deactivates the load shedding mode. For an example, see *Sample Environmental-Sensor-Level Event Rule* (on page 216).

Off and Lock Icons for Outlets

This section further explains the following two icons for outlets, which display in the load shedding mode.

- Lock icon 🔒 : It means the outlet WILL be automatically powered on after deactivating the load shedding mode.

- Off icon ⏻ : It means the outlet WILL NOT be automatically powered on when deactivating the load shedding mode.

▶ **Which outlets show the lock icon 🔒:**

- Non-critical outlets that were powered ON prior to the load shedding mode
- Non-critical outlets that you manually switch on during the load shedding mode

Note: The switching-on operation does not power on the selected non-critical outlets while the load shedding mode is active, but will cause those outlets to be automatically turn on after disabling the load shedding mode.

June 2018

▶ **Which outlets show the Off icon** ⏻ :

- Any outlets, critical or non-critical, that were powered OFF prior to the load shedding mode
- Any outlets, critical or non-critical, that you manually switch off during the load shedding mode

Individual Outlet Pages

An outlet's data/setup page is opened after clicking the outlet's name on the Outlets overview page. See ***Outlets*** (on page 100).

The individual outlet's page shows this outlet's detailed information. See ***Detailed Information on Outlet Pages*** (on page 109).

In addition, you can perform the following operations on this outlet page. Note that only outlet-switching capable models show the power-control buttons, and you must have the Switch Outlet permission to perform outlet-switching operations. Therefore, only Legrand Switched PDUs support the following power-control operation.

▶ **To power control this outlet:**

1. Click one of the power-control buttons.

Button/command	Action
⏻ On	Power ON.
⏻ Off	Power OFF.
↻ Cycle	Power cycle. ▪ Power cycling the outlet(s) turns the outlet(s) off and then back on.

2. Confirm it on the confirmation message.

▶ **To configure this outlet:**

1. Click Edit Settings.

Settings	
	Edit Settings
Name	
State on device startup	PDU defined (last known)
Power off period during power cycle	PDU defined (10 seconds)
Non-critical	False

2. Configure available fields. Note that the fields marked with * are only available on outlet-switching capable models.

Field	Description
Name	Type an outlet name up to 64 characters long.
*State on device startup	Click this field to select this outlet's initial power state after Legrand PDU powers up. ▪ Options: *on*, *off*, *last known* and *PDU defined*. See **Options for Outlet State on Startup** (on page 96). ▪ Note that any option other than "PDU defined" will override the global outlet state setting on this particular outlet.
*Power off period during power cycle	Select an option to determine how long this outlet is turned off before turning back on. ▪ Options: *PDU defined* or customized time. See **Power-Off Period Options for Individual Outlets** (on page 110). ▪ Note that any time setting other than "PDU defined" will override the global power-off period setting on this particular outlet.
*Non-critical	Select this checkbox only when you want this outlet to turn off in the load shedding mode. See **Load Shedding Mode** (on page 105).

3. Click Save.

4. The outlet's custom name, if available, is displayed in the outlets list, following by its label in parentheses.

▶ **Other operations:**

- You can go to another outlet's data/setup page by clicking the outlet selector [⬍] on the top-left corner.
- You can go to the associated Inlet's or overcurrent protector's data pages by clicking the Inlet or Overcurrent Protector links in the Details section.
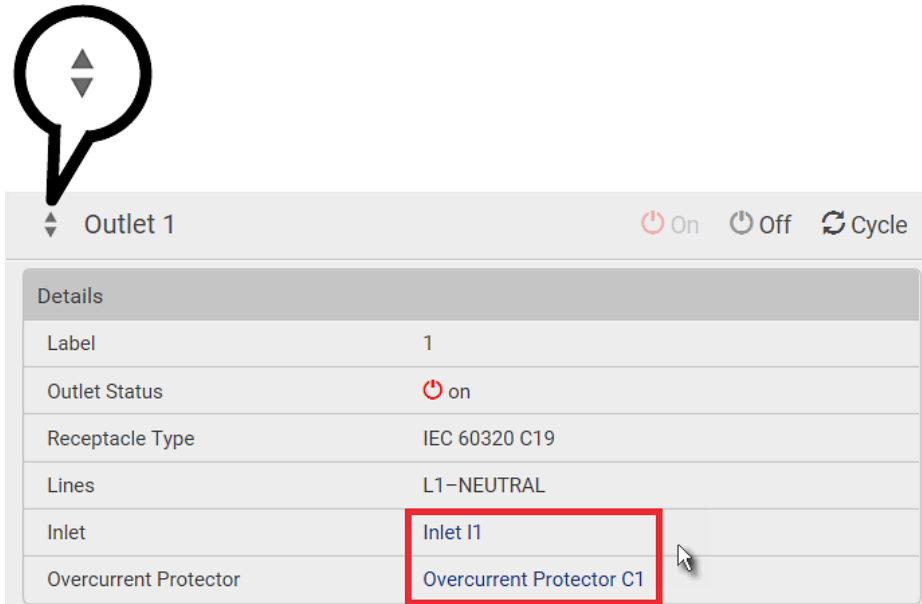
Detailed Information on Outlet Pages

Each outlet's data page has the Details section for showing general outlet information.

▶ **Details section:**

Field	Description
Label	The physical outlet number
Outlet Status	This information is only available on outlet-switching capable models.
	On or Off
Receptacle Type	This outlet's receptacle type
Lines	Lines associated with this outlet
Inlet	Inlet associated with this outlet
Overcurrent Protector	This information is available only when your Legrand PDU has overcurrent protectors.
	Overcurrent protector associated with this outlet

Power-Off Period Options for Individual Outlets

There are two options for setting the power-off period during the power cycle on each individual outlet's page. See **Individual Outlet Pages** (on page 107).

Option	Function
PDU defined (xxx)	Follows the global power-off period setting, which is set on **PDU** (on page 94). The value xxx in parentheses is the current global value.
Customized time	If selecting this option, do either of the following: ▪ Click [▲▼] to select an existing time option. ▪ Type a new value *with an appropriate time unit added*. See **Time Units** (on page 98).

OCPs
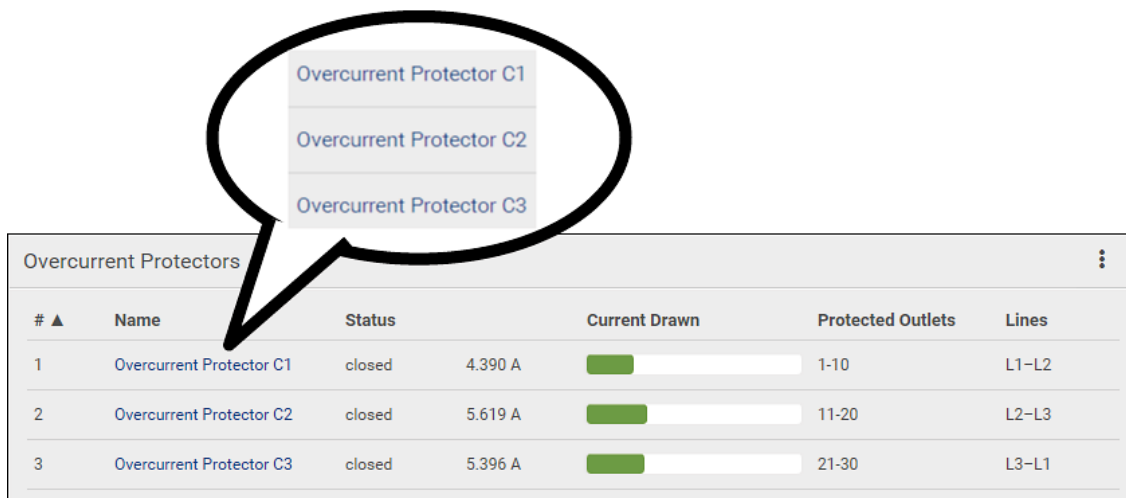
The OCPs page is available only when your Legrand PDU has overcurrent protectors, such as circuit breakers.

The OCPs page lists all overcurrent protectors as well as their status. If any OCP trips or its current level enters the alarmed state, it is highlighted in red or yellow. See **Yellow- or Red-Highlighted Sensors** (on page 120).

To open the OCPs page, click 'OCPs' in the **Menu** (on page 84).

You can go to each OCP's data/setup page by clicking its name on this page.

If wanted, you can resort the list by clicking the desired column header. See **Sorting a List** (on page 86).

► **Overcurrent protector overview:**

• OCP status - open (tripped) or closed
• Current drawn and current bar

The RMS current bars change colors to indicate the status if the OCP thresholds have been configured and enabled.

Status	Bar colors
normal	
above upper warning	
above upper critical	

Note: The "below lower warning" and "below lower critical" states also show yellow and red colors respectively. However, it is not meaningful to enable the two thresholds for current levels.

- Protected outlets, which are indicated with outlet numbers
- Associated lines

▶ **To configure current thresholds for multiple overcurrent protectors:**

OCP thresholds, when enabled, help you identify the OCP whose RMS current enters the warning or critical level with the yellow or red color. In addition, you can have Legrand PDU automatically generate alert notifications for any warning or critical status. See ***Event Rules and Actions*** (on page 184).

Note: By default, upper thresholds of an OCP's RMS current have been configured. See **Default Voltage and Current Thresholds** *(on page 479). You can modify them as needed.*

1. Click ⋮ > Threshold Bulk Setup.
2. Select one or multiple OCPs.
   - To select all OCPs, simply click the topmost checkbox in the header row.

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

June 2018

For concepts of thresholds, deassertion hysteresis and assertion timeout, see ***Sensor Threshold Settings*** (on page 473).

5. Click Save.

Individual OCP Pages

An OCP's data/setup page is opened after clicking any OCP's name on the OCPs or Dashboard page. See ***OCPs*** (on page 110) or ***Dashboard*** (on page 87).

▶ **General OCP information:**

Field	Description
Label	This OCP's physical number.
Status	open or closed.
Type	This OCP's type.
Rating	This OCP's rated current.
Lines	Lines associated with this OCP.
Protected Outlets	Outlets associated with this OCP.
Inlet	Inlet associated with this OCP. This information is useful only when your PDU has multiple inlets.
RMS current	This OCP's current state and readings, including current drawn and current remaining.

▶ **To customize this OCP's name:**

1. Click Edit Settings.
2. Type a name.
3. Click Save.

▶ **To view this OCP's RMS current chart:**

This OCP's data chart is shown in the Overcurrent Protector History section.
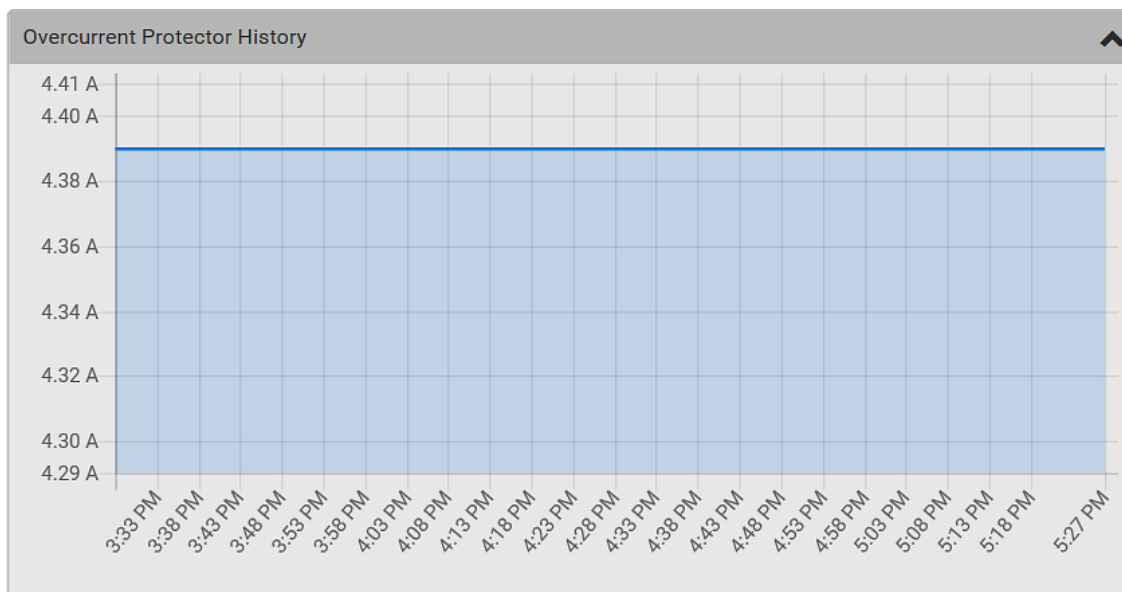
- To retrieve the exact data at a particular time, hover your mouse over the data line in the chart. Both the time and data are displayed as illustrated below.
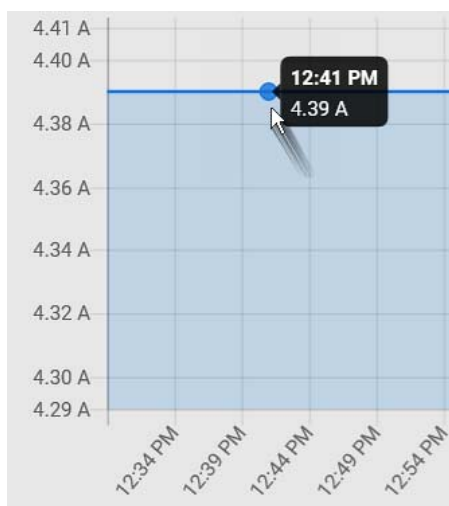
▶ **To configure this OCP's threshold settings:**

By default, upper thresholds of an OCP's RMS current have been configured. See *Default Voltage and Current Thresholds* (on page 479). You can modify them as needed.

Note: The threshold values set for an individual OCP will override the bulk threshold values stored on that particular OCP. To configure thresholds for multiple OCPs at a time, see **OCPs** *(on page 110).*

1. Click the Thresholds title bar at the bottom of the page to display the threshold data.

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

Thresholds				^
				Edit Thresholds
Sensor ▲	Lower Critical	Lower Warning	Upper Warning	Upper Critical
RMS Current	---	---	10.4 A	12.8 A

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

Lower Critical	☐	0	A
Lower Warning	☐	0	A
Upper Warning	☑	10.4	A
Upper Critical	☑	12.8	A
Deassertion Hysteresis		1	A
Assertion Timeout		0	Samples

For concepts of thresholds, deassertion hysteresis and assertion timeout, see **Sensor Threshold Settings** (on page 473).

4. Click Save.

► **Other operations:**

- You can go to another OCP's data/setup page by clicking the OCP selector ⬍ on the top-left corner.
- You can go to the associated Inlet's data page by clicking the Inlet link in the Details section.

⬍ Overcurrent Protector C1	
Details	
Label	C1
Status	closed
Type	1-Pole Circuit Breaker
Rating	16 A
Lines	L1
Protected Outlets	1-4
Inlet	Inlet I1

Peripherals

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

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

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

Legrand PDU 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 121).

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

One Legrand PDU can manage a maximum of 32 sensors/actuators.

*Note: To disable the automatic management function, go to **PDU** (on page 94). You need to manually manage a sensor/actuator only when it is not under management.*

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

Open the Peripherals page by clicking Peripherals in the *Menu* (on page 84). Then you can:

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

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

If wanted, you can resort the list by clicking the desired column header. See **Sorting a List** (on page 86).

▶ **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 120). An actuator is never highlighted.

Column	Description
Name	By default the Legrand PDU 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 125).
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 121).
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 122).
Position	The data indicates where this sensor or actuator is located in the sensor chain. See **Identifying the Sensor Position and Channel** (on page 123).
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 (32), 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 124). 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 121).
   - ▪ 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 (QLLemu0001) ⬍

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 124).
4. Now released sensors/actuators become "unmanaged."

Managed ones show one of the managed states.

▶ **To configure default threshold settings:**

Note that any changes made to default threshold settings not only re-determine the initial threshold values 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 125).

1. Click ⋮ > Default Threshold Setup.

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

Peripherals Default Thresholds

Edit Thresholds

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

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

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 473).

4. Click Save.

Tip: To customize the threshold settings on a per-sensor basis, go to **Individual Sensor/Actuator Pages** *(on page 125).*

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

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

   - To select multiple actuators, click 🗹 to make checkboxes appear and then select desired actuators.

2. Click the desired button.

   ⏻ On : Turn ON.

   ⏻ Off : Turn OFF.

*Note: Per default you can turn on as many dry contact actuators as possible, 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 **PDU** (on page 94).*

3. Confirm the operation when prompted.

*Tip: If intending to control the actuator via the front panel, see **Front Panel Settings** (on page 224).*

Yellow- or Red-Highlighted Sensors

The Legrand PDU 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 473).

# ▲	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 121).
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.
OCP alarm		Open	▪ Circuit breaker trips. -- OR -- ▪ Fuse blown.

Managed vs Unmanaged Sensors/Actuators

To manually manage or unmanage/release a sensor or actuator, see **Peripherals** (on page 116).

▶ **Managed sensors/actuators:**

- Legrand PDU 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 121).
- 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:**

- Legrand PDU 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 Legrand PDU. 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 120).

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

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

Note that for a contact closure sensor, the normal state depends on the normal setting you have configured. Refer to the Environmental Sensors 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	▪ The communication with the managed actuator is lost. -- OR -- ▪ DX sensor packages are upgrading their sensor firmware.

▶ **Unmanaged sensor/actuator states:**

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

Note: Unmanaged sensors or actuators will disappear from the web interface after they are no longer physically connected to the Legrand PDU. To manage a sensor/actuator, go to **Peripherals** *(on page 116).*

Finding the Sensor's Serial Number

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

A DPX2, DPX3, DX or DX2 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 Legrand PDU. Match the serial number from the tag to those listed in the sensor table.

Peripheral Devices							On Off ☑
# ▲	Name	Reading	State	Type	Serial Number	Position	Actuator
1	On/Off 1		normal	Contact Closure	QLLemu0001	Port 1, Chain Position 1, Channel 1	
2	On/Off 2		normal	Contact Closure	QLLemu0001	Port 1, Chain Position 1, Channel 3	
3	Temperature 1	24.0 °C	normal	Temperature	QMTemu0005	Port 1, Chain Position 5	
4	Absolute Humidity 1	9.2 g/m³	normal	Absolute Humidity	QMSemu0004	Port 1, Chain Position 4	
5	Relative Humidity 1	42 %	normal	Humidity	QMSemu0004	Port 1, Chain Position 4	

Identifying the Sensor Position and Channel

Raritan has developed five types of environmental sensor packages - DPX, DPX2, DPX3, DX and DX2 series. Only DPX2, DPX3, DX and DX2 sensor packages can be daisy chained.

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

Peripheral Devices							On Off ☑
# ▲	Name	Reading	State	Type	Serial Number	Position	Actuator
1	On/Off 1		normal	Contact Closure	QLLemu0001	Port 1, Chain Position 1, Channel 1	
2	On/Off 2		normal	Contact Closure	QLLemu0001	Port 1, Chain Position 1, Channel 3	
3	Temperature 1	24.0 °C	normal	Temperature	QMTemu0005	Port 1, Chain Position 5	
4	Absolute Humidity 1	9.2 g/m³	normal	Absolute Humidity	QMSemu0004	Port 1, Chain Position 4	
5	Relative Humidity 1	42 %	normal	Humidity	QMSemu0004	Port 1, Chain Position 4	

- DPX series shows the sensor port number only.

    For example, *Port 1*.

- DPX2, DPX3, 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 DPX2, DPX3, DX and DX2 series, but NOT indicated for DPX series.

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

Managing One Sensor or Actuator

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

Tip: When the total of managed sensors/actuators reaches the maximum value (32), 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 116).*

▶ **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 (QLLemu0001) ▲▼

Cancel   Manage

- To let Legrand PDU 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.

# ▲	Name	Reading	State	Type	Serial Number	Position
1	On/Off 1		normal	Contact Closure	QLLemu0001	Port 1, Chain Position 1, Channel 1
2	On/Off 2		normal	Contact Closure	QLLemu0001	Port 1, Chain Position 1, Channel 3
3	Relative Humidity 1	42 %	normal	Humidity	QMSemu0004	Port 1, Chain Position 4
4	Absolute Humidity 1	9.2 g/m³	normal	Absolute Humidity	QMSemu0004	Port 1, Chain Position 4
5	Temperature 1	24.0 °C	normal	Temperature	QMSemu0004	Port 1, Chain Position 4

Peripheral Devices — ⏻ On

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 116).

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 120). In addition, you can have Legrand PDU automatically generate alert notifications for any warning or critical status. See *Event Rules and Actions* (on page 184).

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

1. Click Edit Thresholds.

Sensor	
	Edit Thresholds
Reading	23.3 °C
State	normal
Last Time Changed	7/26/2017, 10:13:00 AM Eastern Daylight Time

Tip: The date and time shown on the Legrand PDU web interface are automatically converted to your computer's time zone. To avoid any time confusion, you can apply the same time zone settings as those of Legrand PDU to your computer.

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

Sensor			
			Edit Thresholds
Use Default Thresholds	✔		
Lower Critical	✔	10	°C
Lower Warning	✔	15	°C
Upper Warning	✔	57	°C
Upper Critical	✔	68	°C
Deassertion Hysteresis		1	°C
Assertion Timeout		0	Samples
		✖ Cancel	✔ Save

- 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 116).

- 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 473).*

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
Binary Sensor Subtype	This field is available for a contact closure sensor only.
	Determine the sensor type of your contact closure detector. ▪ *Contact Closure* detects the door lock or door open/closed status. ▪ *Smoke Detection* detects the appearance of smoke. ▪ *Water Detection* detects the appearance of water on the floor. ▪ *Vibration* detects the vibration of the floor.
Name	A name for the sensor or actuator.
Description	Any descriptive text you want.
Location (X, Y and Z)	Describe the sensor's or actuator's location in the data center by typing alphanumeric values for the X, Y and Z coordinates. See ***Sensor/Actuator Location Example*** (on page 129).
	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 ***PDU*** (on page 94).
Alarmed to Normal Delay	This field is available for the DX-PIR presence detector only.
	It determines the wait time before the Legrand PDU announces that the presence detector is back to normal after it already returns to normal. Adjust the value in seconds.

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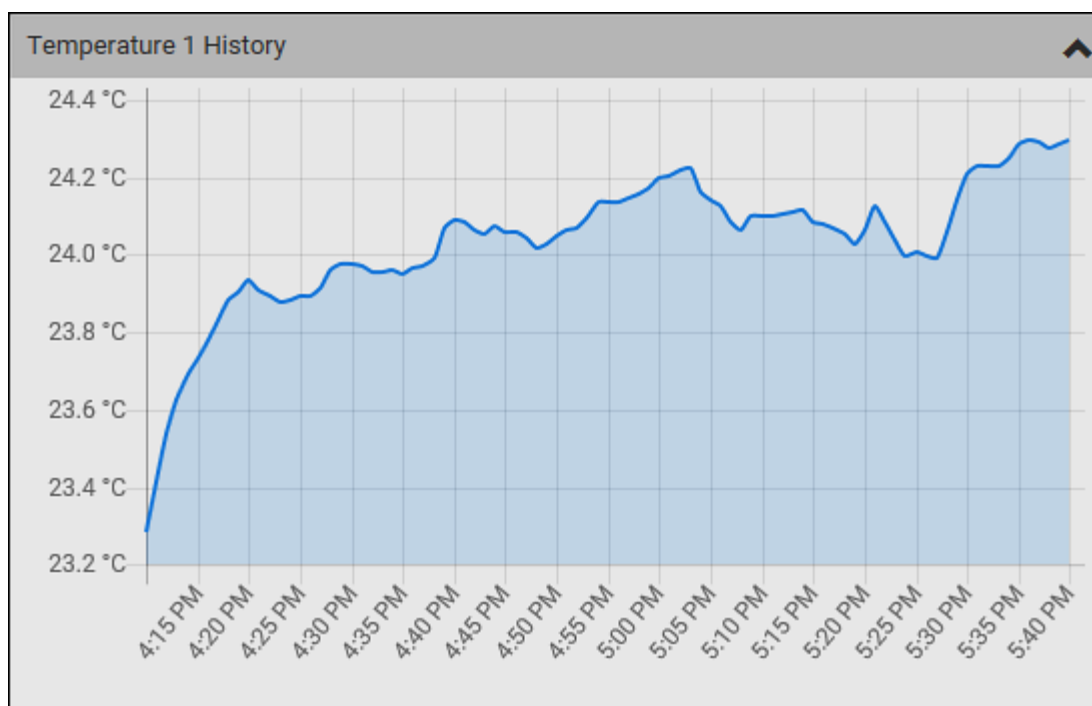
- To retrieve the exact data at a particular time, hover your mouse over the data line in the chart. Both the time and data are displayed as illustrated below.
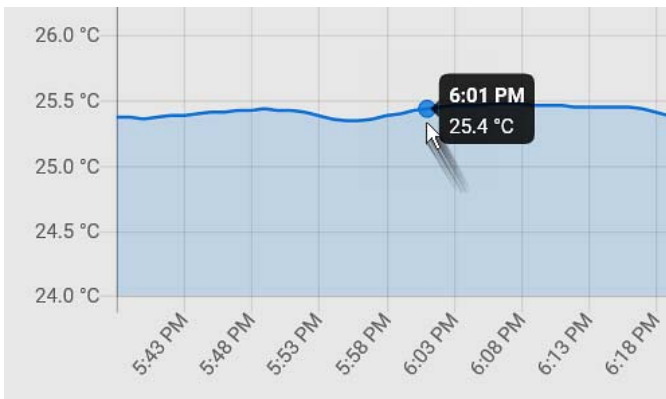
▶ **To turn on or off an actuator:**

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 possible, 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 **PDU** (on page 94).*

▶ **Other operations:**

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

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

Sensor/Actuator Location Example

Use the X, Y and Z coordinates to describe each sensor's or actuator's physical location in the data center. See ***Individual Sensor/Actuator Pages*** (on page 125).

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 ***PDU*** (on page 94).

June 2018

User Management

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

Legrand PDU 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 Legrand PDU so you must assign one or multiple roles to each user.

Click 'User Management' in the **Menu** (on page 84), and the following submenu displays.
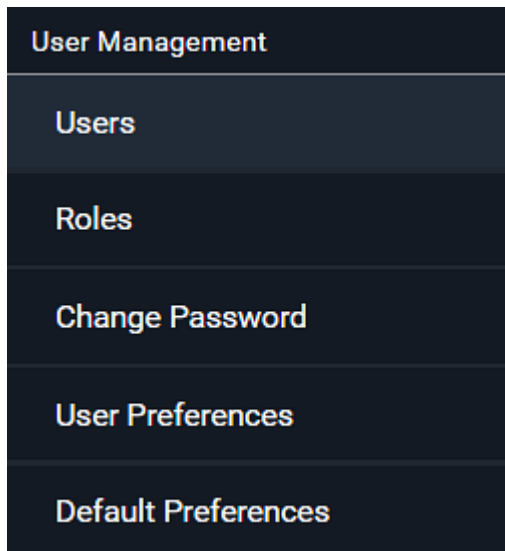
Submenu command	Refer to...
Users	**Creating Users** (on page 130)
Roles	**Creating Roles** (on page 135)
Change Password	**Changing Your Password** (on page 81)
User Preferences	**Setting Your Preferred Measurement Units** (on page 137)
Default Preferences	**Setting Default Measurement Units** (on page 137)

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 > .

Users			
Enabled ▲	User name	Full Name	Roles
✔	admin	Administrator	Admin
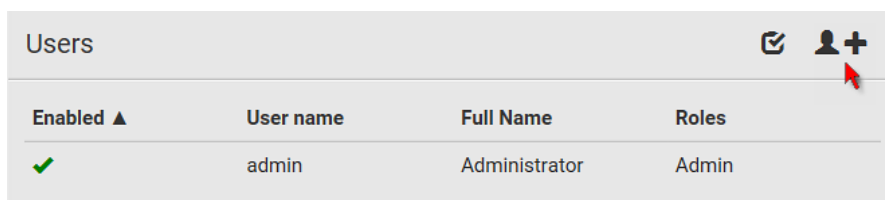
Note that you must enter information in the fields showing the message 'required.'

required

▶ **User information:**

Field/setting	Description
User Name	The name the user enters to log in to the Legrand PDU. ▪ 4 to 32 characters ▪ Case sensitive ▪ Spaces are NOT permitted.
Full Name	The user's first and last names.
Password, Confirm Password	▪ 4 to 64 characters ▪ Case sensitive ▪ Spaces are permitted.
Telephone Number	The user's telephone number
eMail Address	The user's email address ▪ Up to 128 characters ▪ Case sensitive
Enable	When selected, the user can log in to the Legrand PDU.
Force password change on next login	When selected, a password change request automatically appears when next time the user logs in. For details, see **Changing Your Password** (on page 81).

▶ **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 162).

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 160).*
Security Level	Click the field to select a preferred security level from the list: ▪ None: No authentication and no privacy. This

Field/setting	Description
	is the default.
	▪ Authentication: Authentication and no privacy.
	▪ Authentication & Privacy: Authentication and privacy.

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

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

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

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

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

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

▶ **Preferences:**

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

Field	Description
Temperature Unit	Preferred units for temperatures -- °C (Celsius) or °F (Fahrenheit).

Field	Description
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 137).*

▶ **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 ▮+ New Role. This newly-created role will be then automatically assigned to the user account currently being created. See ***Creating Roles*** (on page 135).

Built-in role	Description
Admin	Provide full permissions.
Operator	Provide frequently-used permissions, including: • Acknowledge Alarms • Change Own Password • Change Pdu, Inlet, Outlet & Overcurrent Protector Configuration • Switch Outlet (if your Legrand PDU is outlet-switching capable) • 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.

Enabled	User name ▲	Full Name	Roles
✔	admin	Administrator	Admin
✖	John		Operator
✔	Mary		Operator
✔	Teresa		Admin

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 86).

▶ **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 130).
   - 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.

Edit User - John	🗑
User	
User Name	John
Full Name	
Password	

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 🗑.

Users		☑ 👤+ 🗑
☐ **Enabled**	**User name ▲**	**Full Name**	**Roles**
☐ ✔	admin	Administrator	Admin
☑ ✖	John		Operator
☐ ✔	Mary		Operator
☐ ✔	Teresa		Admin

4. Click Delete on the confirmation message.

Creating Roles

A role is a combination of permissions. Each user must have at least one role.
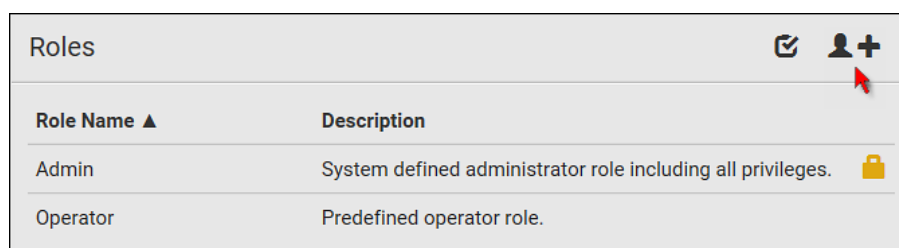
The Legrand PDU provides two built-in roles.

Built-in role	Description
Admin	Provide full permissions.
Operator	Provide frequently-used permissions, including: • Acknowledge Alarms • Change Own Password • Change Pdu, Inlet, Outlet & Overcurrent Protector Configuration • Switch Outlet (if your Legrand PDU is outlet-switching capable) • View Event Settings • View Local Event Log

If the two do not satisfy your needs, add new roles. Legrand PDU supports up to 64 roles.

▸ **To create a role:**

1. Choose User Management > Roles > 👤➕.

Roles	☑ 👤➕
Role Name ▲	**Description**
Admin	System defined administrator role including all privileges. 🔒
Operator	Predefined operator role.

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 ⌄ 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, on an outlet-switching capable model, you can specify the outlets that users can switch on/off as shown below. To select all outlets, select the 'All Outlets' checkbox instead.

☐ Switch Outlet	2-4 and 7	⌃
☐ All Outlets	☐ Outlet 5	
☐ Outlet 1	☐ Outlet 6	
☑ Outlet 2	☑ Outlet 7	
☑ Outlet 3	☐ Outlet 8	
☑ Outlet 4		

6. Click Save.

Now you can assign the role to any user. See *Creating Users* (on page 130) or *Editing or Deleting Users* (on page 133).

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 86).

Roles	☑ ☍+
Role Name ▲	**Description**
Admin	System defined administrator role including all privileges. 🔒
Manager	Able to change all settings except for security settings
Operator	Predefined operator role.

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.

Edit Role - Manager	🗑
Settings	
Role Name	Manager
Description	Able to change all settings except for security settings

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 🗑 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 Legrand PDU 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 133).*

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 137).

▶ **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 -- °C (Celsius) or °F (Fahrenheit).
Length Unit	Preferred units for length or height -- Meter or Feet.
Pressure Unit	Preferred units for pressure -- Pascal or Psi. • Pascal = one newton per square meter • Psi = pounds per square inch

3. Click Save.

Setting Default Measurement Units

Default measurement units are applied to all Legrand PDU user interfaces across all users, including users accessing the Legrand PDU via external authentication servers.

For a list of affected user interfaces, see *User Interfaces Showing Default Units* (on page 138). 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 137) or* **Creating Users** *(on page 130).*

▶ **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 130).
- 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 201).
- Front panel LCD display.

Device Settings

Click 'Device Settings' in the **Menu** (on page 84), and the following submenu displays.

Menu command	Submenu command	Refer to...
Network		**Configuring Network Settings** (on page 140)
Network Services	HTTP	**Changing HTTP(S) Settings** (on page 158)
	SNMP	**Configuring SNMP Settings** (on page 160)
	SMTP Server	**Configuring SMTP Settings** (on page 161)
	SSH	**Changing SSH Settings** (on page 162)
	Telnet	**Changing Telnet Settings** (on page 163)
	Modbus	**Changing Modbus Settings** (on page 163)
	Server Advertising	**Enabling Service Advertising** (on page 164)
Security	IP Access Control	**Creating IP Access Control Rules** (on page 165)

Menu command	Submenu command	Refer to...
	Role Based Access Control	**Creating Role Based Access Control Rules** (on page 168)
	SSL Certificate	**Setting Up an SSL/TLS Certificate** (on page 170)
	Authentication	**Setting Up External Authentication** (on page 173)
	Login Settings	**Configuring Login Settings** (on page 179)
	Password Policy	**Configuring Password Policy** (on page 180)
	Service Agreement	**Enabling the Restricted Service Agreement** (on page 181)
Date/Time		**Setting the Date and Time** (on page 182)
Event Rules		**Event Rules and Actions** (on page 184)
Data Logging		**Setting Data Logging** (on page 219)
Data Push		**Configuring Data Push Settings** (on page 220)
Server Reachability		**Monitoring Server Accessibility** (on page 221)
Front Panel		**Front Panel Settings** (on page 224)
Serial Port		**Configuring the Serial Port** (on page 224)
Lua Scripts		**Lua Scripts** (on page 225)
Miscellaneous		**Miscellaneous** (on page 229)

Configuring Network Settings

Configure wired, wireless, and Internet protocol-related settings on the Network page after **connecting the Legrand PDU to your network** (on page 23).

You can enable both the wired and wireless networking on Legrand PDU 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 Legrand PDU enters the port forwarding mode so that Legrand PDU has more than one IPv4 or IPv6 address in the port forwarding mode.

However, Legrand PDU 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 142).
   - 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 150) and **Static Route Examples** (on page 148).
3. To configure IPv4/IPv6 settings for a *wired* network, click the ETH1, ETH2 or BRIDGE section. See **Wired Network Settings** (on page 141).

- 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 144).

- You must connect a USB wireless LAN adapter to the Legrand PDU 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 143).
6. Click Save.

▶ **After enabling either or both Internet protocols:**

After enabling IPv4 and/or IPv6, all but not limited to the following protocols will be compliant with the selected Internet protocol(s):

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

Note: The Legrand PDU supports TLS 1.0, 1.1 and 1.2.

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 150).

▶ **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.

- **DHCP settings:** Optionally specify the preferred hostname, which must meet the following requirements:
  - Consists of alphanumeric characters and/or hyphens
  - Cannot begin or end with a hyphen
  - Cannot contain more than 63 characters
  - Cannot contain punctuation marks, spaces, and other symbols

- **Static settings:** Assign a static IPv4 address, which follows this syntax "IP address/prefix length".
    Example: *192.168.84.99/24*

▶ **IPv6 settings:**

Field/setting	Description
Enable IPv6	Enable or disable the IPv6 protocol.
IP Auto Configuration	Select the method to configure IPv6 settings. ▪ *Automatic*: Auto-configure IPv6 settings via DHCPv6. ▪ *Static*: Manually configure the IPv6 settings.

- **Automatic settings:** Optionally specify the preferred hostname, which must meet the above requirements.
- **Static settings:** Assign a static IPv6 address, which follows this syntax "IP address/prefix length".
    Example: *fd07:2fa:6cff:1111::0/128*

Common Network Settings

Common Network Settings are OPTIONAL, not required. Therefore, leave them unchanged if there are no specific local networking requirements.

Field	Description
Cascading Mode	Leave it to the default "None" unless you are establishing a cascading chain. For more information, refer to: ▪ ***Cascading Multiple Legrand PDUs for Sharing Ethernet Connectivity*** (on page 32) ▪ ***Setting the Cascading Mode*** (on page 150)
DNS Resolver Reference	Determine which IP address is used when the DNS resolver returns both IPv4 and IPv6 addresses. ▪ IPv4 Address: Use the IPv4 addresses. ▪ IPv6 Address: Use the IPv6 addresses.
DNS Suffixes (optional)	Specify a DNS suffix name if needed.
First/Second/Third DNS Server	Manually specify static DNS server(s). ▪ If any static DNS server is specified in these fields, it will override the DHCP-assigned DNS server. ▪ If DHCP (or Automatic) is selected for IPv4/IPv6 settings, and there are NO static DNS servers specified, the Legrand PDU will use DHCP-assigned DNS servers.

Field	Description
IPv4/IPv6 Routes	You need to configure these settings only when your local network contains two subnets, and you want Legrand PDU 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 148).

Ethernet Interface Settings

By default both ETH1 and ETH2 interfaces on Legrand PDU 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.

Enable Interface   ☑

▶ **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.
Duplex	Select a duplex mode.
	• Auto: The Legrand PDU selects the optimum transmission mode through auto-negotiation.
	• Full: Data is transmitted in both directions simultaneously.
	• Half: Data is transmitted in one direction (to or from the Legrand PDU) at a time.
Current State	Show the LAN's current status, including the current speed and duplex mode.

Note: Auto-negotiation is disabled after setting both the speed and duplex settings of the Legrand PDU to NON-Auto values, which may result in a duplex mismatch.

![Legrand logo]

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 150).

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.
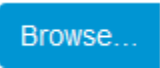
▶ **Interface Settings:**

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 Legrand PDU has detected a wireless USB LAN adapter. If not, verify whether the USB LAN adapter is firmly connected or whether it is supported.
SSID	Type the name of the wireless access point (AP).
Force AP BSSID	If the BSSID is available, select this checkbox.
BSSID	Type the MAC address of an access point.
Enable High Throughput (802.11n)	Enable or disable 802.11n protocol.
Authentication	Select an authentication method. ▪ *No Authentication*: No authentication data is required. ▪ *PSK*: A Pre-Shared Key is required. ▪ *EAP - PEAP*: Use Protected Extensible Authentication Protocol. Only MSCHAPv2 is supported. Enter required authentication data in the fields that appear.
Pre-Shared Key	This field appears only when PSK is selected. Type the PSK string.
Identity	This field appears only when 'EAP - PEAP' is selected. Type your user name.
Password	This field appears only when 'EAP - PEAP' is selected. Type your password.

June 2018

Field/setting	Description
CA Certificate	This field appears only when 'EAP - PEAP' is selected.
	A third-party CA certificate may or may not be needed. If needed, follow the steps below.

- **Available settings for the CA Certificate:**

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*** .

Field/setting	Description
Enable verification of TLS certificate chain	Select this checkbox for the Legrand PDU to verify the validity of the TLS certificate that will be installed. ▪ For example, the Legrand PDU 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 wireless connection if system clock is incorrect	When this checkbox is deselected, and if the system time is incorrect, the installed TLS certificate is considered not valid yet and will cause the wireless network connection to fail. When this checkbox is selected, it will make the wireless network connection successful when the Legrand PDU system time is earlier than the firmware build before synchronizing with any NTP server. ▪ The incorrect system time issue may occur when the Legrand PDU has once been powered off for a long time.

► **IPv4 settings:**

Field/setting	Description
Enable IPv4	Enable or disable the IPv4 protocol.
IP Auto Configuration	Select the method to configure IPv4 settings. ▪ *DHCP*: Auto-configure IPv4 settings via DHCP servers. ▪ *Static*: Manually configure the IPv4 settings.

- **DHCP settings:** Optionally specify the preferred hostname, which must meet the following requirements:
  - Consists of alphanumeric characters and/or hyphens
  - Cannot begin or end with a hyphen
  - Cannot contain more than 63 characters
  - Cannot contain punctuation marks, spaces, and other symbols
- **Static settings:** Assign a static IPv4 address, which follows this syntax "IP address/prefix length".
  Example: *192.168.84.99/24*

▶ **IPv6 settings:**

Field/setting	Description
Enable IPv6	Enable or disable the IPv6 protocol.
IP Auto Configuration	Select the method to configure IPv6 settings. • *Automatic*: Auto-configure IPv6 settings via DHCPv6. • *Static*: Manually configure the IPv6 settings.

- **Automatic settings:** Optionally specify the preferred hostname, which must meet the above requirements.
- **Static settings:** Assign a static IPv6 address, which follows this syntax "IP address/prefix length".
  Example: *fd07:2fa:6cff:1111::0/128*

▶ **(Optional) To view the wireless LAN diagnostic log:**

- Click Show WLAN Diagnostic Log. See ***Wireless LAN Diagnostic Log*** (on page 146).

Wireless LAN Diagnostic Log

The Legrand PDU provides a diagnostic log for inspecting connection errors that occurred over the wireless network interface. The information is useful for technical support.

Note that the WLAN Diagnostic Log shows data only after the Network Interface is set to Wireless.

Each entry in the log consists of:

- ID number
- Date and time
- Description

▶ **To view the log:**

1. Choose Device Settings > Network > WIRELESS > Show WLAN Diagnostic Log. See ***Configuring Network Settings*** (on page 140).
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 86).

▶ **To clear the diagnostic log:**

1. On the top-right corner of the log, click ⋮ > 🗑 **Clear Log**.
2. Click Clear Log on the confirmation message.

Static Route Examples

This section describes two static route examples: IPv4 and IPv6. Both examples assume that two network interface controllers (NIC) have been installed in one network server, leading to two available subnets, and IP forwarding has been enabled. All of the NICs and Legrand PDUs 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 150).*

▶ **IPv4 example:**
- Your Legrand PDU: *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*
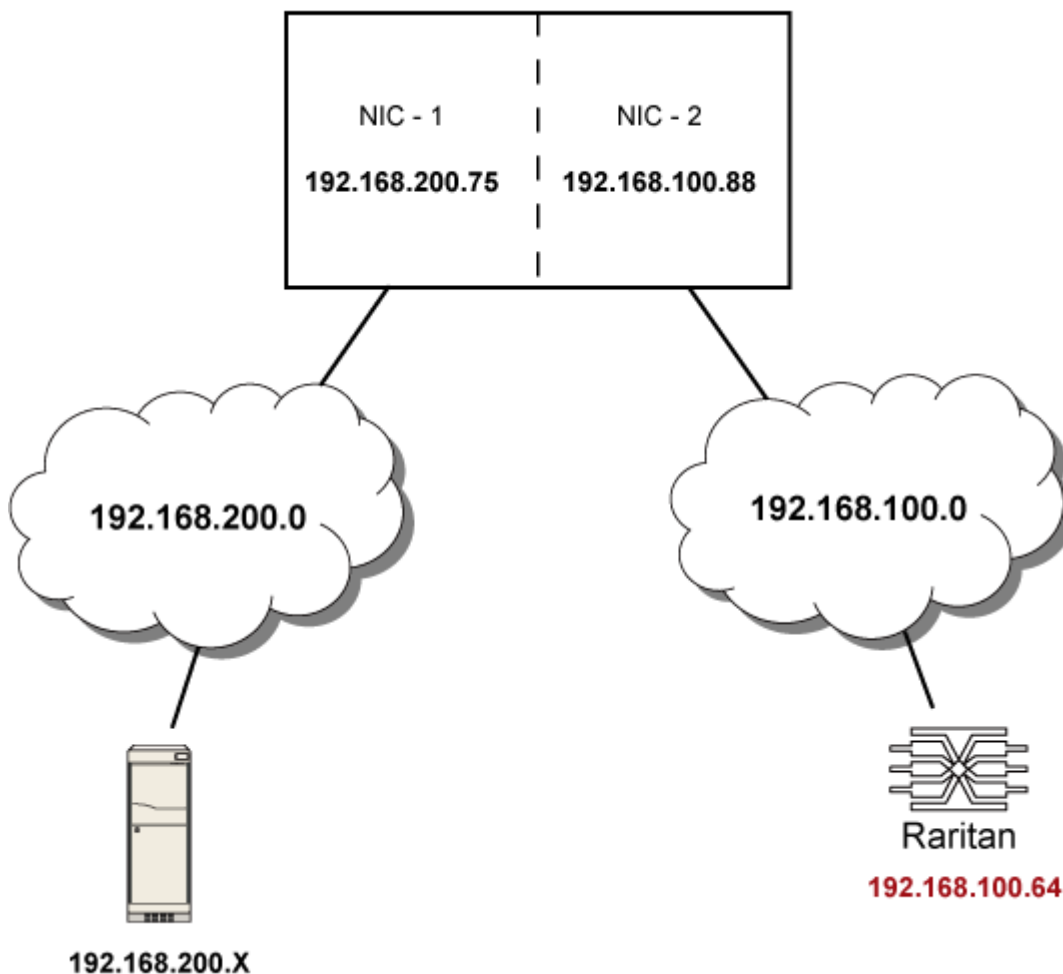
In this example, NIC-2 (192.168.100.88) is the next hop router for your Legrand PDU to communicate with any device in the other subnet 192.168.200.0.

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.

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.*
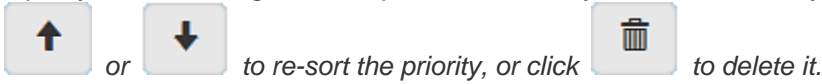
▶ **IPv6 example:**

- Your Legrand PDU: *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*
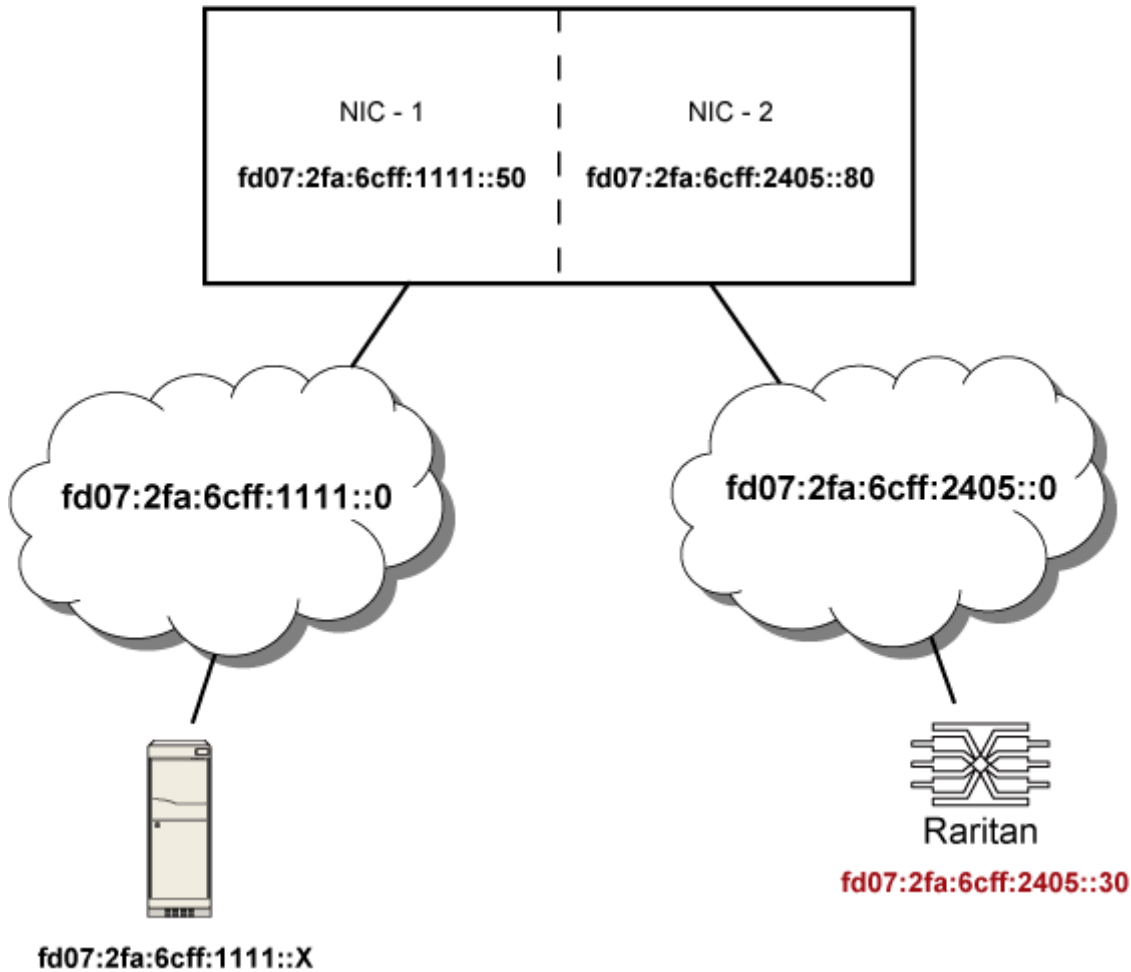
In this example, NIC-2 (fd07:2fa:6cff:2405::80) is the next hop router for your Legrand PDU to communicate with any device in the other subnet fd07:2fa:6cff:1111::0.

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.

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.*
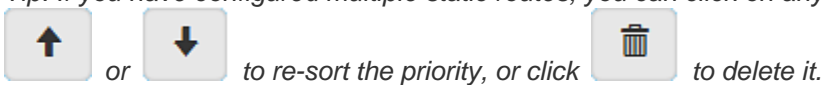
Interface Names

When your local multiple networks are "directly reachable", you should select Interface for static routes. Then choose the interface where another network is connected.
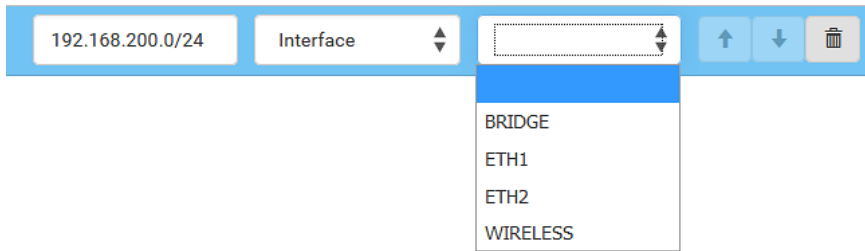
▶ **Interface list:**

Interface name	Description
BRIDGE	When another wired network is connected to the Ethernet port of your Legrand PDU, and your Legrand PDU 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 Legrand PDU, select this interface name.
ETH2	When another wired network is connected to the ETH2 port of your Legrand PDU, select this interface name.
WIRELESS	When another wireless network is connected to your Legrand PDU, select this interface name.

Setting the Cascading Mode

A maximum of 16 Legrand PDUs can be cascaded to share one Ethernet connection. See *Cascading Multiple Legrand PDUs for Sharing Ethernet Connectivity* (on page 32).

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 152).

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: Legrand PDU in the Port Forwarding mode does not support APIPA. See **APIPA and Link-Local Addressing** *(on page 16).*

▶ **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 Legrand PDU to a Computer* (on page 30).
   - To find the IP address, see *Device Info* (on page 70).
2. Log in to its web interface. See *Login* (on page 79).
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 153).

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
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 141) or *Wireless Network Settings* (on page 144)

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 155).

▶ **Enable R/STP if a cascade loop is preferred:**

- You can "loop" a cascading chain to create network communication redundancy (Bridging mode only), but only when your network supports **R/STP** protocol.

Make sure that your network has R/STP enabled if using a cascade loop (Bridging mode) *or else network loops may occur*.

► **Online cascading information:**

For detailed information on the cascading configuration and restrictions, refer to the *Cascading Guide*, which is available from the Legrand PDU section of Raritan website's ***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 150).

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:**
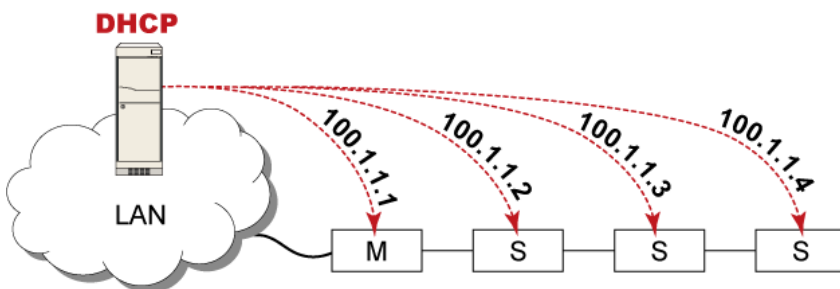
> In this mode, the DHCP server communicates with every cascaded device respectively and assigns four *different* IP addresses. Each device has its own IP address.
>
> The way to remotely access each cascaded device is completely the same as accessing a standalone device in the network.

• **"Port Forwarding" mode:**
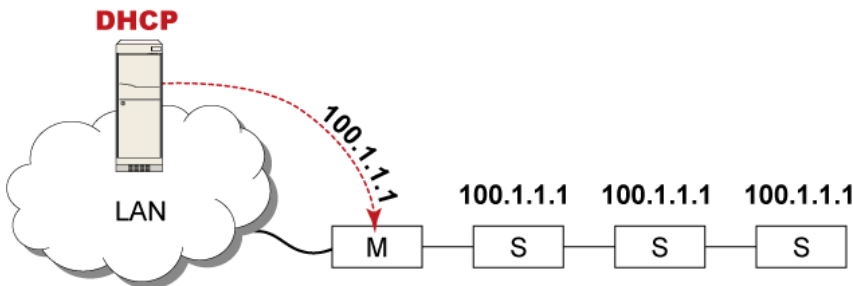
> In this mode, the DHCP server communicates with the master device alone and assigns one IP address to the master device. All slave devices share the same IP address as the master device.
>
> You must specify a 5XXXX port number (where X is a number) when remotely accessing any slave device with the shared IP address. See ***Port Number Syntax*** (on page 153).

► **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

- 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 155) 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 153) 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 482).*

▶ **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 150).
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

The Legrand PDU supports the following network communication services.

Network Services

- HTTP
- SNMP
- SMTP Server
- SSH
- Telnet
- Modbus
- Service Advertising

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 269).

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 158)
SNMP	**Configuring SNMP Settings** (on page 160)
SMTP Server	**Configuring SMTP Settings** (on page 161)
SSH	**Changing SSH Settings** (on page 162)
Telnet	**Changing Telnet Settings** (on page 163)
Modbus	**Changing Modbus Settings** (on page 163)
Service Advertising	**Enabling Service Advertising** (on page 164)

Important: Legrand 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 Legrand PDU so it is a more secure protocol than HTTP. The Legrand PDU supports TLS *1.0*, *1.1* and *1.2*.

By default, any access to the Legrand PDU 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 Legrand PDU 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 Legrand PDU device's SSL/TLS-based protocols, including HTTPS, support AES 128- and 256-bit ciphers. The exact cipher to use is negotiated between Legrand PDU and the client (such as a web browser), which is impacted by the cipher priority of Legrand PDU and the client's cipher availability/settings.

Tip: To force Legrand PDU 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.
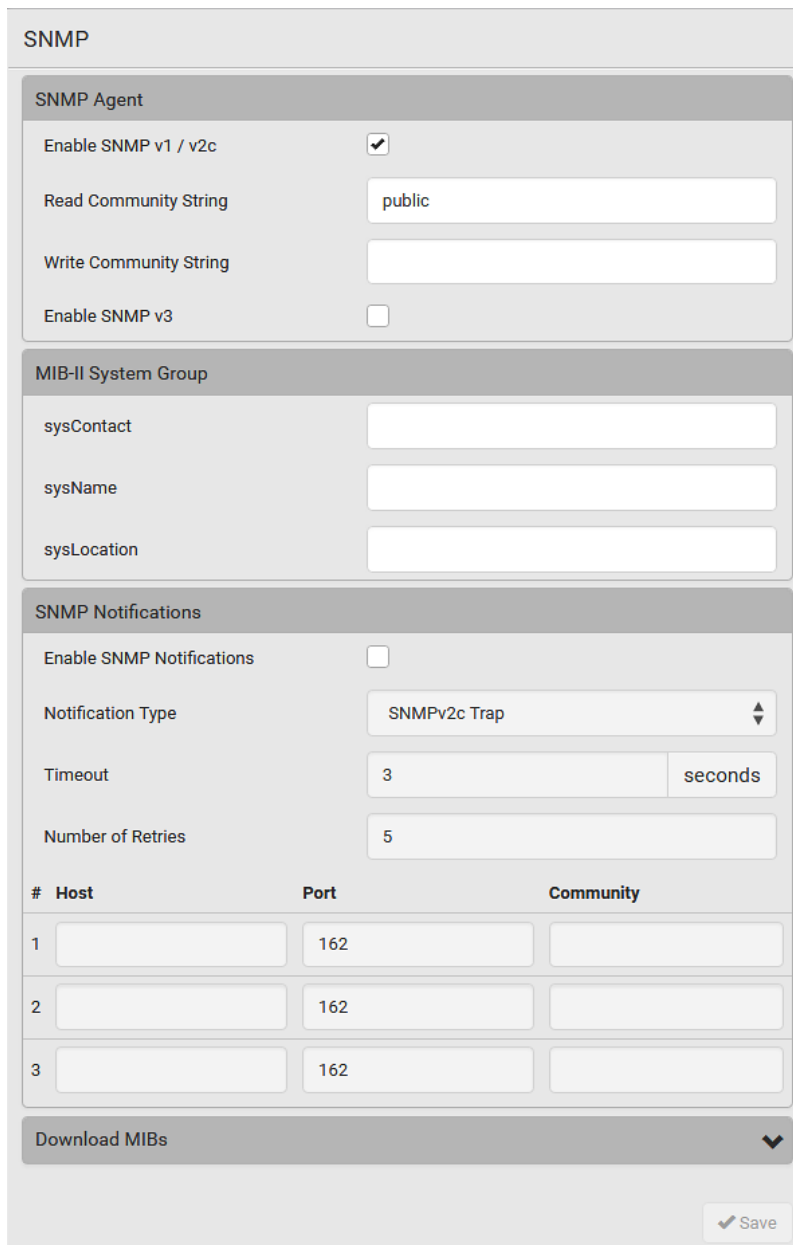
Configuring SNMP Settings

You can enable or disable SNMP communication between an SNMP manager and the Legrand PDU. Enabling SNMP communication allows the manager to retrieve and even control the power status of each outlet.

Besides, you may need to configure the SNMP destination(s) if the built-in "System SNMP Notification Rule" is enabled and the SNMP destination has not been set yet. See **_Event Rules and Actions_** (on page 184).

▶ **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	seconds
Number of Retries	5	

#	Host	Port	Community
1		162	
2		162	
3		162	

Download MIBs	⌄

✔ Save

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 262)
        - ***SNMPv3 Notifications*** (on page 263)

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 196). To add more than three SNMP destinations, you can create new SNMP notification actions. See* **Send an SNMP Notification** *(on page 202).*

5. You must download the SNMP MIB for your Legrand PDU 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 265).

6. Click Save.

Configuring SMTP Settings

The Legrand PDU can be configured to send alerts or event messages to a specific administrator by email. See ***Event Rules and Actions*** (on page 184).

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 236).

▶ **To set SMTP server settings:**
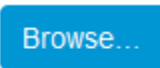
1. Choose Device Settings > Network Services > SMTP Server.

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.

Field	Description
User Name, Password	Type a user name and password for authentication after selecting the above checkbox. ▪ The length of user name and password ranges between 4 and 64. Case sensitive. ▪ Spaces are not allowed for the user name, but allowed for the password.
Enable SMTP over TLS (StartTLS)	If your SMTP server supports the Transport Layer Security (TLS), select this checkbox.

▪ **Settings for the CA Certificate:**

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 490).

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 Legrand PDU device's SSL/TLS-based protocols, including SMTP over StartTLS, support AES 128- and 256-bit ciphers. The exact cipher to use is negotiated between Legrand PDU and the client (such as a web browser), which is impacted by the cipher priority of Legrand PDU and the client's cipher availability/settings.

Tip: To force Legrand PDU 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 130).

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

You can enable or disable the Modbus/TCP access to the Legrand PDU, set it to the read-only mode, or change the TCP port.

▶ **To change the Modbus/TCP settings:**

1. Choose Device Settings > Network Services > Modbus.
2. To enable the Modbus/TCP access, select the "Modbus/TCP Access" checkbox.
3. To use a different port, type a new port number.
4. To enable the Modbus read-only mode, select the checkbox of the "Read-only mode" field. To enable the read-write mode, deselect it.

June 2018

Enabling Service Advertising

The Legrand PDU 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 16).

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 Legrand PDU. 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 141).*

▶ **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 Legrand PDU 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 Legrand PDU to be redirected to HTTPS, see **Changing HTTP(S) Settings** *(on page 158).*

Submenu command	Refer to
IP Access Control	**Creating IP Access Control Rules** (on page 165)
Role Based Access Control	**Creating Role Based Access Control Rules** (on page 168)
SSL Certificate	**Setting Up an SSL/TLS Certificate** (on page 170)
Authentication	**Setting Up External Authentication** (on page 173)
Login Settings	**Configuring Login Settings** (on page 179)
Password Policy	**Configuring Password Policy** (on page 180)
Service Agreement	**Enabling the Restricted Service Agreement** (on page 181)

Creating IP Access Control Rules

IP access control rules (firewall rules) determine whether to accept or discard traffic to/from the Legrand PDU, 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 Legrand PDU, 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 Legrand PDU.
   - Outbound rules control the data sent from the Legrand PDU.
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.

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 cannot edit or delete any rule.
4. Perform the desired action.
   - Make changes to the selected rule, and then click Save. For information on each field, see *Creating IP Access Control Rules* (on page 165).

- 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 cannot select any rule.
4. Perform the desired action.
   - Make changes to the selected rule, and then click Save. For information on each field, see *Creating Role Based Access Control Rules* (on page 168).

   - 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.

Important: Legrand uses TLS instead of SSL 3.0 due to published security vulnerabilities in SSL 3.0. Make sure your network infrastructure, such as LDAP and mail services, uses TLS rather than SSL 3.0.

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

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 Legrand PDU. See **Creating a CSR** (on page 170).
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 Legrand PDU. See **Installing a CA-Signed Certificate** (on page 171).

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 Legrand PDU create a *self-signed* certificate. See **Creating a Self-Signed Certificate** (on page 172).
- Appropriate, valid certificate and key files are already available, and you just need to import them. See **Installing or Downloading Existing Certificate and Key** (on page 173).

Creating a CSR

Follow this procedure to create the CSR for your Legrand PDU.

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

▶ **To create a CSR:**
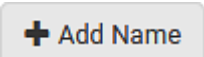
1. Choose Device Settings > Security > SSL Certificate.
2. Provide the information requested.
   ▪ **Subject:**

Field	Description
Country	The country where your company is located. Use the standard ISO country code. For a list of ISO codes, visit the **ISO website** (**http://www.iso.org/iso/country_codes/iso_3166_code_lists.htm**).
State or Province	The full name of the state or province where your company is located.
Locality	The city where your company is located.
Organization	The registered name of your company.
Organizational Unit	The name of your department.
Common Name	The fully qualified domain name (FQDN) of your Legrand PDU.
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 Legrand PDU. ▪ 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 SSL Key to create both the CSR and private key. This may take several minutes to complete.
4. Click Download Certificate Signing Request to download the CSR to your computer.
   a. You are prompted to open or save the file. Click Save to save it onto your computer.
   b. Submit it to a CA to obtain the digital certificate.
   c. If the CSR contains incorrect data, click Delete Certificate Signing Request to remove it, and then repeat the above steps to re-create it.
5. To store the newly-created private key on your computer, click Download Key in the **New SSL Certificate** section.

Note: The Download Key button in the Active SSL Certificate *section is for downloading the private key of the currently-installed certificate rather than the newly-created one.*

- You are prompted to open or save the file. Click Save to save it onto your computer.
6. After getting the CA-signed certificate, install it. See ***Installing a CA-Signed Certificate*** (on page 171).

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 170).

After receiving the CA-signed certificate, install it onto the Legrand PDU.

▶ **To install the CA-signed certificate:**
1. Choose Device Settings > Security > SSL Certificate.
2. Click **Browse...** to navigate to the CA-signed certificate file.
3. Click Upload to install it.
4. To verify whether the certificate has been installed successfully, check the data shown in the Active SSL Certificate section.

Creating a Self-Signed Certificate

When appropriate certificate and key files for the Legrand PDU 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.'

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

1. Choose Device Settings > Security > SSL Certificate.

2. Enter information.

Field	Description
Country	The country where your company is located. Use the standard ISO country code. For a list of ISO codes, visit the ***ISO website*** (***http://www.iso.org/iso/country_codes/iso_3166_code_lists.htm***).
State or Province	The full name of the state or province where your company is located.
Locality	The city where your company is located.
Organization	The registered name of your company.
Organizational Unit	The name of your department.
Common Name	The fully qualified domain name (FQDN) of your Legrand PDU.
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 Legrand PDU. ▪ Only 2048 is available now.
Self-Sign	**Ensure this checkbox is selected, which indicates that you are creating a self-signed certificate.**
Validity in days	This field appears after the Self Sign checkbox is selected. Type the number of days for which the self-signed certificate will be valid.

A password is not required for a self-signed certificate so the Challenge and Confirm Challenge fields disappear.

3. Click Create New SSL Key to create both the self-signed certificate and private key. This may take several minutes to complete.

4. Once complete, do the following:

   a. Double check the data shown in the New SSL Certificate section.

   b. If correct, click "Install Key and Certificate" to install the self-signed certificate and private key.

   Tip: To verify whether the certificate has been installed successfully, check the data shown in the Active SSL Certificate section.

   If incorrect, click "Delete Key and Certificate" to remove the self-signed certificate and private key, and then repeat the above steps to re-create them.

5. (Optional) To download the self-signed certificate and/or private key, click Download Certificate or Download Key in the New SSL Certificate section.

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

   Note: The Download Key button in the Active SSL Certificate *section is for downloading the private key of the currently-installed certificate rather than the newly-created one.*

Installing or Downloading Existing Certificate and Key

You can download the already-installed certificate and private key from any Legrand PDU for backup or file transfer. For example, you can install the files onto a replacement Legrand PDU, 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 Legrand PDU without going through the process of creating a CSR or a self-signed certificate.

Note: If you are using a certificate that is part of a chain of certificates, each part of the chain is signed during the validation process.
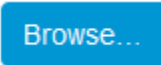
▶ **To download active key and certificate files from the Legrand PDU:**

1.   Choose Device Settings > Security > SSL Certificate.
2.   In the *Active SSL Certificate* section, click Download Key and Download Certificate respectively.

Note: The Download Key button in the New SSL Certificate section, if present, is for downloading the newly-created private key rather than the one of the currently-installed certificate.

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

▶ **To install available key and certificate files onto the Legrand PDU:**

1.   Choose Device Settings > Security > SSL Certificate.
2.   Select the "Upload Key and Certificate" checkbox at the bottom of the page.
3.   The Key File and Certificate File fields appear. Click [Browse...] to select the key and/or certificate file.
4.   Click Upload. The selected files are installed.
5.   To verify whether the certificate has been installed successfully, check the data shown in the Active SSL Certificate section.

Setting Up External Authentication

Important: Legrand 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.

June 2018

For security purposes, users attempting to log in to the Legrand PDU must be authenticated. The Legrand PDU supports the following authentication mechanisms:

- Local user database on the Legrand PDU
- Lightweight Directory Access Protocol (LDAP)
- Remote Access Dial-In User Service (Radius) protocol

By default, the Legrand PDU is configured for local authentication. If you stay with this method, you only need to create user accounts. See **Creating Users** (on page 130).

If you prefer external authentication, you must provide the Legrand PDU with information about the external Authentication and Authorization (AA) server.

If both local and external authentication is needed, create user accounts on the Legrand PDU in addition to providing the external AA server data.

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

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 236).

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 174).
2. Enter required data for external AA server(s) on the Legrand PDU. See **Adding LDAP/LDAPS Servers** (on page 175) or **Adding Radius Servers** (on page 177).
   - For illustrations, see **LDAP Configuration Illustration** (on page 431) or **Radius Configuration Illustration** (on page 442).
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 178).

▶ **Special note about the AES cipher:**

The Legrand PDU device's SSL/TLS-based protocols, including LDAPS, support AES 128- and 256-bit ciphers. The exact cipher to use is negotiated between Legrand PDU and the client (such as a web browser), which is impacted by the cipher priority of Legrand PDU and the client's cipher availability/settings.

Tip: To force Legrand PDU 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 Legrand PDU 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 Legrand PDU. 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 Legrand PDU 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.

Field/setting	Description
Port (TLS)	**Configurable only when "TLS" is selected in the Security field.** The default is 636. Either use the default port or specify another one.
Enable verification of LDAP Server Certificate	Select this checkbox if it is required to validate the LDAP server's certificate by the Legrand PDU 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 490).*
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`.
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.

Field/setting	Description
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 Legrand PDU 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 178).*

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 Legrand PDU, 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 Legrand PDU 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 Legrand PDU and the LDAP server to use the same NTP server(s).

Adding Radius Servers

To use Radius authentication, enable it and enter the information you have gathered.

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

required

▶ **To add Radius servers:**

1. Choose Device Settings > Security > Authentication.
2. Click New in the Radius section.
3. Enter information.

Field/setting	Description
IP Address / Hostname	The IP address or hostname of your Radius server.

Field/setting	Description
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 Legrand PDU 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 178).*

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 175) or **Adding Radius Servers** (on page 177).
- 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 Legrand PDU 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 Legrand PDU always tries external authentication first. Whenever the external authentication fails, the Legrand PDU switches to local authentication.

✔ Use Local Authentication if Remote Authentication is not available
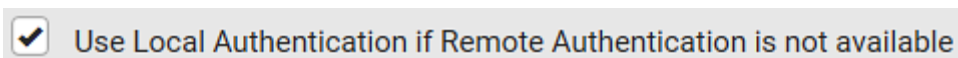
3. Click Save.

▶ **To disable external authentication:**

1. In the Authentication Type, select Local.
2. Click Save.

Configuring Login Settings

Choose Device Settings > Security > Login Settings to open the Login Settings page, where you can:

- Configure the user blocking feature.

Note: The user blocking function applies only to local authentication instead of external authentication through AA servers.

- Determine the timeout period for any inactive user.
- Prevent simultaneous logins using the same login name.

▶ **To configure user blocking:**

1. To enable the user blocking feature, select the "Block user on login failure" checkbox.
2. In the "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 98).
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 Legrand PDU.
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 388).*

▶ **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 98).

- 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 Legrand PDU.

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.

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 Legrand PDU.

▶ **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 98).

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 Legrand PDU 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 Legrand PDU.

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 189)

▶ **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 Legrand PDU manually, or link to a Network Time Protocol (NTP) server.

Note: If you are using Sunbird's Power IQ to manage the Legrand PDU, you must configure Power IQ and the Legrand PDU 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   [📅]   to select a date. For details, see *Calendar* (on page 183).

▪ Type values in the Time field using the hh:mm:ss format, or click 🔼 🔽 to adjust values.

   ▪ The time is measured in 12-hour format so you must correctly specify AM or PM by clicking the AM or PM button.

| 12 | : | 00 | : | 00 | AM |

Use the NTP server

▪ Select "Synchronize with NTP Server."

▪ There are two ways to assign the NTP servers:

   ▪ To use the DHCP-assigned NTP servers, DO NOT enter any NTP servers for the First and Second NTP Server.

   DHCP-assigned NTP servers are available only when either IPv4 or IPv6 DHCP is enabled.

   ▪ To use the manually-specified NTP servers, specify the primary NTP server in the First Time Server field. A secondary NTP server is optional.

   Click Check NTP Servers to verify the validity and accessibility of the manually-specified NTP servers.

---

5. Click Save.

Legrand PDU follows the NTP server sanity check per the IETF RFC. If your Legrand PDU has problems synchronizing with a Windows NTP server, see *Windows NTP Server Synchronization Solution* (on page 184).

The 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.
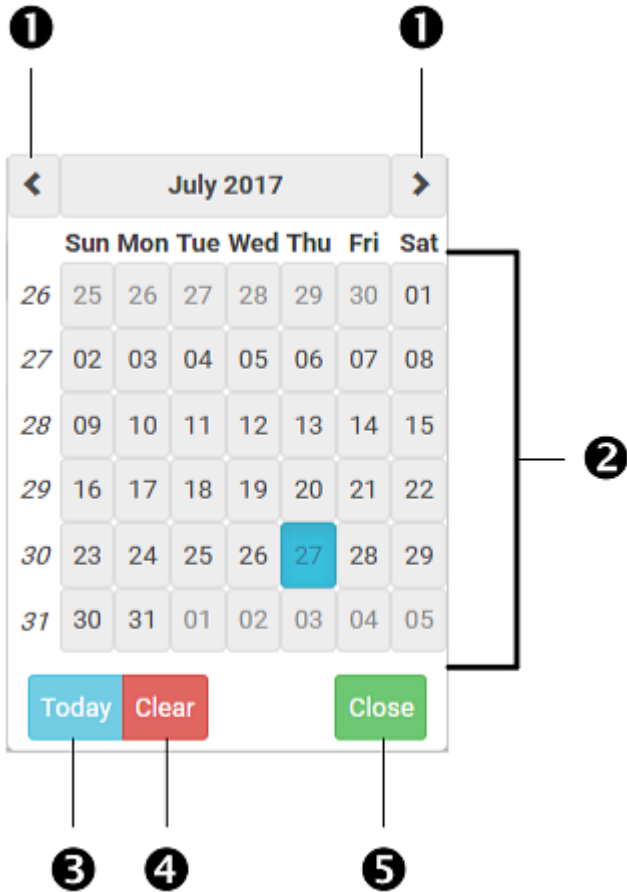
Number	Item	Description
1	arrows	Switch between months.
2	dates (01-31)	All dates of the selected month. To select a date, simply click it.
3	Today	Select today's date.
4	Clear	Clear the entry, if any, in the Date field.
5	Close	Close the calendar.

Windows NTP Server Synchronization Solution

The NTP client on the Legrand PDU follows the NTP RFC so the Legrand PDU 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 Legrand PDU.

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 Legrand PDU. 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."
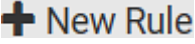
An event rule consists of two parts:

- Event: This is the situation where the Legrand PDU 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 Legrand PDU notifies the system administrator of the event via email.

If you want the Legrand PDU 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 Legrand PDU 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 196).

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 Legrand PDU 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 185).

▶ **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 Legrand PDU 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 206).

Built-in Rules and Rule Configuration

Legrand PDU 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 Legrand PDU 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 189).*
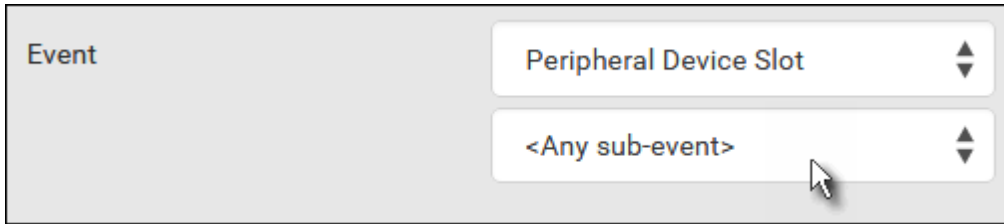
- *System SNMP Notification Rule:*

    This causes SNMP traps or informs to be sent to specified IP addresses or hosts when ANY event occurs to the Legrand PDU. It is disabled by default.

- *System Tamper Detection Alarmed:*

    This causes the Legrand PDU to send alarm notifications if a DX tamper sensor has been connected and the Legrand PDU detects that the tamper sensor enters the alarmed state. It is enabled by default.

- *System Tamper Detection Unavailable:*

    This causes the Legrand PDU to send alarm notifications if a DX tamper sensor was once connected or remains connected but then the Legrand PDU does not detect the presence of the tamper sensor. It is enabled by default.

▶ **Event rule configuration illustration:**

1. Choose Device Settings > Event Rules > ✚ New Rule.

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 Legrand PDU, 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.
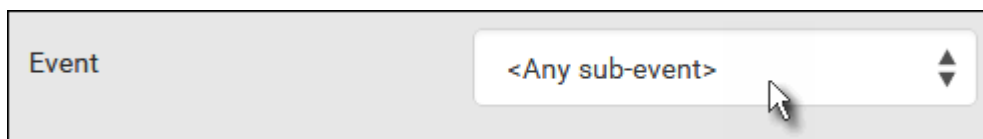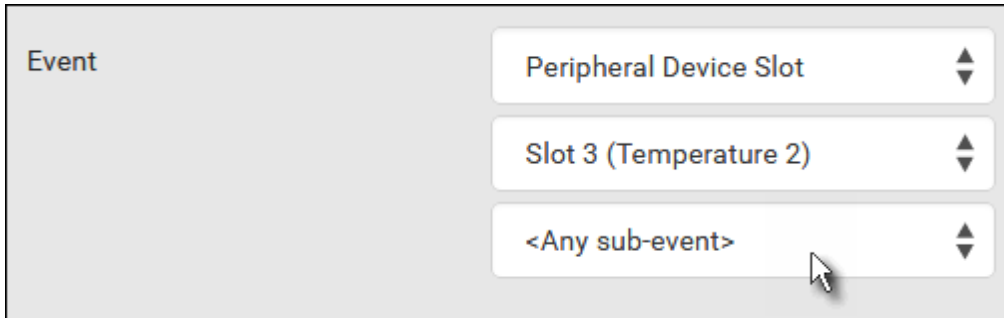
Event	<Any sub-event>	⬍

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.
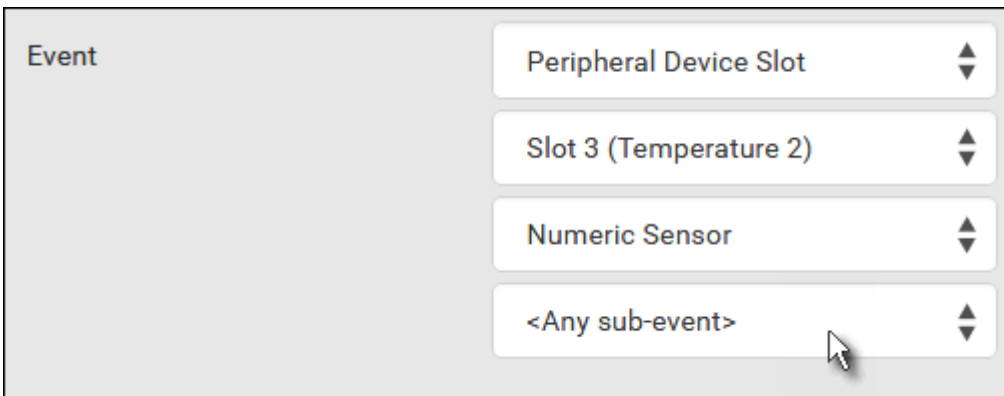
| Event | Peripheral Device Slot ⬍ |
| | \<Any sub-event\> ⬍ |

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 Legrand PDU to react only when the selected temperature sensor's reading enters the upper critical range. A "Trigger condition" field appears, requiring you to define the "exact" condition related to the "upper critical" event.

7. Select the desired radio button to finish the event configuration. Refer to the following table for different types of radio buttons.
   - If needed, you may refer to event rule examples in the section titled *Sample Event Rules* (on page 214).
8. To select any action(s), select them one by one from the Available Actions list.
   - To select all available actions, click Select All.
9. To remove any action(s) from the Selected Actions field, click that action's ✖.
   - To remove all actions, click Deselect All.

▶ **Radio buttons for different events:**

According to the event you select, the "Trigger condition" field containing three radio buttons may or may not appear.

Event types	Radio buttons
Numeric sensor threshold-crossing events, or the occurrence of the selected event -- true or false	Available radio buttons include "Asserted," "Deasserted" and "Both." ▪ Asserted: Legrand PDU takes the action only when the selected event occurs. That is, the status of the event transits from FALSE to TRUE. ▪ Deasserted: Legrand PDU 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: Legrand PDU takes the action both when the event occurs (asserts) and when the event stops/disappears (deasserts).

Event types	Radio buttons
State sensor state change	Available radio buttons include "Alarmed/Open/On," "No longer alarmed/Closed/Off" and "Both." • Alarmed/Open/On: Legrand PDU takes the action only when the chosen sensor enters the alarmed, open or on state. • No longer alarmed/Closed/Off: Legrand PDU takes the action only when the chosen sensor returns to the normal, closed, or off state. • Both: Legrand PDU takes the action whenever the chosen sensor switches its state.
Sensor availability	Available radio buttons include "Unavailable," "Available" and "Both." • Unavailable: Legrand PDU takes the action only when the chosen sensor is NOT detected and becomes unavailable. • Available: Legrand PDU takes the action only when the chosen sensor is detected and becomes available. • Both: Legrand PDU takes the action both when the chosen sensor becomes unavailable or available.
Network interface link state	• Link state is up: Legrand PDU takes the action only when the network link state changes from down to up. • Link state is down: Legrand PDU takes the action only when the network link state changes from up to down. • Both: Legrand PDU takes the action whenever the network link state changes.
Function enabled or disabled	• Enabled: Legrand PDU takes the action only when the chosen function is enabled. • Disabled: Legrand PDU takes the action only when the chosen function is disabled. • Both: Legrand PDU takes the action when the chosen function is either enabled or disabled.
Restricted service agreement	• Accepted: Legrand PDU takes the action only when the specified user accepts the restricted service agreement. • Declined: Legrand PDU takes the action only when the specified user rejects the restricted service agreement. • Both: Legrand PDU takes the action both when the specified user accepts or rejects the restricted service agreement.

June 2018

Event types	Radio buttons
Server monitoring event	▪ Monitoring started: Legrand PDU takes the action only when the monitoring of any specified server starts. ▪ Monitoring stopped: Legrand PDU takes the action only when the monitoring of any specified server stops. ▪ Both: Legrand PDU takes the action when the monitoring of any specified server starts or stops.
Server reachability	▪ Unreachable: Legrand PDU takes the action only when any specified server becomes inaccessible. ▪ Reachable: Legrand PDU takes the action only when any specified server becomes accessible. ▪ Both: Legrand PDU takes the action when any specified server becomes either inaccessible or accessible.
Device connection or disconnection, such as a USB-cascaded slave device	▪ Connected: Legrand PDU takes the action only when the selected device is physically connected to it. ▪ Disconnected: Legrand PDU takes the action only when the selected device is physically disconnected from it. ▪ Both: Legrand PDU takes the action both when the selected device is physically connected to it and when it is disconnected.

Default Log Messages

These default log messages are recorded internally and emailed to specified recipients when Legrand PDU events occur (are TRUE) or, in some cases, stop or become unavailable (are FALSE). See **Send Email** (on page 200) to configure email messages.

Event/context	Default message when the event = TRUE	Default message when the event = FALSE
Card Reader Management > Card inserted	Card Reader with id '[CARDREADERID]' connected.	
Card Reader Management > Card Reader attached	Card Reader with id '[CARDREADERID]' disconnected.	
Card Reader Management > Card Reader detached	Card of type '[SMARTCARDTYPE]' with ID '[SMARTCARDID]' inserted.	
Card Reader Management > Card removed	Card of type '[SMARTCARDTYPE]' with ID '[SMARTCARDID]' removed.	
Device > System started	System started.	
Device > System reset	System reset performed by user '[USERNAME]' from host '[USERIP]'.	

Event/context	Default message when the event = TRUE	Default message when the event = FALSE
Device > Firmware validation failed	Firmware validation failed by user '[USERNAME]' from host '[USERIP]'.	
Device > Firmware update started	Firmware upgrade started from version '[OLDVERSION]' to version '[VERSION]' by user '[USERNAME]' from host '[USERIP]'.	
Device > Firmware update completed	Firmware upgraded successfully from version '[OLDVERSION]' to version '[VERSION]' by user '[USERNAME]' from host '[USERIP]'.	
Device > Firmware update failed	Firmware upgrade failed from version '[OLDVERSION]' to version '[VERSION]' by user '[USERNAME]' from host '[USERIP]'.	
Device > Device identification changed	Config parameter '[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].	
Device > Sending Syslog message failed	Sending Syslog message to server [SYSLOGSERVER]:[SYSLOGPORT] ([SYSLOGTRANSPORTPROTO]) failed. [ERRORDESC].	

Event/context	Default message when the event = TRUE	Default message when the event = FALSE
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 > 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.
Energywise > Enabled	User '[USERNAME]' from host '[USERIP]' enabled EnergyWise.	User '[USERNAME]' from host '[USERIP]' disabled EnergyWise.
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].
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].

Event/context	Default message when the event = TRUE	Default message when the event = FALSE
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].
Inlet > * > Enabled	Inlet '[INLET]' has been enabled by user '[USERNAME]' from host '[USERIP]'.	Inlet '[INLET]' has been disabled by user '[USERNAME]' from host '[USERIP]'.
Inlet > * > Sensor > * > Unavailable	Sensor '[INLETSENSOR]' on inlet '[INLET]' unavailable.	Sensor '[INLETSENSOR]' on inlet '[INLET]' available.
Inlet > * > Sensor > * > Above upper critical threshold	Sensor '[INLETSENSOR]' on inlet '[INLET]' asserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[INLETSENSOR]' on inlet '[INLET]' deasserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT].
Inlet > * > Sensor > * > Above upper warning threshold	Sensor '[INLETSENSOR]' on inlet '[INLET]' asserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[INLETSENSOR]' on inlet '[INLET]' deasserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT].
Inlet > * > Sensor > * > Below lower warning threshold	Sensor '[INLETSENSOR]' on inlet '[INLET]' asserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[INLETSENSOR]' on inlet '[INLET]' deasserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT].
Inlet > * > Sensor > * > Below lower critical threshold	Sensor '[INLETSENSOR]' on inlet '[INLET]' asserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[INLETSENSOR]' on inlet '[INLET]' deasserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT].
Inlet > * > Sensor > * > Reset	Sensor '[INLETSENSOR]' on inlet '[INLET]' has been reset by user '[USERNAME]' from host '[USERIP]'.	
Inlet > * > Sensor > * > Normal	Sensor '[INLETSENSOR]' on inlet '[INLET]' entered normal state.	Sensor '[INLETSENSOR]' on inlet '[INLET]' exited normal state.
Inlet > * > Sensor > * > Failed	Sensor '[INLETSENSOR]' on inlet '[INLET]' entered failed state.	Sensor '[INLETSENSOR]' on inlet '[INLET]' entered normal state.
Inlet > * > Sensor > * > OK	Sensor '[INLETSENSOR]' on inlet '[INLET]' entered OK state.	Sensor '[INLETSENSOR]' on inlet '[INLET]' exited OK state.
Inlet > * > Sensor > * > Warning	Sensor '[INLETSENSOR]' on inlet '[INLET]' entered warning state.	Sensor '[INLETSENSOR]' on inlet '[INLET]' exited warning state.
Inlet > * > Sensor > * > Critical	Sensor '[INLETSENSOR]' on inlet '[INLET]' entered critical state.	Sensor '[INLETSENSOR]' on inlet '[INLET]' exited critical state.
Inlet > * > Sensor > * > Self-Test	Sensor '[INLETSENSOR]' on inlet '[INLET]' started self test.	Sensor '[INLETSENSOR]' on inlet '[INLET]' finished self test.
Inlet > Pole > * > Sensor > Unavailable	Sensor '[PDUPOLESENSOR]' on pole '[INLETPOLE]' of inlet '[INLET]' unavailable.	Sensor '[PDUPOLESENSOR]' on pole '[INLETPOLE]' of inlet '[INLET]' available.

Event/context	Default message when the event = TRUE	Default message when the event = FALSE
Inlet > Pole > * > Sensor > Above upper critical threshold	Sensor '[PDUPOLESENSOR]' on pole '[INLETPOLE]' of inlet '[INLET]' asserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[PDUPOLESENSOR]' on pole '[INLETPOLE]' of inlet '[INLET]' deasserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT].
Inlet > Pole > * > Sensor > Above upper warning threshold	Sensor '[PDUPOLESENSOR]' on pole '[INLETPOLE]' of inlet '[INLET]' asserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[PDUPOLESENSOR]' on pole '[INLETPOLE]' of inlet '[INLET]' deasserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT].
Inlet > Pole > * > Sensor > Below lower warning threshold	Sensor '[PDUPOLESENSOR]' on pole '[INLETPOLE]' of inlet '[INLET]' asserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[PDUPOLESENSOR]' on pole '[INLETPOLE]' of inlet '[INLET]' deasserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT].
Inlet > Pole > * > Sensor > Below lower critical threshold	Sensor '[PDUPOLESENSOR]' on pole '[INLETPOLE]' of inlet '[INLET]' asserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[PDUPOLESENSOR]' on pole '[INLETPOLE]' of inlet '[INLET]' deasserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT].
Inlet > Pole > * > Sensor > Normal	Sensor '[PDUPOLESENSOR]' on pole '[INLETPOLE]' of inlet '[INLET]' entered normal state.	Sensor '[PDUPOLESENSOR]' on pole '[INLETPOLE]' of inlet '[INLET]' exited normal state.
Inlet > Pole > * > Sensor > Failed	Sensor '[PDUPOLESENSOR]' on pole '[INLETPOLE]' of inlet '[INLET]' entered failed state.	Sensor '[PDUPOLESENSOR]' on pole '[INLETPOLE]' of inlet '[INLET]' exited failed state.
Inlet > Pole > * > Sensor > Warning	Sensor '[PDUPOLESENSOR]' on pole '[INLETPOLE]' of inlet '[INLET]' entered warning state.	Sensor '[PDUPOLESENSOR]' on pole '[INLETPOLE]' of inlet '[INLET]' exited warning state.
Inlet > Pole > * > Sensor > Critical	Sensor '[PDUPOLESENSOR]' on pole '[INLETPOLE]' of inlet '[INLET]' entered critical state.	Sensor '[PDUPOLESENSOR]' on pole '[INLETPOLE]' of inlet '[INLET]' exited critical state.
Inlet > Pole > * > Sensor > Self-Test	Sensor '[PDUPOLESENSOR]' on pole '[INLETPOLE]' of inlet '[INLET]' started self test.	Sensor '[PDUPOLESENSOR]' on pole '[INLETPOLE]' of inlet '[INLET]' finished self test.
Outlet > * > Power control > Powered on	Outlet '[OUTLET]' has been powered on by user '[USERNAME]' from host '[USERIP]'.	
Outlet > * > Power control > Powered off	Outlet '[OUTLET]' has been powered off by user '[USERNAME]' from host '[USERIP]'.	
Outlet > * > Power control > Power cycled	Outlet '[OUTLET]' power cycle initiated by user '[USERNAME]' from host '[USERIP]'.	
Outlet > * > Sensor > Outlet State > On/Off	Outlet '[OUTLET]' state changed to on.	Outlet '[OUTLET]' state changed to off.
Overcurrent Protector > * > Sensor > * > Unavailable	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]'	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]'

Event/context	Default message when the event = TRUE	Default message when the event = FALSE
	unavailable.	available.
Overcurrent Protector > * > Sensor > * > Above upper critical threshold	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' asserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' deasserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT].
Overcurrent Protector > * > Sensor > * > Above upper warning threshold	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' asserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' deasserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT].
Overcurrent Protector > * > Sensor > * > Below lower warning threshold	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' asserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' deasserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT].
Overcurrent Protector > * > Sensor > * > Below lower critical threshold	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' asserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' deasserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT].
Overcurrent Protector > * > Sensor > Trip > Open/Close	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' is open.	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' is closed.
PDU > Controller > * > Communication failed	Communication with controller '[CONTROLLER]' (board ID [BOARDID]) failed.	Communication with controller '[CONTROLLER]' (board ID [BOARDID]) restored.
PDU > Controller > * > Firmware update	Controller '[CONTROLLER]' with board ID [BOARDID] has started firmware update	Controller '[CONTROLLER]' with board ID [BOARDID] has completed firmware update
PDU > Controller > * > Incompatible	Controller '[CONTROLLER]' with board ID [BOARDID] is incompatible.	Controller '[CONTROLLER]' with board ID [BOARDID] is no longer incompatible.
PDU > Controller > * > OK	Controller '[CONTROLLER]' with board ID [BOARDID] is OK.	Controller '[CONTROLLER]' with board ID [BOARDID] is no longer OK.
PDU > Load Shedding > Started	PX placed in Load Shedding Mode by user '[USERNAME]' from host '[USERIP]'.	PX removed from Load Shedding Mode by user '[USERNAME]' from host '[USERIP]'.
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.

June 2018

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 > Webcam attached	Webcam '[WEBCAMNAME]' ('[WEBCAMUVCID]') added to port '[WEBCAMUSBPORT]'.	
Webcam Management > Webcam detached	Webcam '[WEBCAMNAME]' ('[WEBCAMUVCID]') removed from port '[WEBCAMUSBPORT]'.	
Webcam Management > Webcam settings changed	Webcam '[WEBCAMNAME]' settings changed by user '[USERNAME]'.	

The asterisk symbol (*) represents anything you select for the 'trigger' events.

Available Actions

The Legrand PDU comes with three built-in actions, which cannot be deleted. You can create additional actions for responding to different events.

▶ **Built-in actions:**

- *System Event Log Action:*

  This action records the selected event in the internal log when the event occurs.

- *System SNMP Notification Action:*

  This action sends SNMP notifications to one or multiple IP addresses after the selected event occurs.

  Note: No IP addresses are specified for this notification action by default so you must enter IP addresses before applying this action to any event rule. See **Editing or Deleting a Rule/Action** *(on page 213). 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 160).*

- *System Tamper Alarm:*

  This action causes the Legrand PDU to show the alarm for the DX tamper sensor, if any, on the Dashboard page until a person acknowledges it. By default, this action has been assigned to the built-in tamper detection event rules. For information on acknowledging an alarm, see *Dashboard - Alarms* (on page 93).

▶ **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.

Note: The "Change load shedding state" and "Switch outlets" options are only available for outlet-switching capable models.

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 197).
Change load shedding state	Enters or quits the load shedding mode. See *Change Load Shedding State* (on page 198).
Execute an action group	Creates a group of actions comprising existing actions. See *Action Group* (on page 198).
Log event message	Records the selected events in the internal log. See *Log an Event Message* (on page 199).
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 199).

June 2018

Action	Function
Record snapshots to webcam storage	Makes a connected webcam start or stop taking snapshots. See **Record Snapshots to Webcam Storage** (on page 199).
Send email	Emails a textual message. See **Send Email** (on page 200).
Send sensor report	Reports the readings or status of the selected sensors, including internal or external sensors. See **Send Sensor Report** (on page 201).
Send snapshots via email	Emails the snapshots captured by a connected Logitech® webcam (if available). See **Send Snapshots via Email** (on page 202).
Send SNMP notification	Sends SNMP traps or informs to one or multiple SNMP destinations. See **Send an SNMP Notification** (on page 202).
Start/stop Lua script	If you are a developer who can create a Lua script, you can upload it to the Legrand PDU, and have the Legrand PDU automatically perform or stop the script in response to an event. See **Start or Stop a Lua Script** (on page 204).
Switch outlets	Switches on, off or cycles the power to the specified outlet(s). See **Switch Outlets** (on page 204).
Switch peripheral actuator	Switches on or off the mechanism or system connected to the specified actuator. See **Switch Peripheral Actuator** (on page 205).
Syslog message	Makes the Legrand PDU automatically forward event messages to the specified syslog server. See **Syslog Message** (on page 205).

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 184).
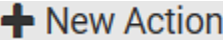
Alarm

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 Legrand PDU 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 87).

▶ **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:

- Syslog message
- Send email

If no appropriate actions are available, create them first.
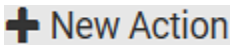
a. To select any methods, select them one by one in the Available field.

   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 Legrand PDU 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 196).

▶ **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.

Change Load Shedding State

The "Change load shedding state" action is available only when your Legrand PDU is able to control outlet power. Use this action to activate or deactivate the load shedding mode for responding to a specific event. For additional information, see *Load Shedding Mode* (on page 105).

▶ **Operation:**

1. Choose Device Settings > Event Rules > ✚ New Action.
2. Select "Change load shedding state" from the Action list.
3. In the Operation field, select either one below:
   - Start Load Shedding: Enters the load shedding mode when the specified event occurs.
   - Stop Load Shedding: Quits the load shedding mode when the specified event occurs.

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 189).

Push Out Sensor Readings

You can configure the Legrand PDU 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 Legrand PDU, you can also configure the Legrand PDU 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 220).

Tip: To send the data at a regular interval, schedule this action. See **Scheduling an Action** *(on page 206). Note that the "Asset management log" is generated only when there are changes made to any asset strips or asset tags, such as connection or disconnection events.*

▶ **Operation:**

1. Choose Device Settings > Event Rules > ➕ **New Action**.
2. Select "Push out sensor readings" from the Action list.
3. Select a server or host which receives the asset strip data or sensor log in the Destination field.
    ▪ If the desired destination is not available yet, go to the Data Push page to specify it.

Record Snapshots to Webcam Storage

This option allows you to define an action that starts or stops a specific webcam from taking snapshots.

Per default the snapshots are stored on the Legrand PDU. See **Viewing and Managing Locally-Saved Snapshots** (on page 253).

It is recommended to specify a remote server to store as many snapshots as possible. See **Changing Storage Settings** (on page 254).

▶ **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 Legrand PDU is 10. If you set it for a number greater than 10 and the storage location is on the Legrand PDU, 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.

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 Legrand PDU placeholders. The placeholders represent information which is pulled from the Legrand PDU 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 210).

▶ **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 161).

   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 189).

5. If needed, select the Use Custom Log Message checkbox, and then create a custom message up to 1024 characters in the provided field.

   ▪ When clicking anywhere inside the text box, the Event Context Information displays, showing a list of placeholders and their definitions. Just scroll down to select the desired placeholder. For details, see **Placeholders for Custom Messages** (on page 210).
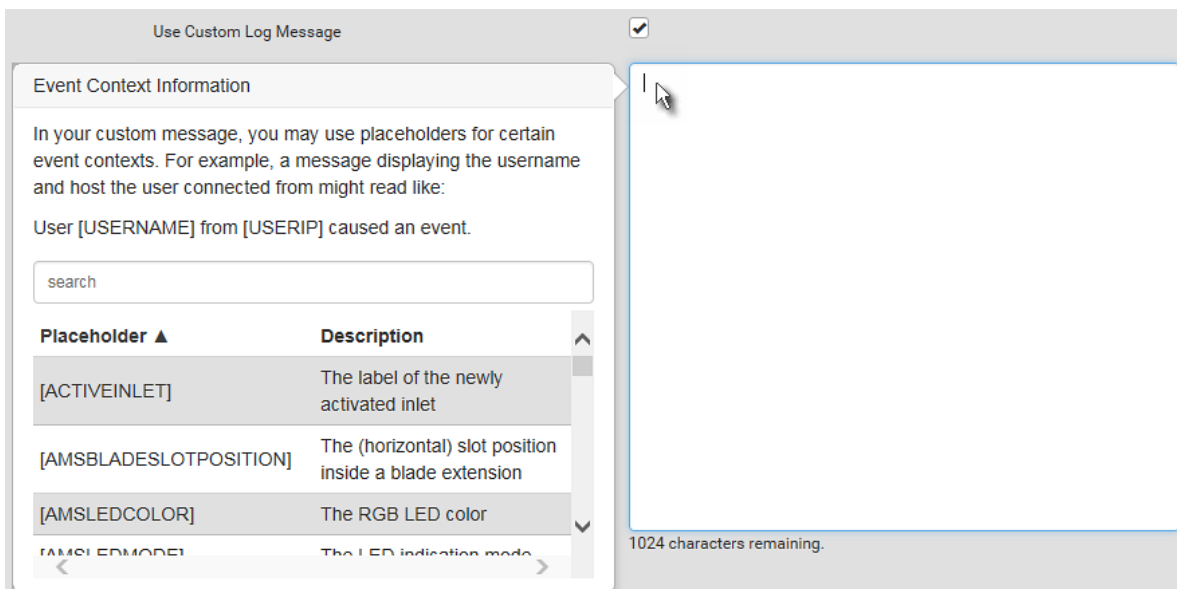
   ▪ To start a new line in the text box, press Enter.

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 Legrand PDU 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.

- Inlet sensors, including RMS current, RMS voltage, active power, apparent power, power factor and active energy.
- Outlet state sensors, which are available on outlet-switching capable PDUs only.
- Overcurrent protector sensors, including RMS current and tripping state.
- Peripheral device sensors, which can be any Raritan environmental sensor packages connected to the Legrand PDU, such as temperature or humidity sensors.

An example of this action is available in the section titled *Send Sensor Report Example* (on page 208).

▶ **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

   a. If no messaging actions are available, create them now. See *Available Actions* (on page 196).

   b. To select any methods, select them one by one in the Available field.

   To add all available methods, simply click Select All.

   c. To delete any methods, click a method's ✖ in the Selected field.

   To remove all methods, simply click Deselect All.

4. In the Available Sensors field, select the desired target's sensor.

   a. Click the first ↕ to select a target component from the list.

   Peripheral Devices ↕ Temperature 1 ⊕ ⊖
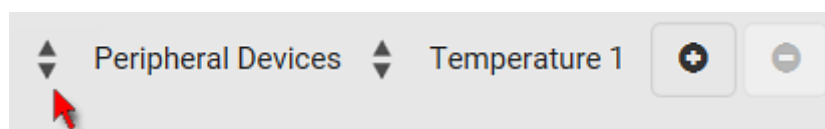
   b. Click the second ↕ to select the specific sensor for the target from the list.

   Peripheral Devices ↕ Temperature 1 ⊕ ⊖
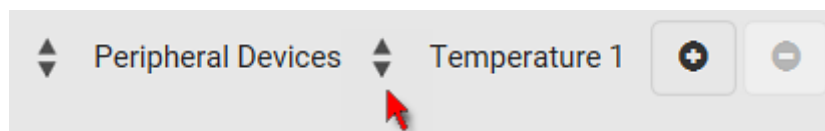
   c. Click ⊕ to add the selected sensor to the Report Sensors list box.

   For example, to monitor the current reading of the Inlet 1, select Inlet 1 from the left field, and then select RMS Current from the right field.

5. To report additional sensors simultaneously, repeat the above step to add more sensors.

- To remove any sensor from the Report Sensors list box, select it and click [⊖icon]. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.
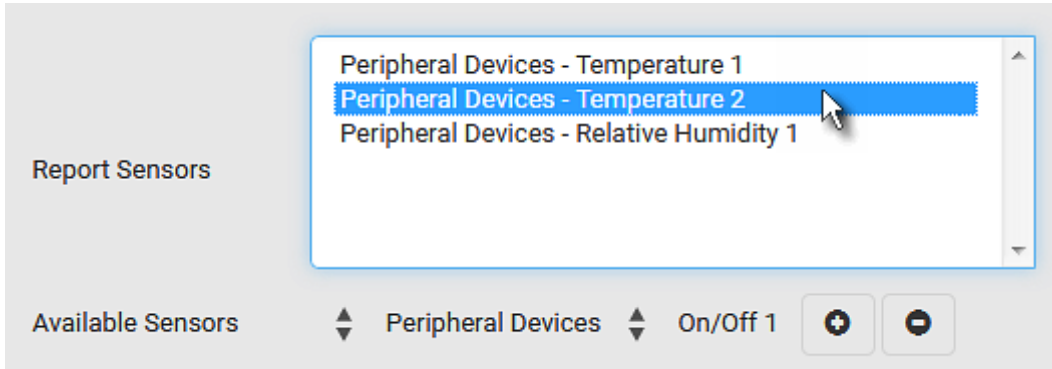
- To immediately send out the sensor report, click Send Report Now.

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 210).*

Send Snapshots via Email

This option notifies one or multiple persons for the selected events by emailing snapshots or videos captured by a connected Logitech® webcam.

▶ **Operation:**

1. Choose Device Settings > Event Rules > **➕ New Action**.
2. Select "Send snapshots via email" from the Action list.
3. In the "Recipient Email Addresses" field, specify the email address(es) of the recipient(s). Use a comma to separate multiple email addresses.
4. 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 161).
5. Select the webcam that is capturing the images you want sent in the email.
6. Adjust the values of the following:

   - Number of Snapshots - the number of snapshots to be taken when the event occurs. For example, you can specify 10 images be taken once the event triggers the action.
   - Snapshots per Mail - the number of snapshots to be sent at one time in the email.
   - Time Before First Snapshot - the amount of time in seconds between when the event is triggered and the webcam begins taking snapshots.
   - Time Between Snapshots - the amount of time in seconds between when each snapshot is taken.

Send an SNMP Notification

This option sends an SNMP notification to one or multiple SNMP destinations.

▶ **Operation:**

1. Choose Device Settings > Event Rules > **➕ New Action**.
2. Select "Send SNMP notification" from the Action list.
3. Select the type of SNMP notification. See either procedure below according to your selection.

▶ **To send SNMP v2c notifications:**

1. In the Notification Type field, select SNMPv2c Trap or SNMPv2c Inform.

2. For SNMP INFORM communications, leave the resend settings at their default or do the following:

   a. In the Timeout field, specify the interval of time, in seconds, after which a new inform communication is resent if the first is not received. For example, resend a new inform communication once every 3 seconds.

   b. In the Number of Retries field, specify the number of times you want to resend the inform communication if it fails. For example, inform communications are resent up to 5 times when the initial communication fails.

3. In the Host fields, enter the IP address of the device(s) you want to access. This is the address to which notifications are sent by the SNMP system agent.

4. In the Port fields, enter the port number used to access the device(s).

5. In the Community fields, enter the SNMP community string to access the device(s). The community is the group representing the Legrand PDU and all SNMP management stations.

Tip: An SNMP v2c notification action permits only a maximum of three SNMP destinations. To assign more than three SNMP destinations to a specific rule, first create several SNMP v2c notification actions, each of which contains completely different SNMP destinations, and then add all of these SNMP v2c notification actions to the same rule.

▶ **To send SNMP v3 notifications:**

1. In the Notification Type field, select SNMPv3 Trap or SNMPv3 Inform.

2. For SNMP TRAPs, the engine ID is prepopulated.

3. For SNMP INFORM communications, leave the resend settings at their default or do the following:

   a. In the Timeout field, specify the interval of time, in seconds, after which a new inform communication is resent if the first is not received. For example, resend a new inform communication once every 3 seconds.

   b. In the Number of Retries field, specify the number of times you want to resend the inform communication if it fails. For example, inform communications are resent up to 5 times when the initial communication fails.

4. For both SNMP TRAPS and INFORMS, enter the following as needed and then click OK to apply the settings:

   a. Host name

   b. Port number

   c. User ID for accessing the host -- make sure the User ID has the SNMPv3 permission.

   d. Select the host security level

Security level	Description
"noAuthNoPriv"	Select this if no authorization or privacy protocols are needed.
"authNoPriv"	Select this if authorization is required but no privacy protocols are required. • Select the authentication protocol - MD5 or SHA • Enter the authentication passphrase and then confirm the authentication passphrase
"authPriv"	Select this if authentication and privacy protocols are required. • Select the authentication protocol - MD5 or SHA • Enter the authentication passphrase and confirm the authentication passphrase • Select the Privacy Protocol - DES or AES • Enter the privacy passphrase and then confirm the privacy passphrase

Start or Stop a Lua Script

If you have created or loaded a Lua script file into the Legrand PDU, 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 225).

▶ **To automatically start or stop a Lua script:**

1. Choose Device Settings > Event Rules > **➕ New Action**.
2. Select "Start/stop Lua script" from the Action list.
3. In the Operation field, select Start Script or Stop Script.
4. In the Script field, select the script that you want it to be started or stopped when an event occurs.
   ▪ No script is available if you have not created or loaded it into the Legrand PDU.
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 Outlets

The "Switch outlets" action is available only when your Legrand PDU is outlet-switching capable. This action turns on, off or power cycles a specific outlet.

▶ **Operation:**

1. Choose Device Settings > Event Rules > **➕ New Action**.
2. Select "Switch outlets" from the Action list.
3. In the Operation field, select an operation for the selected outlet(s).

- Turn Outlet On: Turns on the selected outlet(s).
- Turn Outlet Off: Turns off the selected outlet(s).
- Cycle Outlet: Cycles power to the selected outlet(s).

4. To specify the outlet(s) where this action will be applied, select them one by one from the Available Outlets list.
   - To add all outlets, click Select All.
5. To remove any outlets from the Selected Outlets field, click that outlet's ✖.
   - To remove all outlets, click Deselect All.
6. If "Turn Outlet On" or "Cycle Outlet" is selected in step 3, you can choose to select the "Use sequence order and delays" checkbox so that all selected outlets will follow the power-on sequence defined on the page of *Outlets* (on page 100).

Switch Peripheral Actuator

If you have any actuator connected to the Legrand PDU, you can set up the Legrand PDU so it automatically turns on or off the system controlled by the actuator when a specific event occurs.

Note: For information on connecting actuators, see **DX or DX2 Sensor Packages** *(on page 47).*

▶ **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.

Legrand PDU 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 236).

▶ **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.

Transport protocols	Next steps
TCP	NO TLS certificate is required. Type an appropriate port number in the TCP Port field.

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 490).*

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 Legrand PDU 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 196).

▶ **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. [12 : 00 AM] 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 208).
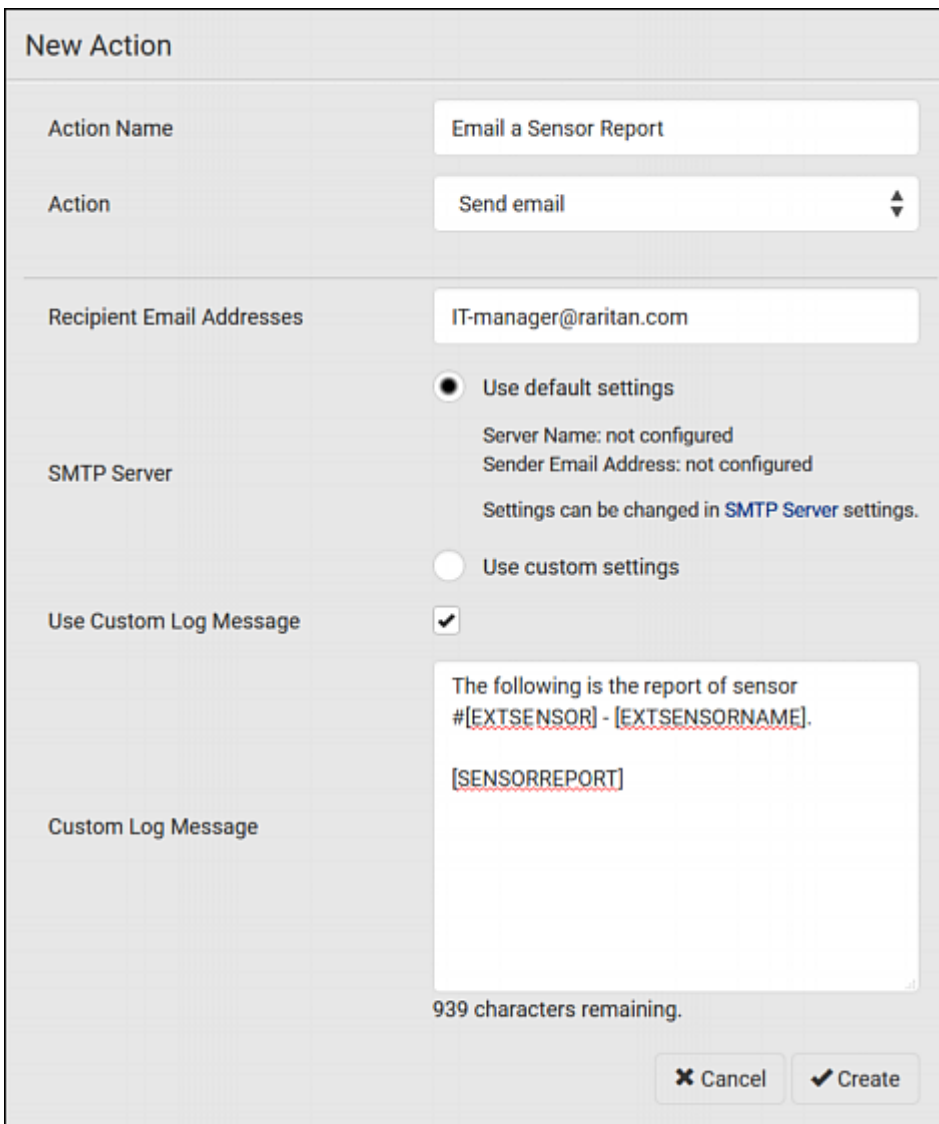
Send Sensor Report Example

To create a scheduled action for emailing a temperature sensor report hourly, it requires:

- A 'Send email' action
- A 'Send sensor report' action
- A timer - that is, the scheduled action

▶ **Steps:**

1. Click ✚ New Action to create a 'Send email' action that sends an email to the desired recipient(s). For details, see **Send Email** (on page 200).
   - In this example, this action is named *Email a Sensor Report.*
   - If intended, you can customize the email messages 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: not configured Sender Email Address: not configured Settings can be changed in SMTP Server settings. ◯ Use custom settings
Use Custom Log Message	✔
Custom Log Message	The following is the report of sensor #[EXTSENSOR] - [EXTSENSORNAME]. [SENSORREPORT] 939 characters remaining.

✖ Cancel   ✔ Create

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 201).
   - In this example, this action is named *Send Temperature Sensor Readings.*

June 2018

- 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 Available -- ⇕
		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 206).

- 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 Legrand PDU will send out an email containing the specified temperature sensor readings hourly every day.

Whenever you want the Legrand PDU to stop sending the temperature report, simply deselect the Enabled checkbox in the timer.

Placeholders for Custom Messages

The action "Send email" allows you to customize event messages. See *Send Email* (on page 200).

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.

June 2018

If wanted, you can resort the list by clicking the desired column header. See *Sorting a List* (on page 86).

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
[ACTIVEINLET]	The label of the newly activated inlet
[AMSBLADESLOTPOSITION]	The (horizontal) slot position, an action applies to
[AMSLEDCOLOR]	The RGB LED color
[AMSLEDMODE]	The LED indication mode
[AMSLEDOPMODE]	The LED operating mode
[AMSNAME]	The name of an asset strip
[AMSNUMBER]	The numeric ID of an asset strip
[AMSRACKUNITPOSITION]	The (vertical) rack unit position, an action applies to
[AMSSTATE]	The human readable state of an asset strip
[AMSTAGID]	The asset tag ID
[CARDREADERID]	The id of a card reader
[CIRCUITCTRATING]	The circuit CT rating
[CIRCUITCURRENTRATING]	The circuit current rating
[CIRCUITNAME]	The circuit name
[CIRCUITPOLE]	The circuit power line identifier
[CIRCUITSENSOR]	The circuit sensor name
[CIRCUIT]	The circuit identifier
[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
[EXTSENSORNAME]	The name of a peripheral device
[EXTSENSORSLOT]	The ID of a peripheral device slot
[EXTSENSOR]	The peripheral device identifier
[IFNAME]	The human readable name of a network interface
[INLETPOLE]	The inlet power line identifier
[INLETSENSOR]	The inlet sensor name
[INLET]	The power inlet label

Placeholder	Definition
[ISASSERTED]	Boolean flag whether an event condition became true (1) or false (0)
[LDAPERRORDESC]	An LDAP error occurred
[LHXFANID]	The ID of a fan connected to an LHX/SHX
[LHXPOWERSUPPLYID]	The ID of an LHX/SHX power supply
[LHXSENSORID]	The ID of an LHX/SHX sensor probe
[LOGMESSAGE]	The original log message
[MONITOREDHOST]	The name or IP address of a monitored host
[OCPSENSOR]	The overcurrent protector sensor name
[OCP]	The overcurrent protector label
[OLDVERSION]	The firmware version the device is being upgraded from
[OUTLETNAME]	The outlet name
	Note: If any outlet does not have a name, neither an outlet name nor an outlet number will be shown in the custom message for it. Therefore, it is recommended to check the availability of all outlet names if intending to use this placeholder.
[OUTLETPOLE]	The outlet power line identifier
[OUTLETSENSOR]	The outlet sensor name
[OUTLET]	The outlet label
[PDUPOLESENSOR]	The sensor name for a certain power line
[PDUSENSOR]	The PDU sensor name
[PERIPHDEVPOSITION]	The position of an attached peripheral device
[PHONENUMBER]	The phone number an SMS was sent to
[PORTID]	The label of the external port, the event triggering device is connected to
[PORTTYPE]	The type of the external port (for example, 'feature' or 'auxiliary'), the event triggering device is connected to
[POWERMETERPOLE]	The PMC power meter line identifier
[POWERMETERSENSOR]	The PMC power meter sensor name
[POWERMETER]	The PMC power meter ID
[RADIUSERRORDESC]	A Radius error occurred
[ROMCODE]	The rom code of an attached peripheral device
[SENSORREADINGUNIT]	The unit of a sensor reading
[SENSORREADING]	The value of a sensor reading
[SENSORREPORT]	The formatted sensor report contents
[SENSORSTATENAME]	The human readable state of a sensor

Placeholder	Definition
[SENSORTHRESHOLDNAME]	The name of the threshold being crossed
[SENSORTHRESHOLDVALUE]	The value of the threshold being crossed
[SMARTCARDID]	The id of a smart card
[SMARTCARDTYPE]	The type of a smart card
[SMTPRECIPIENTS]	The list of recipients, an SMTP message was sent to
[SMTPSERVER]	The name or IP address of an SMTP server
[SYSCONTACT]	SysContact as configured for SNMP
[SYSLOCATION]	SysLocation as configured for SNMP
[SYSNAME]	SysName as configured for SNMP
[TIMEREVENTID]	The id of a timer event
[TIMESTAMP]	The timestamp of the event occurrence
[TRANSFERSWITCHREASON]	The transfer reason
[TRANSFERSWITCHSENSOR]	The transfer switch sensor name
[TRANSFERSWITCH]	The transfer switch label
[UMTARGETROLE]	The name of a user management role, an action was applied on
[UMTARGETUSER]	The user, an action was triggered for
[USERIP]	The IP address, a user connected from
[USERNAME]	The user who triggered an action
[VERSION]	The firmware version the device is upgrading to

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. Besides, you cannot delete built-in rules and actions. See **Built-in Rules and Rule Configuration** *(on page 185) or* **Available Actions** *(on page 196).*

▶ **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 PDU-Level Event Rule
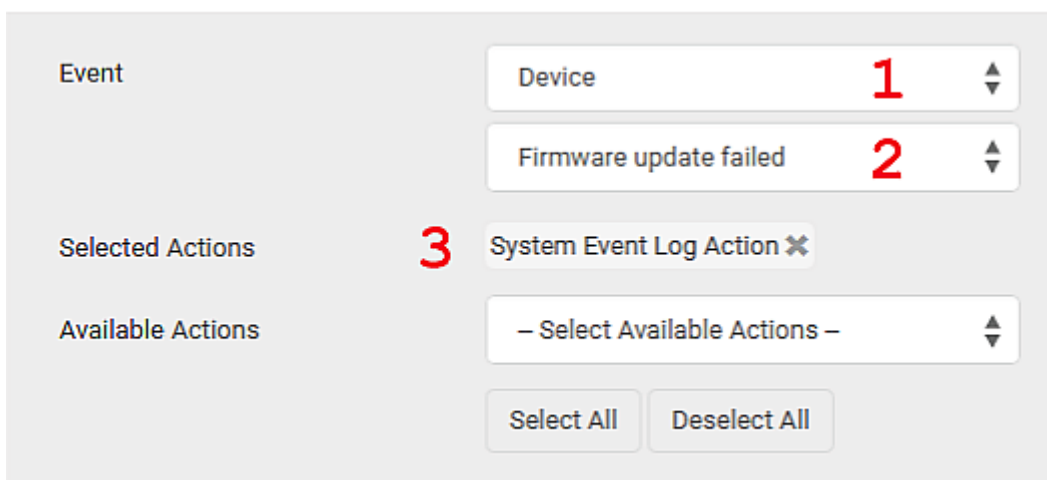
In this example, we want the Legrand PDU to record the firmware upgrade failure in the internal log when it happens.

The event rule involves:

- Event: Device > Firmware update failed
- Action: System Event Log Action

▶ **To create this PDU-level event rule:**

1. For an event at the PDU level, select "Device" in the Event field.

2. Select "Firmware update failed" so that the Legrand PDU responds to the event related to firmware upgrade failure.

3. To make the Legrand PDU record the firmware update failure event in the internal log, select "System Event Log Action" in the Available Actions field.

Event		Device	**1**	▲▼
		Firmware update failed	**2**	▲▼
Selected Actions	**3**	System Event Log Action ✖		
Available Actions		– Select Available Actions –		▲▼
		Select All	Deselect All	

Sample Outlet-Level Event Rule

In this example, we want the Legrand PDU to send SNMP notifications to the SNMP manager for any sensor change event of outlet 3.

The event rule involves:

- Event: Outlet > Outlet 3 > Sensor > Any sub-event
- Action: System SNMP Notification Action

▶ **To create this outlet-level event rule:**

1. For an event at the outlet level, select "Outlet" in the Event field.

2. Select "Outlet 3" because that is the desired outlet.

3. Select "Sensor" to refer to sensor-related events.

4. Select "Any sub-event" to include all events related to all sensors of this outlet and all thresholds, such as current, voltage, upper critical threshold, upper warning threshold, lower critical threshold, lower warning threshold, and so on.

5. To make the Legrand PDU send SNMP notifications, select "System SNMP Notification Action" in the Available Actions field.

Note: The SNMP notifications may be SNMP v2c or SNMP v3 traps/informs, depending on the settings for the System SNMP Notification Action. See **Enabling and Configuring SNMP** *(on page 262).*

Then the SNMP notifications are sent when:

- Any numeric sensor's reading enters the warning or critical range.
- Any sensor reading or state returns to normal.
- Any sensor becomes unavailable.
- The active energy sensor is reset.
- Any state sensor changes its state.

For example, when the outlet 3's voltage exceeds the upper warning threshold, the SNMP notifications are sent, and when the voltage drops below the upper warning threshold, the SNMP notifications are sent again.

Sample Inlet-Level Event Rule

In this example, we want the Legrand PDU to send SNMP notifications to the SNMP manager for any sensor change event of the Inlet I1.

The event rule involves:

- Event: Inlet > Sensor > Any sub-event
- Action: System SNMP Notification Action

▶ **To create the above event rule:**

1. For an event at the inlet level, select "Inlet" in the Event field.
2. Select "Sensor" to refer to sensor-related events.
3. Select "Any sub-event" to include all events related to all sensors of this inlet and all thresholds, such as current, voltage, upper critical threshold, upper warning threshold, lower critical threshold, lower warning threshold, and so on.
4. To make the Legrand PDU send SNMP notifications, select "System SNMP Notification Action" in the Available Actions box.

June 2018

Note: The SNMP notifications may be SNMP v2c or SNMP v3 traps/informs, depending on the settings for the System SNMP Notification Action. See **Enabling and Configuring SNMP** *(on page 262).*

Event	Inlet	1
	Sensor	2
	\<Any sub-event\>	3
Selected Actions	4 System SNMP Notification Action ✖	
Available Actions	– Select Available Actions –	
	Select All Deselect All	

Then the SNMP notifications are sent when:

- Any numeric sensor's reading enters the warning or critical range.
- Any sensor reading or state returns to normal.
- Any sensor becomes unavailable.
- The active energy sensor is reset.

For example, when the Inlet I1's voltage exceeds the upper warning threshold, the SNMP notifications are sent, and when the voltage drops below the upper warning threshold, the SNMP notifications are sent again.

Sample Environmental-Sensor-Level Event Rule

This section applies to outlet-switching capable models only.

In this example, we want Legrand PDU to activate the load shedding function 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 activating the load shedding**

1. Choose Device Settings > Event Rules > ➕ New Action.
2. In this illustration, assign the name "Activate Load Shedding" to the new action.
3. In the Action field, select "Change load shedding state."

4. In the Operation field, select Start Load Shedding.

5. Click Create to finish the creation.

After the new action is created, follow the procedure below to create an event rule that triggers the load shedding mode 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: Activate Load Shedding

▶ **Step 2: create the contact closure-triggered load shedding event rule**

1. Click ✚ New Rule on the Event Rules page.

2. In this illustration, assign the name "Contact Closure Triggered Load Shedding" 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 116).*

5. Select "State Sensor/Actuator" because the contact closure sensor is a state sensor.

6. Select "Alarmed" since we want the Legrand PDU 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 "Activate Load Shedding" from the Available Actions list.

A Note about Infinite Loop

You should avoid building an infinite loop when creating event rules.

The infinite loop refers to a condition where the Legrand PDU 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 Legrand PDU 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 Legrand PDU 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

June 2018

Example 3

This example illustrates a situation where two event rules combined regarding the outlet state changes causes the Legrand PDU to continuously power cycle outlets 1 and 2 in turn.

Event selected	Action included
Outlet > Outlet 1 > Sensor > Outlet State > On/Off > Both (trigger condition)	Cycle Outlet 2 (Switch outlets --> Cycle Outlet --> Outlet 2)
Outlet > Outlet 2 > Sensor > Outlet State > On/Off > Both (trigger condition)	Cycle Outlet 1 (Switch outlets --> Cycle Outlet --> Outlet 1)

A Note about Untriggered Rules

In some cases, a measurement exceeds a threshold causing the Legrand PDU to generate an alert. The measurement then returns to a value within the threshold, but the Legrand PDU does not generate an alert message for the Deassertion event. Such scenarios can occur due to the hysteresis tracking the Legrand PDU uses. See **"To De-assert" and Deassertion Hysteresis** (on page 477).

Setting Data Logging

The Legrand PDU 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 Legrand PDU 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 Legrand PDU device's SNMP agent must be enabled for this feature to work. See **Enabling and Configuring SNMP** *(on page 262). 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 Legrand PDU, it is NOT recommended to do so.

Configuring Data Push Settings

You can push the sensor log to a remote server for data synchronization. The data will be sent in JSON format using HTTP POST requests. You need to set up the destination and authentication for data push on the Legrand PDU.

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 184).
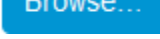
▶ **To configure data push settings:**

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 490).*

5. If the destination server requires authentication, select the Use Authentication checkbox, and enter the following data.

   - User name
   - Password

6. In the Entry Type field, determine the data that will be transmitted.

   - Asset management tag list: Transmit the information of the specified asset strip(s), including the general status of the specified strip(s) and a list of asset tags. The asset tags list also includes those on blade extension strips, if any.
   - Asset management log: Transmit the log of all asset strips, which is generated when there are changes made to asset tags and asset strips, including asset tag connection or disconnection events.
   - Sensor log: Transmit the record of all logged sensors, including their sensor readings and/or status. Logged sensors refer to all internal and/or environmental sensors/actuators that you have selected on the Data Logging page. See **Setting Data Logging** (on page 219).

Note: Legrand PDU does NOT support asset management strips so you can ignore asset management-related data.

7. Click Create.

8. Repeat the same steps for additional destinations.

▶ **To modify or delete data push settings:**

1. On the Data Push page, click the one you want in the list.

2. Perform either action below.

- ▪ To modify settings, make necessary changes and then click Save.
- ▪ To delete it, click 🗑 Delete, and then confirm it on the confirmation message.

Monitoring Server Accessibility

You can monitor whether specific IT devices are alive by having the Legrand PDU 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.

Legrand PDU can monitor the accessibility of any IT device, such as database servers, remote authentication servers, power distribution units (PDUs), and so on. It supports monitoring a maximum of 8 devices.

The default ping settings may not be suitable for monitoring devices that require high connection reliability so it is strongly recommended that you should adjust the ping settings for optimal results.

*Tip: To make the Legrand PDU 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 184). An example is available in **Example: Ping Monitoring and SNMP Notifications** (on page 222).*

▶ **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).
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 Legrand PDU resumes pinging after the monitored equipment is declared "Unreachable." Valid range is 1 to 1200 (seconds).

Field	Description
Number of consecutive failures before disabling feature (0 = unlimited)	The number of times the monitored equipment is declared "Unreachable" consecutively before the Legrand PDU disables the ping monitoring feature for it and shows "Waiting for reliable connection." Valid range is 0 to 100.

5. Click Create.
6. To add more IT devices, repeat the same steps.

In the beginning, the status of the added IT equipment shows "Waiting for reliable connection," which means the requested number of consecutive successful or unsuccessful pings has not reached before Legrand PDU can declare that the monitored device is reachable or unreachable.

▶ **To check the server monitoring states and results:**

1. After adding IT equipment for monitoring, all IT devices are listed on the Server Reachability page.
2. The column labeled "Ping Enabled" indicates whether the monitoring for the corresponding IT device is activated or not.
3. The column labeled "Status" indicates the accessibility of monitored equipment.

Status	Description
Reachable	The monitored equipment is accessible.
Unreachable	The monitored equipment is inaccessible.
Waiting for reliable connection	The connection between the Legrand PDU 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 221).
   - To delete it, click 🗑 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 Legrand PDU to make sure that PDU is properly operating all the time, and the Legrand PDU 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 Legrand PDU 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 Legrand PDU 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 Legrand PDU 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 Legrand PDU stop pinging the target PDU for 60 seconds (1 minute) after the PDU inaccessibility is declared, enter the following data. After 60 seconds, the Legrand PDU 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 Legrand PDU 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 213).*

Front Panel Settings

You can set up the default mode of the front panel display, and front panel functions for outlet switching or actuator control.

Note that available front panel settings are model dependent.

- Outlet switching -- available on outlet-switching capable models only. That is, Legrand Switched PDUs.
- Actuator control -- available on all models.
- Default front panel mode setup -- available on all models.

▶ **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 58).*

Mode	Data entered
Automatic mode	The LCD display cycles through both the inlet and overcurrent protector information. This is the default.
	Overcurrent protector information is available only when you Legrand PDU has overcurrent protectors.
Inlet overview	The LCD display cycles through the inlet information only.

   ▪ To enable the front panel outlet-switching function, select the "Outlet switching" checkbox.
   ▪ To enable the front panel actuator-control function, select the "Peripheral actuator control" checkbox.
   ▪ Now you can turn on or off outlets/actuators by operating the front panel. See **Power Control** (on page 66) and **Peripherals** (on page 67).

Configuring the Serial Port

You can change the bit rate of the serial port labeled CONSOLE on the Legrand PDU. The default bit rate for console operation is 115200 bps.

The Legrand PDU supports using the following devices via the serial interface:

- A computer for console management.
- A Raritan serial access product -- see **Connection to Raritan Serial Access Products** (on page 496)

You can set diverse bit-rate settings for console operations. Usually the Legrand PDU can detect the device type, and automatically apply the preset bit rate.

The Legrand PDU will indicate the detected device in the Port State section of the Serial Port page.

▶ **To change the serial port's baud rate settings:**

1. To configure serial port settings, choose Device Settings > Serial Port.
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 Legrand PDU, leave it at the default (115200 bps).

Lua Scripts

If you can write or obtain any Lua scripts, you can create or load them into the Legrand PDU to control its behaviors.

Legrand also provides some Lua scripts examples, which you can load as needed.

Note: Not all Legrand Lua script examples can apply to your Legrand PDU model. You should read each example's introduction before applying them.
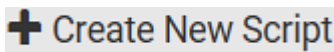
You must have the Administrator Privileges to manage Lua scripts.

Writing or Loading a Lua Script

You can enter or load up to 4 scripts to the Legrand PDU.

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 228).*

▶ **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 (-)
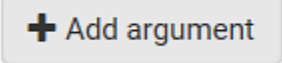
   Note: Spaces are NOT permitted.
3. Determine whether and when to automatically execute the loaded script.

Checkbox	Behavior when selected
Start automatically at system boot	Whenever the Legrand PDU 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 226) or* **Start or Stop a Lua Script** *(on page 204).*
5. In the Source Code section, do one of the following. It is recommended to leave the Enable Syntax Highlighting checkbox selected unless you do not need different text colors to identify diverse code syntaxes.

- To write a Lua script, type the codes in the Source Code section.
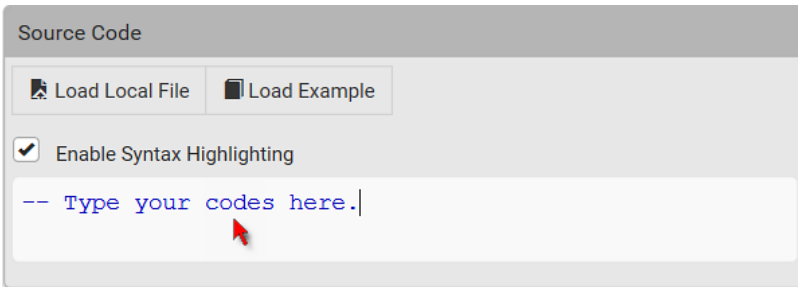
- To load an existing Lua script file, click Load Local File.
- To use one of Legrand's Lua script examples, click Load Example.

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 Legrand'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 226).
- 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 84), and then repeat the above steps.
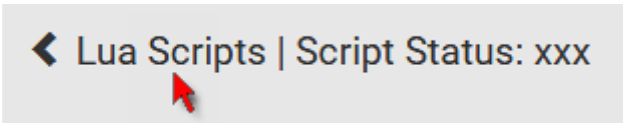
Manually Starting or Stopping a Script

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 Legrand PDU automatically start or stop a script in response to an event, create an event rule. See **Event Rules and Actions** *(on page 184) and* **Start or Stop a Lua Script** *(on page 204).*

▶ **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 228).

3. To start with default arguments, click ▶ Start.

To start with new arguments, click ⋮ > Start with Arguments. Newly-assigned arguments will override default ones.

4. If you chose "Start with Arguments" in the above step, enter the key and value in the Start Lua Script dialog.

- Click **➕ Add argument** if needing additional arguments.

Start Lua Script

Key	Value	
		—

➕ Add Argument

Cancel   Start

5. Click Start.
6. The script output will be shown in the Script Output section.

- If needed, click **🗑 Clear** to delete the existing output data.

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 228).
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
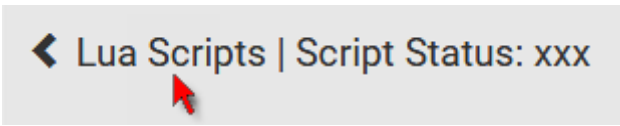
•   Or click "Lua Scripts" in the *Menu* (on page 84).

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 225).

▶   **Restart:**

This column indicates whether the checkbox labeled "Restart after termination" is enabled. See *Writing or Loading a Lua Script* (on page 225).

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 Legrand PDU.

▶   **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.

June 2018

- 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
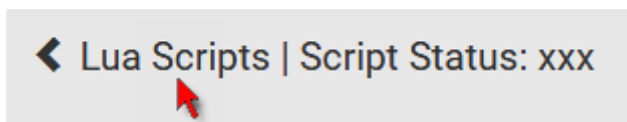
- Or click "Lua Scripts" in the *Menu* (on page 84).

Miscellaneous

By default, the Schroff LHX/SHX heat exchanger support and Cisco EnergyWise feature implemented on the Legrand PDU are disabled.

However, Legrand PDU does NOT support Schroff LHX/SHX so you can ignore the checkbox for this device.

If a Cisco® EnergyWise energy management architecture is implemented in your place, you can enable the Cisco EnergyWise endpoint implemented on the Legrand PDU so that this Legrand PDU becomes part of the Cisco EnergyWise domain.

▶ **To set the Cisco EnergyWise configuration:**

1. Choose Device Settings > Miscellaneous.
2. Select the Enable EnergyWise checkbox.
3. Configure the following:

| Field	Description
Domain name	Type the name of a Cisco EnergyWise domain where the Legrand PDU belongs ▪ Up to 127 printable ASCII characters are permitted. ▪ Spaces and asterisks are NOT acceptable.
Domain password	Type the authentication password (secret) for entering the Cisco EnergyWise domain ▪ Up to 127 printable ASCII characters are permitted. ▪ Spaces and asterisks are NOT acceptable.
Port	Type a User Datagram Protocol (UDP) port number for communications in the Cisco EnergyWise domain. ▪ Range from 1 to 65535. ▪ Default is 43440.
Polling interval	Type a polling interval to determine how often the Legrand PDU is queried in the Cisco EnergyWise domain. ▪ Range from 30 to 600 ms. ▪ Default is 180 ms.

4. Click Save in the *EnergyWise* section.

Maintenance

Click 'Maintenance' in the **Menu** (on page 84), and the following submenu displays.
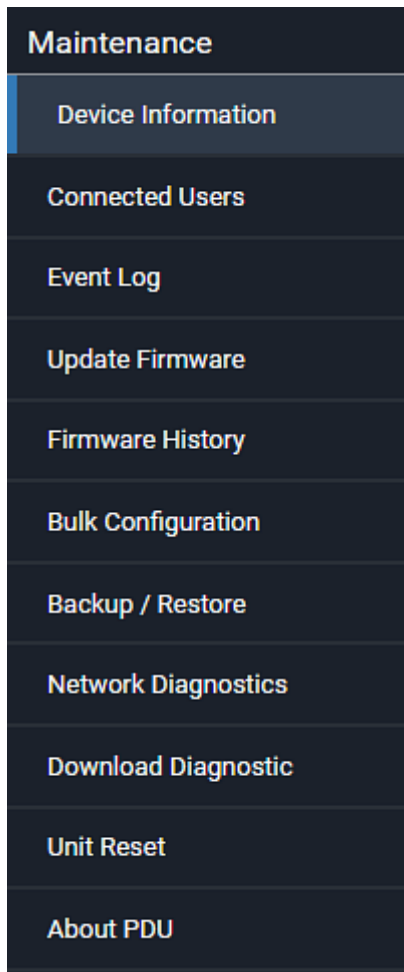
Submenu command	Refer to...
Device Information	**Device Information** (on page 231)
Connected Users	**Viewing Connected Users** (on page 235)
Event Log	**Viewing or Clearing the Local Event Log** (on page 236)
Update Firmware	**Updating the Legrand PDU Firmware** (on page 237)
Firmware History	**Viewing Firmware Update History** (on page 238)
Bulk Configuration	**Bulk Configuration** (on page 239)
Backup/Restore	**Backup and Restore of Device Settings** (on page 243)
Network Diagnostic	**Network Diagnostics** (on page 244)
Download Diagnostic	**Downloading Diagnostic Information** (on page 245)
Unit Reset	▪ **Rebooting the Legrand PDU** (on page 245) ▪ **Resetting All Settings to Factory Defaults** (on page 246)
About PDU	**Retrieving Software Packages Information** (on page 246)

Device Information

Using the web interface, you can retrieve hardware and software information of components or peripheral devices connected to your Legrand PDU.

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	⌃
Product Name	LP-61100
Serial Number	1LV1234567
Rating	100-120V, 12A, 1.2-1.4kVA, 50/60Hz
Device MAC Address	00:0d:5d:0e:e1:a6
Firmware Version	3.4.10.5-44599
Board ID	1371234567
Board Revision	0x14
PDU2-MIB	download
ASSETMANAGEMENT-MIB	download
Network	⌄
Port Forwarding	⌄
Outlets	⌄
Controllers	⌄
Peripheral Devices	⌄

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.
Network	The network information, such as the current networking mode, IPv4 and/or IPv6 addresses and so on.
	This tab also indicates whether the Legrand PDU is part of a cascading configuration. See *Identifying Cascaded Devices* (on page 232).

Section title	Information shown
Port Forwarding	If the port forwarding mode is activated, this section will show a list of port numbers for all cascaded devices.
Outlets	Each outlet's receptacle type, operating voltage and rated current.
Overcurrent Protectors	Each overcurrent protector's type, rated current and the outlets that it protects.
Controllers	Each inlet or outlet controller's serial number, board ID, firmware version and hardware version.
Inlets	Each inlet's plug type, rated voltage and current.
Peripheral Devices	Serial numbers, model names, position and firmware-related information of connected Raritan's environmental sensor packages.

Identifying Cascaded Devices

For information on how to cascade Legrand PDUs, see *Cascading Multiple Legrand PDUs for Sharing Ethernet Connectivity* (on page 32).

This section explains how to identify a cascaded device on the Device Information page.

Note: For detailed information on the cascading configuration and restrictions, refer to the Cascading Guide, *which is available from the Legrand PDU section of Raritan website's* **Support page** *(***http://www.raritan.com/support/***).*

► **To identify the cascading status:**
1. Choose Maintenance > Device Information.
2. Click the Network title bar.

- ▪ If the information shown on this page does not match the latest status, press F5 to reload it.

► **Cascading information in the Bridging mode:**
- The Common section contains two read-only fields for indicating the cascading status. Note that the cascading position is NOT available in the Bridging mode.

Fields	Description
Port Forwarding	Indicates the Port Forwarding is disabled. See *Setting the Cascading Mode* (on page 150).
BRIDGE section	Indicates the device is in the Bridging mode and its IP address.

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 BRIDGE default via 192.168.84.254 (BRIDGE)
IPv6 Routes	none
Port Forwarding	disabled

BRIDGE

IPv4 Address	192.168.84.110/24

▶ **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 150).
Cascade Position	Indicates the position of the Legrand PDU 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

▪ 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.

Network	∧
Common	
DNS Servers	192.168.80.249, 192.168.80.19
DNS Suffixes	rgp.raritan.com.
DNS Resolver Preference	IPv6 Address
Port Forwarding	enabled
Cascade Position	2 (Slave)
Cascaded Device Connected	no

• For a list of port numbers required for accessing each cascaded device in the Port Forwarding mode, click the Port Forwarding title bar on the same page.

Port Forwarding	∨

Viewing Connected Users

You can check which users have logged in to the Legrand PDU and their status. If you have administrator privileges, you can terminate any user's connection to the Legrand PDU.

▶ **To view and manage connected users:**

1. Choose Maintenance > Connected Users. A list of logged-in users displays.

Connected Users				
User name ▲	**IP Adress**	**Client Type**	**Idle Time**	
admin	192.168.84.18	Web GUI	0 min	Disconnect
Mary	192.168.78.77	Web GUI	0 min	Disconnect

If wanted, you can resort the list by clicking the desired column header. See ***Sorting a List*** (on page 86).

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 Legrand PDU.
	 ▪ 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>	192.168.84.14	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 247).

Viewing or Clearing the Local Event Log

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

You can view over 2000 historical events that occurred on the Legrand PDU 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 Legrand PDU web interface are automatically converted to your computer's time zone. To avoid any time confusion, you can apply the same time zone settings as those of Legrand PDU to your computer.

   - 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.

   Filter Event Class: Any

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.

4. 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

5. If wanted, you can resort the list by clicking the desired column header. See ***Sorting a List*** (on page 86).

▶ **To clear the local log:**

1. Click **🗑 Clear Log** on the top-right corner.

2. Click Clear Log on the confirmation message.

Updating the Legrand PDU Firmware

Firmware files are available on the Legrand PDU section of Raritan website's *Support page* (*http://www.raritan.com/support/*).

When performing the firmware upgrade, the Legrand PDU keeps each outlet's power status unchanged so no server operation is interrupted. During and after the firmware upgrade, outlets that have been powered on prior to the firmware upgrade remain powered ON and outlets that have been powered off remain powered OFF.

You must be the administrator or a user with the Firmware Update permission to update the Legrand PDU firmware.

Before starting the upgrade, read the release notes downloaded from the Legrand PDU section of Raritan website's *Support page* (*http://www.raritan.com/support/*). If you have any questions or concerns about the upgrade, contact Legrand 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.

▶ **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 Legrand PDU 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 76).
   ▪ No users can successfully log in to the Legrand PDU.
   ▪ Other users' operation, if any, is forced to suspend.

7. When the update is complete, the Legrand PDU 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 Legrand PDU 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 262).**

▶ **Alternatives:**

To use a different method to update the firmware, refer to:

- *Firmware Update via SCP* (on page 393)
- *Bulk Configuration or Firmware Upgrade via DHCP/TFTP* (on page 411)
- *Firmware Upgrade via USB* (on page 410)

A Note about Firmware Upgrade Time

The PDU firmware upgrade time varies from unit to unit, depending on various external and internal factors.

External factors include, but are not limited to: network throughput, firmware file size, and speed at which the firmware is retrieved from the storage location. Internal factors include: the necessity of upgrading the firmware on the microcontroller and the number of microcontrollers that require upgrade (which depends on the number of outlets). The microcontroller is upgraded only when required. Therefore, the length of firmware upgrade time ranges from approximately 3 minutes (without any microcontroller updated) to almost 7 minutes (with all microcontrollers for 48 outlets updated). Take the above factors into account when estimating the PDU's firmware upgrade time.

The time indicated in this note is for Legrand PDU web-interface-based upgrades. Upgrades through other management systems, such as Sunbird's Power IQ, may take additional time beyond the control of the PDU itself. This note does not address the upgrades using other management systems.

Full Disaster Recovery

For Legrand, disaster recovery can be performed via the USB connection only.

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

Contact Legrand Technical Support for the recovery utility, which works in Windows XP/Vista/7/10 and Linux. In addition, an appropriate Legrand PDU firmware file is required in the recovery procedure.

Viewing Firmware Update History

The firmware upgrade history is permanently stored on the Legrand PDU. 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 86).

Bulk Configuration

The Bulk Configuration feature lets you save generic settings of a configured Legrand PDU device to your computer. You can use this configuration file to copy common settings to other Legrand PDUs of the same model and firmware version. See **Bulk Configuration Restrictions** (on page 240).

A source device is the Legrand PDU device where the configuration file is downloaded/saved. A target device is the Legrand PDU 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 490).

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 243).*

▶ **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 240).
2. Perform the bulk configuration operation, which includes the following steps. For details, see **Performing Bulk Configuration** (on page 241).
   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, Legrand PDU 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 Legrand PDU, the last record similar to the following is displayed at the bottom of both the Bulk Configuration and Backup/Restore pages.

Last Restore: 10/18/2017, 8:33:38 PM GMT+0800, Status: OK

Tip: The date and time shown on the Legrand PDU web interface are automatically converted to your computer's time zone. To avoid any time confusion, you can apply the same time zone settings as those of Legrand PDU to your computer.

▶ **Alternatives:**

To use a different bulk configuration method, refer to:

- **Bulk Configuration via SCP** (on page 393)
- **Bulk Configuration or Firmware Upgrade via DHCP/TFTP** (on page 411)
- **Configuration or Firmware Upgrade with a USB Drive** (on page 402)

Bulk Configuration Restrictions

Before performing bulk configuration, make sure your source and target devices are compatible devices for sharing general settings.

▶ **Restrictions for bulk configuration:**

- The target device must be running the same firmware version as the source device.
- The target device must be of the same model type as the source device.
- Bulk configuration is permitted if the differences between the target and source devices are only "mechanical" designs, such as the length or color of the power cord, the line cord's plug type, or the color of the PDU's chassis.

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 Legrand PDU, whose settings you want to download.
2. Choose Maintenance > Bulk Configuration.
3. Click ![icon] 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 functions as the default one.
6. Now decide which settings are wanted and which are not.

   a. Click ![icon] 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.

Option	Description
Built In	The setting will follow the same setting of Legrand'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.

Bulk Profiles

# ▲	Name	Description	Default Profile
1	Built in		✔
2	custom-1	No network settings copied	
3	custom-2	No user settings copied	

▶ **Step 1: Select the desired bulk configuration profile (optional)**

1. Log in to the source Legrand PDU, 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.
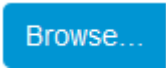
1. Log in to the source Legrand PDU if you have not yet.
2. Choose Maintenance > Bulk Configuration.
3. Check the Bulk Format field. If the chosen value does not match your need, change it.

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 Legrand PDU, which is of the same model and runs the same firmware as the source Legrand PDU.
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 Legrand PDU resets and the login page re-appears.

▶ **Alternatives:**

To use a different bulk configuration method, refer to:

- *Bulk Configuration via SCP* (on page 393)
- *Bulk Configuration or Firmware Upgrade via DHCP/TFTP* (on page 411)
- *Configuration or Firmware Upgrade with a USB Drive* (on page 402)

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.

✔	# ▲	Name
☐	1	Built in
☐	2	custom-1
☐	3	custom-2

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 Legrand PDU, you should perform the Backup/Restore feature.

All Legrand PDU 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 Legrand PDUs, use the Bulk Configuration feature instead. See **Bulk Configuration** *(on page 239).*

▶ **To download a backup Legrand PDU 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 Legrand PDU 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 Legrand PDU resets and the Login page re-appears, indicating that the restore is complete.

Note: On startup, Legrand PDU 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 Legrand PDU, the last record similar to the following is displayed at the bottom of both the Bulk Configuration and Backup/Restore pages.

Last Restore: 10/18/2017, 8:33:38 PM GMT+0800, Status: OK

► **Alternative:**

To use a different method to perform backup/restore, refer to:

● ***Backup and Restore via SCP*** (on page 394)

Network Diagnostics

Legrand PDU 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 389).*

Choose Maintenance > Network Diagnostics, and then perform any function below.

► **Ping:**

1. Type values in the following fields.

Field	Description
Network Host	The name or IP address of the host that you want to check.
Number of Requests	A number up to 20. This determines how many packets are sent for pinging the host.

2. Click Run Ping to ping the host. The Ping results are then displayed.

► **Trace Route:**

1. Type values in the following fields.

Field/setting	Description
Host Name	The IP address or name of the host whose route you want to check.
Timeout(s)	A timeout value in seconds to end the trace route operation.
Use ICMP Packets	To use the Internet Control Message Protocol (ICMP) packets to perform the trace route command, select this checkbox.

2. Click Run. The Trace Route results are then displayed.

▶ **List TCP Connections:**

1. Click the List TCP Connections title bar to show the list.
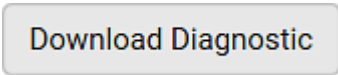
Downloading Diagnostic Information

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

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

This feature is accessible only by users with Administrative Privileges or Unrestricted View Privileges.

▶ **To retrieve a diagnostic file:**

1. Choose Maintenance > Download Diagnostic > [Download Diagnostic].
2. The system prompts you to save or open the file. Save the file then.
3. E-mail this file as instructed by Legrand Technical Support.
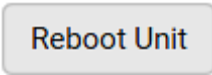
Rebooting the Legrand PDU

You can remotely reboot the Legrand PDU via the web interface.
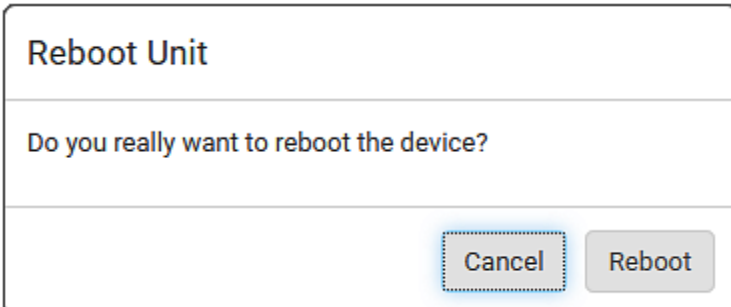
Resetting the Legrand PDU does not interrupt the operation of connected servers because there is no loss of power to outlets. During and after the reboot, outlets that have been powered on prior to the reboot remain powered on, and outlets that have been powered off remain powered off.

Warning: Rebooting the Legrand PDU deletes all webcam snapshots that are saved onto the Legrand PDU locally. If needed, download important snapshots before rebooting the device. See *Viewing and Managing Locally-Saved Snapshots* (on page 253).

▶ **To reboot the device:**

1. Choose Maintenance > Unit Reset > [Reboot Unit].

Reboot Unit

Do you really want to reboot the device?

[Cancel] [Reboot]

2. Click Reboot to restart the Legrand PDU.
3. A message appears, with a countdown timer showing the remaining time of the operation. It takes about one minute to complete.
4. When the restart is complete, the login page opens.

Note: If you are not redirected to the login page after the restart is complete, click the text "this link" in the countdown message.
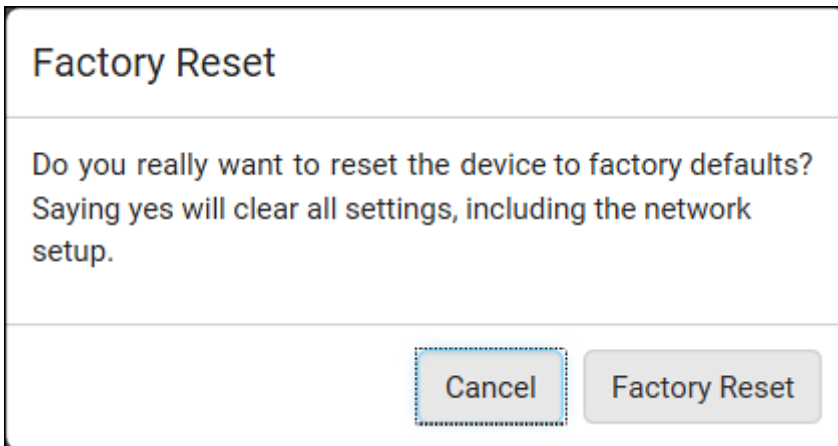
Resetting All Settings to Factory Defaults

You must have the Administrator Privileges to reset all settings of the Legrand PDU to factory defaults.

Important: Exercise caution before resetting the Legrand PDU to its factory defaults. This erases existing information and customized settings, such as user profiles, threshold values, and so on. Only active energy data and firmware upgrade history are retained.

▶ **To reset the device to factory defaults:**

1. Choose Maintenance > Unit Reset > [Reset to Factory Defaults] .

```
Factory Reset

Do you really want to reset the device to factory defaults?
Saying yes will clear all settings, including the network
setup.

        [ Cancel ]   [ Factory Reset ]
```

2. Click Factory Reset to reset the Legrand PDU to factory defaults.
3. A message appears, with a countdown timer showing the remaining time of the operation. It takes about two minutes to complete.
4. When the reset is complete, the login page opens.

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

▶ **Alternative:**

There are two more methods to reset the device to factory defaults.

*   Use the "mechanical" reset button
*   Perform the CLI command

For details, see ***Resetting to Factory Defaults*** (on page 429).

Retrieving Software Packages Information

You can check the current firmware version and the information of all open source packages embedded in the Legrand PDU through the web interface.

▶ **To retrieve the embedded software packages information:**

1. Choose Maintenance > About PDU. 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 Legrand PDU, or when there are snapshots saved onto the Legrand PDU already. See *Connecting a Logitech Webcam* (on page 54).
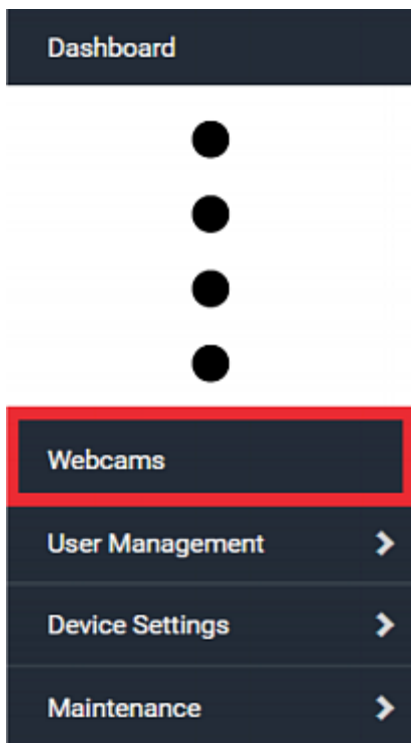
With a Logitech® webcam connected to the Legrand PDU, you can visually monitor the environment around the Legrand PDU via snapshots or videos captured by the webcam.

▶ **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 Legrand PDU or a remote server	▪ **Configuring Webcams and Viewing Live Images** (on page 248) ▪ **Changing Storage Settings** (on page 254)
Send a snapshot or video session's link to other people via email or instant message	**Sending Links to Snapshots or Videos** (on page 251)
Create event rules to trigger emails containing snapshots from a webcam	**Available Actions** (on page 196)

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 84). 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*.

Webcams			
Name ▲	Location	Resolution	Mode
Webcam		352x288	Snapshot

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 Legrand PDU web interface are automatically converted to your computer's time zone. To avoid any time confusion, you can apply the same time zone settings as those of Legrand PDU to your computer.

2. To save the current image onto Legrand PDU or a remote server, click

.
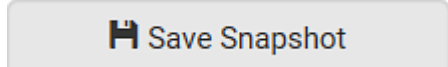
- The default storage location for snapshots is the Legrand PDU device. To save them onto a remote server, see *Changing Storage Settings* (on page 254).
- To download an image onto your computer, move your mouse to that image, right click on it, and choose Save Image As.

3. To have the same live session displayed in a separate window, click

.
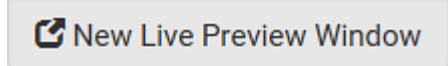
- A separate window appears, which is called the Primary Standalone Live Preview window in this User Guide.
- You can send out this window's URL to share the live image with others. See *Sending Links to Snapshots or Videos* (on page 251).

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.
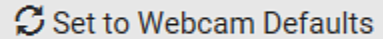
▶ **Image Controls:**

1. Click the Image Controls title bar to expand it.

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 $\boxed{C \text{ Set to Webcam Defaults}}$.

▶ **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 254) and ***Identifying Snapshots Folders on Remote Servers*** (on page 256).

  ▪ 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, Legrand PDU 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 Legrand PDU 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.

❮ Webcam Management | Webcam
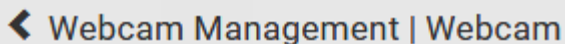
● Or click Webcams again in the ***Menu*** (on page 84).

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 235).*

▶ **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 252).

▶ **To send a snapshot or video link via email or instant message:**

1. Choose Webcams in the **Menu** (on page 84).
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 248).
4. Copy the URL from that live preview window.

a. Select the URL shown on the top of the image.
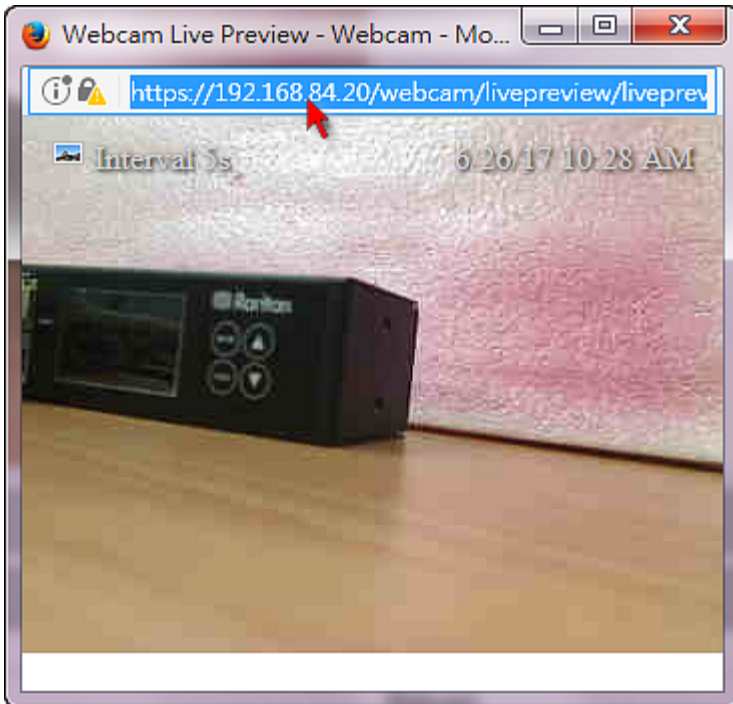
b. Right click to copy the URL, or press CTRL+ C.

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 Legrand PDU 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 Legrand PDU 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 Legrand PDU device by default. For snapshot-saving operations, see *Configuring Webcams and Viewing Live Images* (on page 248).

Up to 10 snapshots can be stored onto the Legrand PDU. 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 Legrand PDU to an FTP or Common Internet File System (CIFS)/Samba server. See **Changing Storage Settings** *(on page 254).*

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 Legrand PDU deletes all webcam snapshots that are saved onto the Legrand PDU 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 Legrand PDU web interface are automatically converted to your computer's time zone. To avoid any time confusion, you can apply the same time zone settings as those of Legrand PDU to your computer.

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 ⟳.

▶ **To manually delete any snapshots:**

1. Click ☑ 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.

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 Legrand PDU web interface only lists the snapshots stored locally on the Legrand PDU 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 Legrand PDU device, which has a limitation of 10 snapshots. Note that any operation involving device reboot will remove the snapshots saved on the Legrand PDU, 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 Legrand PDU.

- Total number of saved snapshots will exceed 10.
- Saved snapshots must be stored *permanently*, or at least should *not* be removed by the Legrand PDU device's reboot.

▶ **To configure the storage settings:**

1. Choose Webcams > Edit Settings.
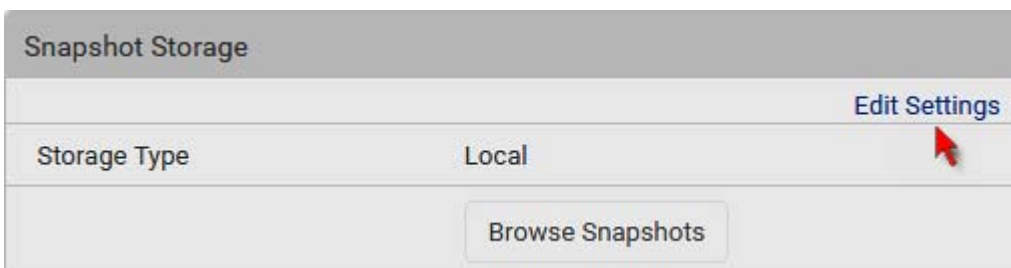
2. Click the Storage Type field to select the desired storage location and configure as needed.

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 Legrand PDU device. 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 Legrand PDU. See ***Viewing and Managing Locally-Saved Snapshots*** (on page 253). ▪ All snapshots are CLEARED when the Legrand PDU 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 Legrand PDU.
	▪ 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 Legrand PDU.
	▪ 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 256).

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 Legrand PDU web interface. If this issue occurs, first restore the connectivity of the remote server and then change the storage settings of the webcam snapshots.
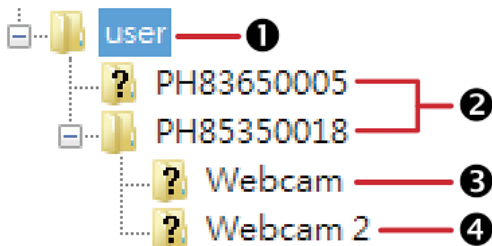

June 2018

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 Legrand PDU device rather than that of the computer or mobile device you are operating.

Tip: To check the time zone of your Legrand PDU, choose Device Settings > Date/Time. See **Setting the Date and Time** *(on page 182).*

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 Legrand PDU device where the webcam is connected. For example, *PH85350018.* ▪ To find your Legrand PDU serial number, see **Device Information** (on page 231).
❸	The name of the webcam that Legrand PDU 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 248). ▪ If the webcam's location is important, you can customize the webcam's name based on its location when configuring Legrand PDU to save snapshots onto a remote server.
❹	The name of the webcam that Legrand PDU 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 Legrand PDU 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, Legrand PDU will create a new folder with the new webcam name while keeping the old folder with the old name.

June 2018

SmartLock and Card Reader

Raritan's SmartLock kits provide several cabinet access control solutions.

Note: For information and installation of the SmartLock kits, refer to the user documentation accompanying the SmartLock kit or download it from Legrand's **Support page** *(***http://www.raritan.com/support/***).*

If you have purchased a SmartLock kit with the door handle controller "DX2-DH2C2", both menu items "SmartLock" and "Card Readers" will appear in the menu after connecting DX2-DH2C2 and the door handles included in the kit.

Note: For information on DX2-DH2C2, you can refer to either the user documentation accompanying the SmartLock kit or 'Environmental Sensors and Actuators Guide' (or Online Help) on Raritan website's **Support page** *(***http://www.raritan.com/support/***).*
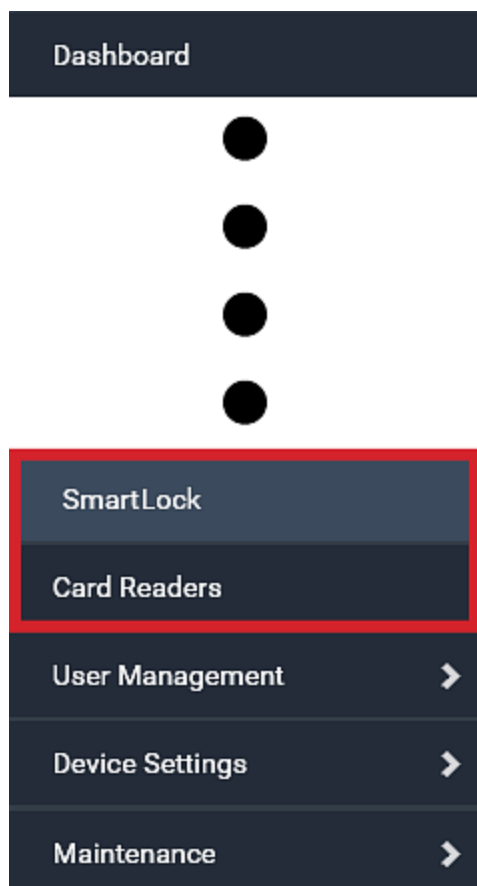
Note that "SmartLock" appears only when your door handles are connected via **DX2-DH2C2** to Legrand PDU, but "Card Readers" appears as long as the Legrand PDU detects any card reader -- directly connected to Legrand PDU, or indirectly connected via DX2-DH2C2.

▶ **SmartLock:**

- This page shows the information of all door handle controllers, DX2-DH2C2, connected to Legrand PDU.
- The page also 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 from this page. See **SmartLock** (on page 258).

▶ **Card Readers:**

- This page shows the information of all card readers connected to Legrand PDU, including:
  - Door handle-integrated card readers connected to DX2-DH2C2.

- External USB card readers connected directly to Legrand PDU.
- See **Card Readers** (on page 261).

SmartLock

To open the SmartLock page, choose SmartLock in the **Menu** (on page 84).

The page lists all DX2-DH2C2 connected to Legrand PDU, including their serial numbers and positions in a sensor chain.

#	Model	Position ▲	Serial Number
2	DX2-DH2C2	Port 1, Chain Position 1	1GE6C00001
1	DX2-DH2C2	Port 1, Chain Position 2	1GE7100002

You can click the desired DX2-DH2C2 to open its details page, and then do the following.

- 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 Legrand PDU cannot detect the types of connected door handles.
- Control the door handles connected to DX2-DH2C2.

▶ **To view the status of the door and card reader:**

There are two door handle sections per DX2-DH2C2 because a DX2-DH2C2 has two door handle ports and two pairs of contact closure sensor terminals. Before you configure the connected door handle, all states in the Door State section are "unavailable" by default, and a lock icon is displayed on each section's top-right corner.

Tip: All sensors of the connected door handles are also listed on the page of **Peripherals** *(on page 116).*

Door Handle 1	⏻ Open	⏻ Close 🔒
Door State		⌃
Name	**State**	**Type**
Door 1	unavailable	Door
Door Lock 1	unavailable	Door Lock
Door Handle Lock 1	unavailable	Door Handle Lock
Card Reader		⌃
Manufacturer/Model	Raritan SmartLock	
Card Type	- - -	
Card ID	- - -	
Setting		
		Edit Settings
Door Handle Type	None	

Door Handle 2	⏻ Open	⏻ Close 🔒
Door State		⌃
Name	**State**	**Type**
Door 2	unavailable	Door
Door Lock 2	unavailable	Door Lock
Door Handle Lock 2	unavailable	Door Handle Lock
Card Reader		⌃
Manufacturer/Model	Raritan SmartLock	
Card Type	- - -	
Card ID	- - -	
Setting		
		Edit Settings
Door Handle Type	None	

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 card reader integrated in 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.*

Note that the same Card Reader information is also available on the page of ***Card Readers*** (on page 261).

▶ **To configure the door handles:**
1. Click Edit Settings in the Setting section.
2. In the Door Handle Type field, select the door handle type you are using.
   ▪ The default is None.
   ▪ If no door handle is being connected to the door-handle port in question on the DX2-DH2C2, select or leave this field to "None."
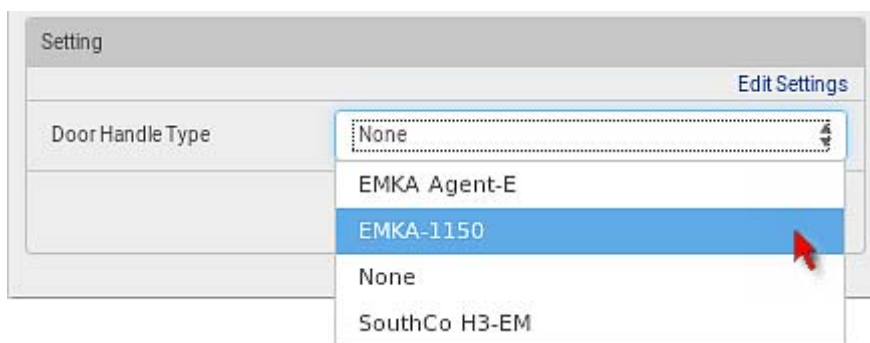
3. Click Save.

▶ **To control the door handles:**
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.

Door Handle 1   ⏻ Open   ⏻ Close
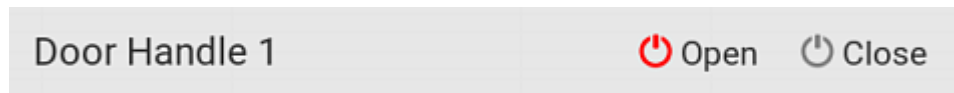
3. Confirm your action on the confirmation message.
4. Now you can physically open the door with the opened door handle.

Tip: You can click Close to re-close the door handle lock when you change your mind before the door handle is physically opened, when the door handle lock is mistakenly opened, or when someone opens it without pulling it out.

Card Readers

To open the Card Readers page, choose Card Readers in the *Menu* (on page 84).

Card Readers

# ▲	Manufacturer/Model	Serial Number	Channel	Card Type	Card ID
1	Raritan SmartLock	1GE44332211	1	- - -	- - -
2	Raritan SmartLock	1GE44332211	2	- - -	- - -
3	Raritan SmartLock	1GEDDCCBBAA	1	- - -	- - -
4	Raritan SmartLock	1GEDDCCBBAA	2	- - -	- - -

This page lists all card readers connected to Legrand PDU, indirectly or directly.

When a user scans his/her smart card with the card reader, Legrand PDU 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 Legrand PDU to perform security features like cabinet access control. Refer to that application's user documentation for more information.

The 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 either one below:
  - Emka Agent E
  - SouthCo H3-EM (H3-EM-67-100 or H3-EM-66-100)
- It is indirectly connected to Legrand PDU via DX2-DH2C2.
- The Channel column indicates which port (channel) on DX2-DH2C2 it is connected to.
- Note that the serial number displayed for this card reader is the serial number of DX2-DH2C2.
  Each DX2-PD2C2 can show two card readers because they have two ports for connecting two door handles with internal card readers.

▶ **External USB card readers:**
- This is an external USB card reader.
- It is directly connected to Legrand PDU via USB.
- The Channel column does not show any data.

Using SNMP

This SNMP section helps you set up the Legrand PDU for use with an SNMP manager. The Legrand PDU 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 Legrand PDU. 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 Legrand PDU.

Important: You must download the SNMP MIB for your Legrand PDU to use with your SNMP manager. See *Downloading SNMP MIB* **(on page 265).**

▶ **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 160).

▶ **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 130).

▶ **To enable SNMP notifications:**
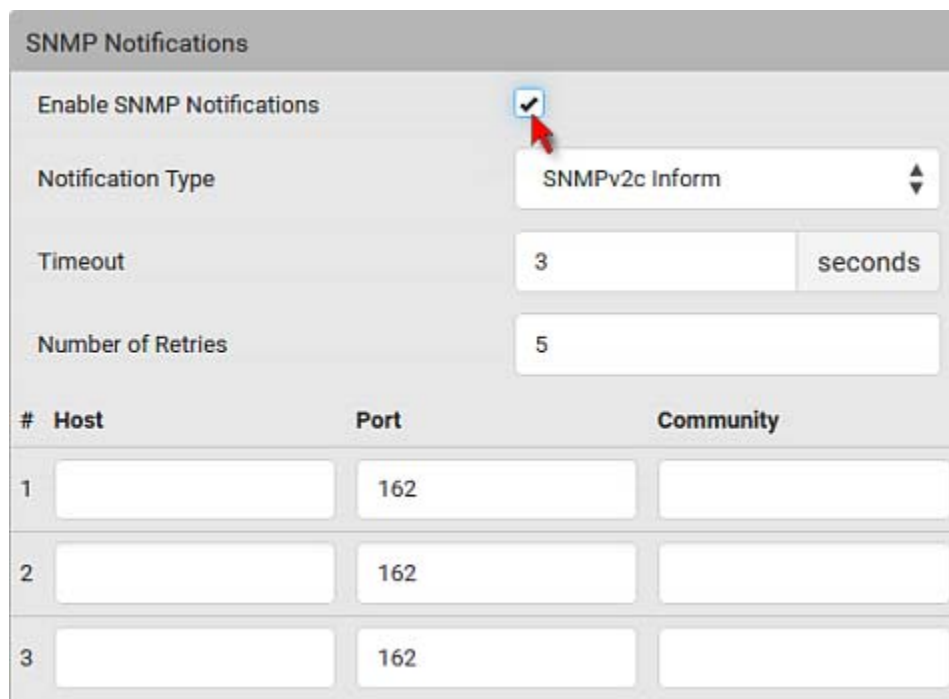
1. Choose Device Settings > Network Services > SNMP.
2. In the SNMP Notifications section, enable the SNMP notification feature, and configure related fields. For details, refer to:
   - ***SNMPv2c Notifications*** (on page 262)
   - ***SNMPv3 Notifications*** (on page 263)

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 196).*

SNMPv2c Notifications

1. Choose Device Settings > Network Services > SNMP.

2. In the SNMP Agent, make sure the Enable SNMP v1/v2c checkbox is selected.
3. In the SNMP Notifications section, make sure the Enable SNMP Notifications checkbox is selected.

4. Select SNMPv2c Trap or SNMPv2c Inform as the notification type.
5. Type values in the following fields.

Field	Description
Timeout	The interval of time, in seconds, after which a new inform communication is resent if the first is not received. ▪ For example, resend a new inform communication once every 3 seconds.
Number of Retries	The number of times you want to resend the inform communication if it fails. ▪ For example, inform communications are resent up to 5 times when the initial communication fails.
Host	The IP address of the device(s) you want to access. This is the address to which notifications are sent by the SNMP agent. You can specify up to 3 SNMP destinations.
Port	The port number used to access the device(s).
Community	The SNMP community string to access the device(s). The community is the group representing the Legrand PDU and all SNMP management stations.

6. Click Save.

SNMPv3 Notifications

1. Choose Device Settings > Network Services > SNMP.
2. In the SNMP Agent, make sure the Enable SNMP v1/v2c checkbox is selected.

3. In the SNMP Notifications section, make sure the Enable SNMP Notifications checkbox is selected.

4. Select SNMPv3 Trap or SNMPv3 Inform as the notification type.
5. For SNMP TRAPs, the engine ID is prepopulated.
6. Type values in the following fields.

Field	Description
Host	The IP address of the device(s) you want to access. This is the address to which notifications are sent by the SNMP agent.
Port	The port number used to access the device(s).
User ID	User name for accessing the device. ▪ Make sure the user has the SNMP v3 access permission.

Field	Description
Timeout	The interval of time, in seconds, after which a new inform communication is resent if the first is not received. • For example, resend a new inform communication once every 3 seconds.
Number of Retries	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.

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 Legrand PDU.

You can download the MIBs from two different pages of the web interface.

▶ **MIB download via the SNMP page:**

1. Choose Device Settings > Network Services > SNMP.
2. Click the Download MIBs title bar.

Download MIBs ⌄

3. Select the desired MIB file to download.
   ▪ PDU2-MIB: The SNMP MIB file for Legrand PDU power management.
   ▪ ASSETMANAGEMENT-MIB: The SNMP MIB file for asset management.

Note: Legrand PDU does NOT support the asset management feature so you can ignore the asset management MIB.

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
3. Click Save to save the file onto your computer.

SNMP Gets and Sets

In addition to sending notifications, the Legrand PDU is able to receive SNMP get and set requests from third-party SNMP managers.

- Get requests are used to retrieve information about the Legrand PDU, such as the system location, and the current on a specific outlet.
- Set requests are used to configure a subset of the information, such as the SNMP system name.

Note: The SNMP system name is the Legrand PDU device name. When you change the SNMP system name, the device name shown in the web interface is also changed.

The Legrand PDU 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 Legrand PDU MIB.
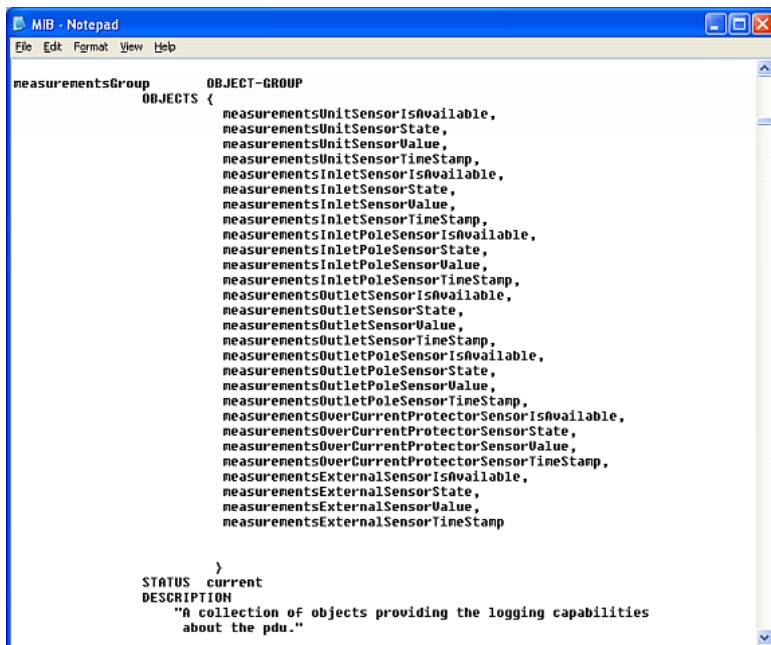
The Legrand PDU MIB

The SNMP MIB file is required for using your Legrand PDU with an SNMP manager. An SNMP MIB file describes the SNMP functions.

Layout

Opening the MIB reveals the custom objects that describe the Legrand PDU system at the unit level as well as at the individual-outlet level.

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 sensor readings of Legrand PDU as a whole. One object listed under this group, measurementsUnitSensorValue, is described later in the MIB as "The sensor value".   pduRatedCurrent, part of the configGroup group, describes the PDU current rating.

SNMP Sets and Thresholds

Some objects can be configured from the SNMP manager using SNMP set commands. Objects that can be configured have a MAX-ACCESS level of "read-write" in the MIB.

These objects include threshold objects, which causes the Legrand PDU to generate a warning and send an SNMP notification when certain parameters are exceeded. See **Sensor Threshold Settings** (on page 473) 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 321). For the web interface, see* **Setting the Date and Time** *(on page 182).*

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.

Using the Command Line Interface

This section explains how to use the command line interface (CLI) to administer the Legrand PDU. CLI commands are case sensitive.

In This Chapter

About the Interface

The Legrand PDU 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 Legrand PDU
- Display the Legrand PDU and network information, such as the device name, firmware version, IP address, and so on
- Configure the Legrand PDU 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 163).*

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 PX2 Serial Console" under the Ports group.

3. In the communications program, press Enter to send a carriage return to the Legrand PDU. The Username prompt appears.

   ```
   Username: _
   ```

4. Type a name and press Enter. The name is case sensitive. Then you are prompted to enter a password.

   ```
   Username: admin
   Password: _
   ```

5. Type a password and press Enter. The password is case sensitive.

   After properly entering the password, the # or > system prompt appears. See ***Different CLI Modes and Prompts*** (on page 271) 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 158) in the User Guide.

2. Launch an SSH or Telnet client and open a console window. A login prompt appears.

   ```
   login as: █
   ```

3. Type a name and press Enter. The name is case sensitive.

   Note: If using the SSH client, the name must NOT exceed 25 characters. Otherwise, the login fails.

Then you are prompted to enter a password.

```
login as: admin
admin@192.168.84.88's password: █
```

4. Type a password and press Enter. The password is case sensitive.

5. After properly entering the password, the # or > system prompt appears. See **Different CLI Modes and Prompts** (on page 271) 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.

Different CLI Modes and Prompts

Depending on the login name you use and the mode you enter, the system prompt in the CLI varies.

- User Mode: When you log in as a normal user, who may not have full permissions to configure the Legrand PDU, the **>** prompt appears.
- Administrator Mode: When you log in as an administrator, who has full permissions to configure the Legrand PDU, 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 Legrand PDU device and network configurations. See **Entering Configuration Mode** (on page 293).
- 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 390).

Closing a Local Connection

Close the window or terminal emulation program when you finish accessing the Legrand PDU over the local connection.

When accessing or upgrading multiple Legrand PDUs, 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 272).

▶ **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 392). To re-execute one of the previous commands, see* **Retrieving Previous Commands** *(on page 392).*

Querying Available Parameters for a Command

f 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 392). To re-execute one of the previous commands, see* **Retrieving Previous Commands** *(on page 392).*

Showing Information

You can use the show commands to view current settings or the status of the Legrand PDU 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 271).*

Network Configuration

This command shows all network configuration and all network interfaces' information, such as the IP address, MAC address, the Ethernet interface's duplex mode, and the wireless interface's status/settings.

```
#       show network
```

IP Configuration

This command shows the IP 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 274).*

```
#       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 Legrand PDU 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 273).*

▶ **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 Legrand PDU 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.
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 Legrand PDU 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*.*

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.

Option	Description
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.

PDU Configuration

This command shows the PDU configuration, such as the device name, firmware version and model type.

```
#      show pdu
```

To show detailed information, add the parameter "details" to the end of the command.

```
#      show pdu details
```

Outlet Information

This command syntax shows the outlet information.

```
#      show outlets <n>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#      show outlets <n> details
```

Variables:

- <n> is one of the options: *all*, or a number.

Option	Description
all	Displays the information for all outlets.
	Tip: You can also type the command without adding this option "all" to get the same data.
A specific outlet number	Displays the information for the specified outlet only.

Displayed information:

- Without the parameter "details," only the outlet name is displayed. For outlet-switching capable models, the outlet state is also displayed.
- With the parameter "details," more outlet information is displayed in addition to the outlet name, such as the outlet rating.

Inlet Information

This command syntax shows the inlet information.

```
#       show inlets <n>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show inlets <n> details
```

Variables:

- <n> is one of the options: *all*, or a number.

Option	Description
all	Displays the information for all inlets.
	Tip: You can also type the command without adding this option "all" to get the same data.
A specific inlet number	Displays the information for the specified inlet only.
	An inlet number needs to be specified only when there are more than 1 inlet on your PDU.

Displayed information:

- Without the parameter "details," only the inlet's name and RMS current are displayed.
- With the parameter "details," more inlet information is displayed in addition to the inlet name and RMS current, such as the inlet's RMS voltage, active power and active energy.

Overcurrent Protector Information

This command is only available for models with overcurrent protectors for protecting outlets.

This command syntax shows the overcurrent protector information, such as a circuit breaker or a fuse.

```
#       show ocp <n>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show ocp <n> details
```

Variables:

- <n> is one of the options: *all*, or a number.

Option	Description
all	Displays the information for all overcurrent protectors.
	Tip: You can also type the command without adding this option "all" to get the same data.

Option	Description
A specific overcurrent protector number	Displays the information for the specified overcurrent protector only.

Displayed information:

- Without the parameter "details," only the overcurrent protector status and name are displayed.
- With the parameter "details," more overcurrent protector information is displayed in addition to status, such as the rating and RMS current value.

Date and Time Settings

This command shows the current date and time settings on the Legrand PDU.

```
#       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 Legrand PDU web and CLI interfaces across all users, especially those users authenticated through remote authentication servers.

```
#       show user defaultPreferences
```

Note: If a user has set his/her own preferred measurement units or the administrator has changed any user's preferred units, the web and CLI interfaces show the preferred measurement units for that user instead of the default ones after that user logs in to the Legrand PDU. See **Existing User Profiles** *(on page 287) for the preferred measurement units for a specific user.*

Environmental Sensor Information

This command syntax shows the environmental sensor's information.

```
#        show externalsensors <n>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#        show externalsensors <n> details
```

```
# 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 Legrand PDU web interface.

Displayed information:

- Without the parameter "details," only the sensor ID, sensor type and reading are displayed.

  Note: A state sensor displays the sensor state instead of the reading.

- With the parameter "details," more information is displayed in addition to the ID number and sensor reading, such as the serial number, sensor position, and X, Y, and Z coordinates.

Note: DPX sensor packages do not provide chain position information.

Environmental Sensor Package Information

Different from the "`show externalsensors`" commands, which show the reading, status and configuration of an individual environmental sensor, the following command shows the information of all connected environmental sensor packages, each of which may contain more than one sensor or actuator.

```
#       show peripheralDevicePackages
```

Information similar to the following is displayed. An environmental sensor package is a peripheral device package.

```
Peripheral Device Package 1
Serial Number:    AEI7A00022
Package Type:     DPX-T1H1
Position:         Port 1
Package State:    operational
Firmware Version: Not available


Peripheral Device Package 2
Serial Number:    AEI7A00021
Package Type:     DPX-T3H1
Position:         Port 1
Package State:    operational
Firmware Version: Not available
```

Actuator Information

This command syntax shows an actuator's information.

```
#       show actuators <n>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show actuators <n> details
```

Variables:

- <n> is one of the options: *all*, or a number.

Option	Description
all	Displays the information for all actuators.
	Tip: You can also type the command without adding this option "all" to get the same data.
A specific actuator number*	Displays the information for the specified actuator only.

* The actuator number is the ID number assigned to the actuator. The ID number can be found using the Legrand PDU 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.

Inlet Sensor Threshold Information

This command syntax shows the specified inlet sensor's threshold-related information.

```
#        show sensor inlet <n> <sensor type>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#        show sensor inlet <n> <sensor type> details
```

Variables:

- <n> is the number of the inlet whose sensors you want to query. For a single-inlet PDU, <n> is always 1.
- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor
unbalancedCurrent	Unbalanced load sensor
lineFrequency	Line frequency sensor

Displayed information:

- Without the parameter "details," only the reading, state, threshold, deassertion hysteresis and assertion timeout settings of the specified inlet sensor are displayed.
- With the parameter "details," more sensor information is displayed, including resolution and range.
- If the requested sensor type is not supported, the "Sensor is not available" message is displayed.

▶ **Additional sensors supported by Legrand PDUs:**

The CLI command(s) listed above can be also applied to the following sensors. Note that the measurement unit of current values in CLI is **A**, not mA.

Sensor type	Description
peakCurrent	Peak current sensor
reactivePower	Reactive power sensor

Sensor type	Description
displacementPowerFactor	Displacement power factor sensor
phaseAngle	Inlet phase angle sensor

Inlet Pole Sensor Threshold Information

This command syntax shows the specified inlet pole sensor's threshold-related information.

```
#        show sensor inletpole <n> <p> <sensor type>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#        show sensor inletpole <n> <p> <sensor type> details
```

Variables:

- <n> is the number of the inlet whose pole sensors you want to query. For a single-inlet PDU, <n> is always 1.
- <p> is the label of the inlet pole whose sensors you want to query.

Pole	Label <p>	Current sensor	Voltage sensor
1	**L1**	L1	L1 - L2
2	**L2**	L2	L2 - L3
3	**L3**	L3	L3 - L1

- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor

Displayed information:

- Without the parameter "details," only the reading, state, threshold, deassertion hysteresis and assertion timeout settings of the specified inlet pole sensor are displayed.
- With the parameter "details," more sensor information is displayed, including resolution and range.
- If the requested sensor type is not supported, the "Sensor is not available" message is displayed.

▶ **Additional sensors supported by Legrand PDUs:**

The CLI command(s) listed above can be also applied to the following sensors. Note that the measurement unit of current values in CLI is **A**, not mA.

Sensor type	Description
peakCurrent	Peak current sensor
reactivePower	Reactive power sensor
displacementPowerFactor	Displacement power factor sensor
phaseAngle	Inlet phase angle sensor

Overcurrent Protector Sensor Threshold Information

This command is only available for models with overcurrent protectors for protecting outlets.

This command syntax shows the specified overcurrent protector sensor's threshold-related information.

```
#       show sensor ocp <n> <sensor type>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show sensor ocp <n> <sensor type> details
```

Variables:

- <n> is the number of the overcurrent protector whose sensors you want to query.
- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor

Displayed information:

- Without the parameter "details," only the reading, state, threshold, deassertion hysteresis and assertion timeout settings of the specified overcurrent protector sensor are displayed.
- With the parameter "details," more sensor information is displayed, including resolution and range.

Environmental Sensor Threshold Information

This command syntax shows the specified environmental sensor's threshold-related information.

```
#        show sensor externalsensor <n>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#        show sensor externalsensor <n> details
```

```
External sensor 3 (Temperature):
Reading: 31.8 deg C
State:   normal

Active Thresholds: Sensor specific thresholds

Default Thresholds for Temperature sensors:
Lower critical threshold: 10.0 deg C
Lower warning threshold:  15.0 deg C
Upper warning threshold:  30.0 deg C
Upper critical threshold: 35.0 deg C
Deassertion hysteresis:   1.0 deg C
Assertion timeout:        0 samples

Sensor Specific Thresholds:
Lower critical threshold: 8.0 deg C
Lower warning threshold:  13.0 deg C
Upper warning threshold:  28.0 deg C
Upper critical threshold: 33.0 deg C
Deassertion hysteresis:   1.0 deg C
Assertion timeout:        0 samples
```

Variables:

- <n> is the environmental sensor number. The environmental sensor number is the ID number assigned to the sensor, which can be found on the Peripherals page of the Legrand PDU web interface.

Displayed information:

- Without the parameter "details," only the reading, threshold, deassertion hysteresis and assertion timeout settings of the specified environmental sensor are displayed.
- With the parameter "details," more sensor information is displayed, including resolution and range.

Note: For a state sensor, the threshold-related and accuracy-related data is NOT available.

Environmental Sensor Default Thresholds

This command syntax shows a certain sensor type's default thresholds, which are the initial thresholds applying to the specified type of sensor.

```
#        show defaultThresholds <sensor type>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#        show defaultThresholds <sensor type> details
```

Variables:

- <sensor type> is one of the following numeric sensor types:

Sensor types	Description
absoluteHumidity	Absolute humidity sensors
relativeHumidity	Relative humidity sensors
temperature	Temperature sensors
airPressure	Air pressure sensors
airFlow	Air flow sensors
vibration	Vibration sensors
all	All of the above numeric sensors *Tip: You can also type the command without adding this option "all" to get the same data.*

Displayed information:

- Without the parameter "details," only the default upper and lower thresholds, deassertion hysteresis and assertion timeout settings of the specified sensor type are displayed.
- With the parameter "details," the threshold range is displayed in addition to default thresholds settings.

Security Settings

This command shows the security settings of the Legrand PDU.

```
#        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).

Authentication Settings

▶ **General authentication settings:**

This command displays the authentication settings of the Legrand PDU, 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> details
```

▶ **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, Legrand PDU 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.

June 2018

Load Shedding Settings

This section applies to outlet-switching capable models only.

This command shows the load shedding settings.

```
#       show loadshedding
```

Displayed information:

- The load shedding state is displayed along with non-critical outlets.

Note: The load shedding mode is associated with critical and non-critical outlets. To specify critical and non-critical outlets through CLI, see **Specifying Non-Critical Outlets** *(on page 296).*

Serial Port Settings

This command shows the baud rate setting of the serial port labeled CONSOLE on the Legrand PDU.

```
#       show serial
```

EnergyWise Settings

This command shows the Legrand PDU device's current configuration for Cisco® EnergyWise.

```
#       show energywise
```

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.

Option	Description
An integer number	Displays the specified number of last entries in the event log. The number ranges between 1 to 10,000.

- <event_type> is one of the following event types.

Event type	Description
all	All events.
device	Device-related events, such as system starting or firmware upgrade event.
userAdministration	User management events, such as a new user profile or a new role.
userActivity	User activities, such as login or logout.
pdu	Displays PDU-related events, such as entry or exit of the load shedding mode.
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.
timerEvent	Scheduled action events.
webcam	Events for webcam management, if available.
cardReader	Events for card reader management, if available.
energywise	Cisco EnergyWise-related events, such as enabling the support of the EnergyWise function.

Note: Legrand PDU does not support features regarding Schroff LHX, modem, Raritan asset management, and transfer switch so you can ignore these event types in the CLI.

Wireless LAN Diagnostic Log

This command shows the diagnostic log for the wireless LAN connection.

```
#      show wlanlog
```

Server Reachability Information

This command shows all server reachability information with a list of monitored servers and status.

```
#      show serverReachability
```

Server Reachability Information for a Specific Server

To show the server reachability information for a certain IT device only, use the following command.

```
#      show serverReachability server <n>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#      show serverReachability server <n> details
```

Variables:

- <n> is a number representing the sequence of the IT device in the monitored server list.
  You can find each IT device's sequence number using the CLI command of `show serverReachability` as illustrated below.

```
-----------------------------------------------------------
#  IP address       Enabled  Status
-----------------------------------------------------------
1  192.168.84.126   Yes      Waiting for reliable connection
2  www.raritan.com  Yes      Waiting for reliable connection
```

Displayed information:

- Without the parameter "details," only the specified device's IP address, monitoring enabled/disabled state and current status are displayed.
- With the parameter "details," more settings for the specified device are displayed, such as number of pings and wait time prior to the next ping.

Command History

This command 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.

Examples

This section provides examples of the show command.

Example 1 - Basic Security Information

The diagram shows the output of the *show security* command.

```
# show security
IPv4 access control: Disabled

IPv6 access control: Disabled

Role based access control for IPv4: Disabled

Role based access control for IPv6: Disabled

Password aging: Disabled

Prevent concurrent user login:    No

Strong passwords: Disabled

Enforce HTTPS for web access: Yes

Restricted Service Agreement: disabled
```

Example 2 - In-Depth Security Information

More information is displayed when typing the *show security details* command.

```
# show security details
IPv4 access control: Disabled

IPv6 access control: Disabled


Role based access control for IPv4: Disabled

Role based access control for IPv6: Disabled

Password aging: Disabled

Prevent concurrent user login:    No
Maximum number of failed logins: 3
User block time:                 10 minutes

User idle timeout: 1440 minutes

Strong passwords: Disabled

Enforce HTTPS for web access: Yes

Restricted Service Agreement: disabled
Restricted Service Agreement Banner Content:
Unauthorized access prohibited; all access and activities not explicitly authori
zed by management are unauthorized. All activities are monitored and logged. The
re is no privacy on this system. Unauthorized access and activities or any crimi
nal activity will be reported to appropriate authorities.
```

Clearing Information

You can use the clear commands to remove unnecessary data from the Legrand PDU.

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 271).*

Clearing Event Log

This command removes all data from the event log.

clear eventlog

   -- OR --

clear eventlog /y

If you entered the command without "/y," a message appears, prompting you to confirm the operation. Type y to clear the event log or n to abort the operation.

If you type y, a message "Event log was cleared successfully" is displayed after all data in the event log is deleted.

Clearing WLAN Log

This command removes all data from the diagnostic log for the wireless LAN (WLAN) connection.

```
#       clear wlanlog
```

   -- OR --

```
#       clear wlanlog /y
```

If you entered the command without "/y," a message appears, prompting you to confirm the operation. Type y to clear the WLAN log or n to abort the operation.

If you type y, a message "WLAN log was cleared successfully" is displayed to indicate all data in the WLAN log has been deleted.

Configuring the Legrand PDU Device and Network

To configure the Legrand PDU 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 271).*

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 293).**

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 271).

PDU Configuration Commands

A PDU configuration command begins with *pdu*. You can use the PDU configuration commands to change the settings that apply to the whole Legrand PDU device.

Changing the PDU Name

This command changes the device name of Legrand PDU.

```
config:#   pdu 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.

Setting the Outlet Power-On Sequence

> This section applies to outlet-switching capable models only.

This command sets the outlet power-on sequence when the PDU powers up.

```
config:#   pdu outletSequence <option>
```

Variables:

- <option> is one of the options: *default*, or a comma-separated list of outlet numbers.

Option	Description
default	All outlets are switched ON in the ASCENDING order (from outlet 1 to the final outlet) when the Legrand PDU powers up.
A comma-separated list of outlet numbers	All outlets are switched ON in the order you specify using the comma-separated list. The list must include all outlets on the PDU.

Setting the Outlet Power-On Sequence Delay

> This section applies to outlet-switching capable models only.

This command sets the delays (in seconds) for outlets when turning on all outlets in sequence.

```
config:#    pdu outletSequenceDelay <outlet1>:<delay1>;<outlet2>:<delay2>;
            <outlet3>:<delay3>;...
```

Separate outlet numbers and their delay settings with a colon. Outlets followed by delays are separated with a semicolon.

Variables:

- <outlet1>, <outlet2>, <outlet3> and the like are individual outlet numbers or a range of outlets using a dash. For example, *3-8* represents outlets 3 to 8.
- <delay1>, <delay2>, <delay3> and the like are the delay time in seconds.

Setting the PDU-Defined Default Outlet State

This section applies to outlet-switching capable models only.

This command determines the initial power condition of all outlets after powering up the PDU.

```
config:#    pdu outletStateOnDeviceStartup <option>
```

Variables:

- <option> is one of the options: *off*, *on* or *lastKnownState*.

Option	Description
off	Switches OFF all outlets when the Legrand PDU powers up.
on	Switches ON all outlets when the Legrand PDU powers up.
lastKnownState	Restores all outlets to the previous status before powering down the Legrand PDU when the PDU powers up again.

Setting the PDU-Defined Cycling Power-Off Period

This section applies to outlet-switching capable models only.

This command sets the power-off period of the power cycling operation for all outlets.

```
config:#    pdu cyclingPowerOffPeriod <timing>
```

Variables:

- <timing> is the time of the cycling power-off period in seconds, which is an integer between 0 and 3600, or *pduDefined* for following the PDU-defined timing.

Setting the Inrush Guard Delay Time

This section applies to outlet-switching capable models only.

This command sets the inrush guard delay.

```
config:#    pdu inrushGuardDelay <timing>
```

Variables:

- <timing> is a delay time between 100 and 100000 milliseconds.

Setting the Outlet Initialization Delay

This section applies to outlet-switching capable models only.

This command determines the outlet initialization delay timing on device startup. See **PDU** (on page 94) for information on outlet initialization delay.

```
config:#    pdu outletInitializationDelayOnDeviceStartup <timing>
```

Variables:

- <timing> is a delay time between 1 and 3600 seconds.

Specifying Non-Critical Outlets

This section applies to outlet-switching capable models only.

This command determines critical and non-critical outlets. It is associated with the load shedding mode. See **Load Shedding Mode** (on page 105).

```
config:#    pdu nonCriticalOutlets <outlets1>:false;<outlets2>:true
```

Separate outlet numbers and their settings with a colon. Separate each "false" and "true" setting with a semicolon.

Variables:

- <outlets1> is one or multiple outlet numbers to be set as critical outlets. Use commas to separate outlet numbers.

  Use a dash for a range of consecutive outlets. For example, *3-8* represents outlets 3 to 8.
- <outlets2> is one or multiple outlet numbers to be set as NON-critical outlets. Use commas to separate outlet numbers.

  Use a dash for a range of consecutive outlets. For example, *3-8* represents outlets 3 to 8.

Enabling or Disabling Data Logging

This command enables or disables the data logging feature.

```
config:#   pdu 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 219).

Setting Data Logging Measurements Per Entry

This command defines the number of measurements accumulated per log entry.

```
config:#   pdu 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 219).

Specifying the Device Altitude

This command specifies the altitude of your Legrand PDU above sea level (in meters). You must specify the altitude of Legrand PDU above sea level if a Raritan's DPX differential air pressure sensor is attached. This is because the device's altitude is associated with the altitude correction factor. See **Altitude Correction Factors** (on page 480).

```
config:#   pdu 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:#   pdu 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 365).*

Enabling or Disabling Peripheral Device Auto Management

This command enables or disables the Peripheral Device Auto Management feature.

```
config:#   pdu peripheralDeviceAutoManagement <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	Enables the automatic management feature for environmental sensor packages.
disable	Disables the automatic management feature for environmental sensor packages.

For more information, see **How the Automatic Management Function Works** (on page 98).

Setting the Maximum Number of Active Powered Dry Contact Actuators

This command determines the upper limit of "active" powered dry contact actuators on one Legrand PDU device.

```
config:#   pdu activePoweredDryContactLimit <number>
```

Variables:

- <number> is the number representing the maximum number of active powered dry contact actuators. Its value ranges between 0 to 24.

Note: An "active" actuator is the one that is turned ON.

Examples

This section illustrates several PDU configuration examples.

Example 1 - PDU Naming

The following command assigns the name "my px12" to the PDU.

```
config:#   pdu name "my px12"
```

Example 2 - Outlet Sequence

The following command causes a 10-outlet PDU to first power on the 8th to 6th outlets and then the rest of outlets in the ascending order after the PDU powers up.

```
config:#   pdu outletSequence 8-6,1-5,9,10
```

Example 3 - Outlet Sequence Delay

The following command determines that the outlet 1's delay is 2.5 seconds, outlet 2's delay is 3 seconds, and the delay for outlets 3 through 5 is 10 seconds.

```
config:#   pdu outletSequenceDelay 1:2.5;2:3;3-5:10
```

Example 4 - Non-Critical Outlets

The following command sets outlets 1, 2, 3, 7, and 9 to be critical outlets, and 4, 5, 6, 8, 10, 11 and 12 to be non-critical outlets on a 12-outlet Legrand PDU.

```
config:#   pdu nonCriticalOutlets 1-3,7,9:false;4-6,8,10-12:true
```

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 Legrand PDU 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 Legrand PDU 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).

June 2018

Interface	Description
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 Legrand PDU.

```
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 Legrand PDU 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 Legrand PDU. 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 Legrand PDU 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 148).

▶ **Method 1: add a static route when the other network is NOT directly reachable:**

```
config:#    network ipv4 staticRoutes add <dest-1> <hop>
```

▶ **Method 2: add a static route when the other network is directly reachable:**

```
config:#    network ipv4 staticRoutes add <dest-1> interface <ETH>
```

▶ **Delete an existing static route:**

```
config:#    network ipv4 staticRoutes delete <route_ID>
```

▶ **Modify an existing static route:**

```
config:#    network ipv4 staticRoutes modify <route_ID> <dest-2> <hop>
```

-- OR --

```
config:#    network ipv4 staticRoutes modify <route_ID> <dest-2> interface <ETH>
```

Variables:

- <dest-1> is a combination of the IP address and subnet mask of the other subnet. The format is *IP address/subnet mask*.
- <hop> is the IP address of the next hop router.
- <ETH> is one of the interfaces: *ETH1, ETH2*, *WIRELESS* and *BRIDGE*. Type "bridge" only when your Legrand PDU 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 Legrand PDU 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).
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 Legrand PDU 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).

Interface	Description
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
- 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 Legrand PDU.

```
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 Legrand PDU 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 Legrand PDU. 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 Legrand PDU 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 148).

▶ **Method 1: add a static route when the other network is NOT directly reachable:**

```
config:#   network ipv6 staticRoutes add <dest-1> <hop>
```

▶ **Method 2: add a static route when the other network is directly reachable:**

```
config:#   network ipv6 staticRoutes add <dest-1> interface <ETH>
```

▶ **Delete an existing static route:**

```
config:#   network ipv6 staticRoutes delete <route_ID>
```

▶ **Modify an existing static route:**

```
config:#   network ipv6 staticRoutes modify <route_ID> <dest-2> <hop>
```

-- OR --

```
config:#   network ipv6 staticRoutes modify <route_ID> <dest-2> interface <ETH>
```

Variables:

- \<dest-1> is the IP address and prefix length of the subnet where the Legrand PDU 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 Legrand PDU 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 Legrand PDU. 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

- <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 or 100Mbps*.

Option	Description
auto	System determines the optimum LAN speed through auto-negotiation.
10Mbps	The LAN speed is always 10 Mbps.
100Mbps	The LAN speed is always 100 Mbps.

Changing the LAN Duplex Mode

This command determines the LAN interface duplex mode.

`config:#`   network ethernet <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 Legrand PDU selects the optimum transmission mode through auto-negotiation.
half	Half duplex: Data is transmitted in one direction (to or from the Legrand PDU) at a time.
full	Full duplex: Data is transmitted in both directions simultaneously.

Setting Wireless Parameters

You must configure wireless parameters, including Service Set Identifier (SSID), authentication method, Pre-Shared Key (PSK), and Basic Service Set Identifier (BSSID) after the wireless networking mode is enabled.

A wireless configuration command begins with *network wireless*.

Note: If current networking mode is not wireless, the SSID, PSK and BSSID values are not applied until the networking mode is changed to "wireless." In addition, a message appears, indicating that the active network interface is not wireless.

Setting the SSID

This command specifies the SSID string.

`config:#`   network wireless SSID <ssid>

Variables:

- <ssid> is the name of the wireless access point, which consists of:
  - Up to 32 ASCII characters
  - No spaces
  - ASCII codes 0x20 ~ 0x7E

Setting the Authentication Method

This command sets the wireless authentication method to either PSK or Extensible Authentication Protocol (EAP).

```
config:#    network wireless authMethod <method>
```

Variables:

- <method> is one of the authentication methods: *PSK* or *EAP*.

Method	Description
PSK	The wireless authentication method is set to PSK.
EAP	The wireless authentication method is set to EAP.

Setting the PSK

If the Pre-Shared Key (PSK) authentication method is selected, you must assign a PSK passphrase by using this command.

```
config:#    network wireless PSK <psk>
```

Variables:

- <psk> is a string or passphrase that consists of:
  - 8 to 63 characters
  - No spaces
  - ASCII codes 0x20 ~ 0x7E

Setting EAP Parameters

When the wireless authentication method is set to EAP, you must configure EAP authentication parameters, including outer authentication, inner authentication, EAP identity, password, and CA certificate.

▶ **Determine the outer authentication protocol:**

```
config:#   network wireless eapOuterAuthentication <outer_auth>
```

▶ **Determine the inner authentication protocol:**

```
config:#   network wireless eapInnerAuthentication <inner_auth>
```

▶ **Set the EAP identity:**

```
config:#   network wireless eapIdentity <identity>
```

▶ **Set the EAP password:**

```
config:#   network wireless eapPassword
```

After performing the above command, the Legrand PDU prompts you to enter the password. Then type the password and press Enter.

▶ **Provide a CA TLS certificate:**

```
config:#   network wireless eapCACertificate
```

After performing the above command, the system prompts you to enter the CA certificate's contents. For details, see **EAP CA Certificate Example** (on page 311).

▶ **Enable or disable verification of the TLS certificate chain:**

```
config:#   network wireless enableCertVerification <option1>
```

▶ **Allow expired and not yet valid TLS certificates:**

```
config:#   network wireless allowOffTimeRangeCerts <option2>
```

▶ **Allow wireless network connection with incorrect system time:**

```
config:#   network wireless allowConnectionWithIncorrectClock <option3>
```

Variables:

- The value of <outer_auth> is *PEAP* because Legrand PDU only supports Protected Extensible Authentication Protocol (PEAP) as the outer authentication.
- The value of <inner_auth> is *MSCHAPv2* because Legrand PDU only supports Microsoft's Challenge Authentication Protocol Version 2 (MSCHAPv2) as the inner authentication.
- <identity> is your user name for the EAP authentication.
- <option1> is one of the options: *true* or *false*.

Option	Description
true	Enables the verification of the TLS certificate chain.
false	Disables the verification of the TLS certificate chain.

- <option2> is one of the options: *true* or *false*.

Option	Description
true	Always make the wireless network connection successful even though the TLS certificate chain contains any certificate which is outdated or not valid yet.
false	The wireless network connection is NOT successfully established when the TLS certificate chain contains any certificate which is outdated or not valid yet.

- <option3> is one of the options: *true* or *false*.

Option	Description
true	Make the wireless network connection successful when the Legrand PDU system time is earlier than the firmware build before synchronizing with the NTP server, causing the TLS certificate to become invalid.
false	The wireless network connection is NOT successfully established when the Legrand PDU finds that the TLS certificate is not valid due to incorrect system time.

EAP CA Certificate Example

This section provides a CA certificate example only. Your CA certificate contents should be different from the contents displayed in this example.

▶ **To provide a CA certificate:**

1. Make sure you have entered the configuration mode. See *Entering Configuration Mode* .
2. Type the following command and press Enter.

   ```
   config:#   network wireless eapCACertificate
   ```

3. The system prompts you to enter the contents of the CA certificate.
4. Open a CA certificate using a text editor. You should see certificate contents similar to the following.

June 2018

```
--- BEGIN CERTIFICATE ---
MIICjTCCAfigAwIBAgIEMaYgRzALBgkqhkiG9w0BAQQwRTELMAkGA1UEBhMCVVMx
NjA0BgNVBAoTLU5hdGlvbmFsIEFlcm9uYXV0aWNzIGFuZCBTcGFjZSBBZG1pbmlz
dHJhdGlvbjAmFxE5NjA1MjgxMzQ5MDUrMDgwMBcROTgwNTI4MTM0OTA1KzA4MDAw
ZzELMAkGA1UEBhMCVVMxNjA0BgNVBAoTLU5hdGlvbmFsIEFlcm9uYXV0aWNzIGFu
ZCBTcGFjZSBBZG1pbmlzdHJhdGlvbjEgMAkGA1UEBRMCMTYwEwYDVQQDEwxTdGV2
ZSBTY2hvY2gwWDALBgkqhkiG9w0BAQEDSQAwRgJBALrAwyYdgxmzNP/ts0Uyf6Bp
miJYktU/w4NG67ULaN4B5CnEz7k57s9o3YY3LecETgQ5iQHmkwlYDTL2fTgVfw0C
AQOjgaswgagwZAYDVR0ZAQH/BFowWDBWMFQxCzAJBgNVBAYTAlVTMTYwNAYDVQQK
Ey1OYXRpb25hbCBBZXJvbmF1dGljyBhbmQgU3BhY2UgQWRtaW5pc3RyYXRpb24x
DTALBgNVBAMTBENSTDEwFwYDVR0BAQH/BA0wC4AJODMyOTcwODEwMBgGA1UdAgQR
MA8ECTgzMjk3MDgyM4ACBSAwDQYDVR0KBAYwBAMCBkAwCwYJKoZIhvcNAQEEA4GB
AH2y1VCEw/A4zaXzSYZJTTUi3uawbbFiS2yxHvgf28+8Js0OHXk1H1w2d6qOHH21
X82tZXd/0JtG0g1T9usFFBDvYK8O0ebgz/P5ELJnBL2+atObEuJy1ZZ0pBDWINR3
WkDNLCGiTkCKp0F5EWIrVDwh54NNevkCQRZita+z4IBO
--- END CERTIFICATE ---
```

5. Select and copy the contents as illustrated below, excluding the starting line containing "BEGIN CERTIFICATE" and the ending line containing "END CERTIFICATE."

```
MIICjTCCAfigAwIBAgIEMaYgRzALBgkqhkiG9w0BAQQwRTELMAkGA1UEBhMCVVMxNjA0BgNVBAoTL
U5hdGlvbmFsIEFlcm9uYXV0aWNzIGFuZCBTcGFjZSBBZG1pbmlzdHJhdGlvbjAmFxE5NjA1MjgxMz
Q5MDUrMDgwMBcROTgwNTI4MTM0OTA1KzA4MDAwZzELMAkGA1UEBhMCVVMxNjA0BgNVBAoTLU5hdGl
vbmFsIEFlcm9uYXV0aWNzIGFuZCBTcGFjZSBBZG1pbmlzdHJhdGlvbjEgMAkGA1UEBRMCMTYwEwYD
VQQDEwxTdGV2ZSBTY2hvY2gwWDALBgkqhkiG9w0BAQEDSQAwRgJBALrAwyYdgxmzNP/ts0Uyf6Bpm
iJYktU/w4NG67ULaN4B5CnEz7k57s9o3YY3LecETgQ5iQHmkwlYDTL2fTgVfw0CAQOjgaswgagwZA
YDVR0ZAQH/BFowWDBWMFQxCzAJBgNVBAYTAlVTMTYwNAYDVQQKEy1OYXRpb25hbCBBZXJvbmF1dGl
jcyBhbmQgU3BhY2UgQWRtaW5pc3RyYXRpb24xDTALBgNVBAMTBENSTDEwFwYDVR0BAQH/BA0wC4AJ
ODMyOTcwODEwMBgGA1UdAgQRMA8ECTgzMjk3MDgyM4ACBSAwDQYDVR0KBAYwBAMCBkAwCwYJKoZIh
vcNAQEEA4GBAH2y1VCEw/A4zaXzSYZJTTUi3uawbbFiS2yxHvgf28+8Js0OHXk1H1w2d6qOHH21X8
2tZXd/0JtG0g1T9usFFBDvYK8O0ebgz/P5ELJnBL2+atObEuJy1ZZ0pBDWINR3WkDNLCGiTkCKp0F
5EWIrVDwh54NNevkCQRZita+z4IBO
```

6. Paste the contents in the terminal.
7. Press Enter.
8. Verify whether the system shows the following command prompt, indicating the provided CA certificate is valid.

```
config:#
```

Setting the BSSID

This command specifies the BSSID.

```
config:#   network wireless BSSID <bssid>
```

Variables:

*   <bssid> is either the MAC address of the wireless access point or *none* for automatic selection.

Configuring the Cascading Mode

This command determines the cascading mode.

```
config:#   network <mode> enabled <option1>
```

Variables:

- <mode> is one of the following cascading modes.

Mode	Description
bridge	The Bridging mode, where each cascaded device is assigned a unique IP address.
portForwarding	The Port Forwarding mode, where every cascaded device in the chain shares the same IP address, with diverse port numbers assigned.

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>
```

Variables:

- <n> is a TCP port number between 1 and 65535. The default HTTP port is 80.
- <option> is one of the options: *true* or *false.*

Option	Description
true	The HTTP port is enabled.
false	The HTTP port is disabled.

Setting the HTTPS Port

The commands used to configure the HTTPS port settings begin with *network services https.*

▶ **Change the HTTPS port:**

```
config:#   network services https port <n>
```

▶ **Enable or disable the HTTPS access:**

```
config:#   network services https enabled <option>
```

Variables:

- <n> is a TCP port number between 1 and 65535. The default HTTPS port is 443.
- <option> is one of the options: *true* or *false.*

Option	Description
true	Forces any access to the Legrand PDU via HTTP to be redirected to HTTPS.
false	No HTTP access is redirected to HTTPS.

Changing the Telnet Configuration

You can enable or disable the Telnet service, or change its TCP port using the CLI commands.

A Telnet command begins with *network services telnet.*

Enabling or Disabling Telnet

This command enables or disables the Telnet service.

```
config:#    network services telnet enabled <option>
```

Variables:

- <option> is one of the options: *true* or *false.*

Option	Description
true	The Telnet service is enabled.
false	The Telnet service is disabled.

Changing the Telnet Port

This command changes the Telnet port.

```
config:#    network services telnet port <n>
```

Variables:

- <n> is a TCP port number between 1 and 65535. The default Telnet port is 23.

Changing the SSH Configuration

You can enable or disable the SSH service, or change its TCP port using the CLI commands.

An SSH command begins with *network services ssh.*

Enabling or Disabling SSH

This command enables or disables the SSH service.

```
config:#    network services ssh enabled <option>
```

Variables:

- <option> is one of the options: *true* or *false.*

Option	Description
true	The SSH service is enabled.
false	The SSH service is disabled.

Changing the SSH Port

This command changes the SSH port.

```
config:#   network services ssh port <n>
```

Variables:

- <n> is a TCP port number between 1 and 65535. The default SSH port is 22.

Determining the SSH Authentication Method

This command syntax determines the SSH authentication method.

```
config:#   network services ssh authentication <auth_method>
```

Variables:

- <option> is one of the options: *passwordOnly*, *publicKeyOnly* or *passwordOrPublicKey*.

Option	Description
passwordOnly	Enables the password-based login only.
publicKeyOnly	Enables the public key-based login only.
passwordOrPublicKey	Enables both the password- and public key-based login. This is the default.

If the public key authentication is selected, you must 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 348).

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.

June 2018

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.

June 2018

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 164) for details.

```
config:#   network services zeroconfig enabled <option>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	The zero configuration protocol is enabled.
false	The zero configuration protocol is disabled.

Examples

This section illustrates several network configuration examples.

Example 1 - Networking Mode

The following command enables the wired networking mode.

```
config:#   network mode wired
```

Example 2 - Enabling Both IP Protocols

The following command determines that both IPv4 and IPv6 protocols are enabled.

```
config:#   network ip proto both
```

Example 3 - Wireless Authentication Method

The following command sets the wireless authentication method to PSK.

```
config:#   network wireless authMethod PSK
```

Example 4 - Static IPv4 Configuration

The following command enables the Static IP configuration mode.

```
config:#   network ipv4 ipConfigurationMode static
```

Time Configuration Commands

A time configuration command begins with *time*.

Determining the Time Setup Method

This command determines the method to configure the system date and time.

```
config:#   time method <method>
```

Variables:

- <method> is one of the time setup options: *manual* or *ntp*.

Mode	Description
manual	The date and time settings are customized.
ntp	The date and time settings synchronize with a specified NTP server.

Setting NTP Parameters

A time configuration command 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.
- <option> is one of these options: *true* or *false*.

Mode	Description
true	Customized NTP server settings override the DHCP-specified NTP servers.
false	Customized NTP server settings do NOT override the DHCP-specified NTP servers.

Customizing the Date and Time

If intending to manually configure the date and time, use the following CLI commands to specify them.

Note: You shall set the time configuration method to "manual" prior to customizing the date and time. See **Determining the Time Setup Method** *(on page 320).*

▶ **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 the Legrand PDU.

```
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 savings time is applied to the time settings.

```
config:#   time autoDST <option>
```

Variables:

- <option> is one of the options: *enable* or *disable.*

Mode	Description
enable	Daylight savings time is enabled.
disable	Daylight savings time is disabled.

Examples

This section illustrates several time configuration examples.

Example 1 - Time Setup Method

The following command sets the date and time settings by using the NTP servers.

```
config:#   time method ntp
```

Example 2 - Primary NTP Server

The following command sets the primary time server to 192.168.80.66.

```
config:#   time ntp firstServer 192.168.80.66
```

Checking the Accessibility of NTP Servers

This command verifies the accessibility of NTP servers specified manually on your Legrand PDU and then shows the result. For instructions on specifying NTP servers via CLI, see **Setting NTP Parameters** (on page 320).

To perform this command successfully, you must:

- Own the "Change Date/Time Settings" permission.
- Customize NTP servers. See **Setting NTP Parameters** (on page 320).

This command is available either in the administrator/user mode or in the configuration mode. See **Different CLI Modes and Prompts** (on page 271).

▶ **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 Legrand PDU 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.

Option	Description
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 381).*

Managing Firewall Rules

You can add, delete or modify firewall rules using the CLI commands.

- An IPv4 firewall control rule command begins with *security ipAccessControl ipv4 rule*.
- An IPv6 firewall control rule command begins with *security ipAccessControl ipv6 rule*.

Adding a Firewall Rule

Depending on where you want to add a new firewall rule in the list, the command for adding a rule varies.

- *IPv4 commands*

▶ **Add a new rule to the bottom of the IPv4 rules list:**

```
config:#    security ipAccessControl ipv4 rule add <direction> <ip_mask> <policy>
```

▶ **Add a new IPv4 rule by inserting it above or below a specific rule:**

```
config:#    security ipAccessControl ipv4 rule add <direction> <ip_mask> <policy> <insert>
            <rule_number>

            -- OR --
```

```
config:#    security ipAccessControl ipv4 rule add <direction> <insert> <rule_number>
            <ip_mask> <policy>
```

- *IPv6 commands*

▶ **Add a new rule to the bottom of the IPv6 rules list:**

```
config:#    security ipAccessControl ipv6 rule add <direction> <ip_mask> <policy>
```

▶ **Add a new IPv6 rule by inserting it above or below a specific rule:**

```
config:#    security ipAccessControl ipv6 rule add <direction> <ip_mask> <policy> <insert>
            <rule_number>

            -- OR --
```

```
config:#    security ipAccessControl ipv6 rule add <direction> <insert> <rule_number>
            <ip_mask> <policy>
```

Variables:

- <direction> is one of the options: *in* or *out.*

Direction	Description
in	Inbound traffic.
out	Outbound traffic.

- <ip_mask> is the combination of the IP address and subnet mask values (or prefix length), which are separated with a slash. For example, an IPv4 combination looks like this: *192.168.94.222/24.*
- <policy> is one of the options: *accept, drop* or *reject*.

Policy	Description
accept	Accepts traffic from/to the specified IP address(es).
drop	Discards traffic from/to the specified IP address(es), without sending any failure notification to the source or destination host.
reject	Discards traffic from/to the specified IP address(es), and an ICMP message is sent to the source or destination host for failure notification.

- <insert> is one of the options: *insertAbove* or *insertBelow*.

Option	Description
insertAbove	Inserts the new rule above the specified rule number. Then: *new rule's number = the specified rule number*
insertBelow	Inserts the new rule below the specified rule number. Then: *new rule's number = the specified rule number + 1*

- <rule_number> is the number of the existing rule which you want to insert the new rule above or below.

Modifying a Firewall Rule

Depending on what to modify in an existing rule, the command varies.

- *IPv4 commands*

▶ **Modify an IPv4 rule's IP address and/or subnet mask:**

```
config:#    security ipAccessControl ipv4 rule modify <direction> <rule_number> ipMask
            <ip_mask>
```

▶ **Modify an IPv4 rule's policy:**

```
config:#    security ipAccessControl ipv4 rule modify <direction> <rule_number> policy
            <policy>
```

▶ **Modify all contents of an existing IPv4 rule:**

```
config:#    security ipAccessControl ipv4 rule modify <direction> <rule_number> ipMask
            <ip_mask> policy <policy>
```

- *IPv6 commands*

▶ **Modify an IPv6 rule's IP address and/or prefix length:**

```
config:#    security ipAccessControl ipv6 rule modify <direction> <rule_number> ipMask
            <ip_mask>
```

▶ **Modify an IPv6 rule's policy:**

```
config:#    security ipAccessControl ipv6 rule modify <direction> <rule_number> policy
            <policy>
```

▶ **Modify all contents of an IPv6 existing rule:**

```
config:#    security ipAccessControl ipv6 rule modify <direction> <rule_number> ipMask
            <ip_mask> policy <policy>
```

Variables:

- <direction> is one of the options: *in* or *out*.

Direction	Description
in	Inbound traffic.
out	Outbound traffic.

- <rule_number> is the number of the existing rule that you want to modify.
- <ip_mask> is the combination of the IP address and subnet mask values (or prefix length), which are separated with a slash. For example, an IPv4 combination looks like this: *192.168.94.222/24*.
- <policy> is one of the options: *accept, drop* or *reject*.

Option	Description
accept	Accepts traffic from/to the specified IP address(es).
drop	Discards traffic from/to the specified IP address(es), without sending any failure notification to the source or destination host.
reject	Discards traffic from/to the specified IP address(es), and an ICMP message is sent to the source or destination host for failure notification.

Deleting a Firewall Rule

The following commands remove a specific IPv4 or IPv6 rule from the list.

▶ IPv4 commands

```
config:#   security ipAccessControl ipv4 rule delete <direction> <rule_number>
```

▶ IPv6 commands

```
config:#   security ipAccessControl ipv6 rule delete <direction> <rule_number>
```

Variables:

- <direction> is one of the options: *in* or *out*.

Direction	Description
in	Inbound traffic.
out	Outbound traffic.

- <rule_number> is the number of the existing rule that you want to remove.

Restricted Service Agreement

The CLI command used to set the Restricted Service Agreement feature begins with `security restrictedServiceAgreement,`

Enabling or Disabling the Restricted Service Agreement

This command activates or deactivates the Restricted Service Agreement.

```
config:#   security restrictedServiceAgreement enabled <option>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	Enables the Restricted Service Agreement feature.
false	Disables the Restricted Service Agreement feature.

June 2018

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 293).*

Example

The following example illustrates how to specify the content of the Restricted Service Agreement.

1. Type the following command and press Enter to start entering the content.

```
config:#   security restrictedServiceAgreement bannerContent
```

2. Type the following content when the CLI prompts you to enter the content.

```
IMPORTANT!! You are accessing a PDU. If you are not the system administrator, do
NOT power off or power cycle any outlet without the permission of the system
administrator.
```

3. Press Enter.
4. Type the following:

```
--END--
```

5. Press Enter again.
6. Verify that the message "Successfully entered Restricted Service Agreement" is displayed, indicating that the content input is successful.

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 381).

Single Login Limitation

This command enables or disables the single login feature, which controls whether multiple logins using the same login name simultaneously is permitted.

```
config:#   security loginLimits singleLogin <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	Enables the single login feature.
disable	Disables the single login feature.

June 2018

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 Legrand PDU 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 381).

▶ **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 381).

Enabling or Disabling Strong Passwords

This command enables or disables the strong password feature.

```
config:#    security strongPasswords enabled <option>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	Enables the strong password feature.
false	Disables the strong password feature.

Minimum Password Length

This command determines the minimum length of the password.

```
config:#    security strongPasswords minimumLength <value>
```

Variables:

- <value> is an integer between 8 and 32.

Maximum Password Length

This command determines the maximum length of the password.

```
config:#    security strongPasswords maximumLength <value>
```

Variables:

- <value> is an integer between 16 and 64.

Lowercase Character Requirement

This command determines whether a strong password includes at least a lowercase character.

```
config:#    security strongPasswords enforceAtLeastOneLowerCaseCharacter <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	At least one lowercase character is required.
disable	No lowercase character is required.

Uppercase Character Requirement

This command determines whether a strong password includes at least a uppercase character.

```
config:#    security strongPasswords enforceAtLeastOneUpperCaseCharacter <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	At least one uppercase character is required.
disable	No uppercase character is required.

Numeric Character Requirement

This command determines whether a strong password includes at least a numeric character.

```
config:#    security strongPasswords enforceAtLeastOneNumericCharacter <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	At least one numeric character is required.
disable	No numeric character is required.

Special Character Requirement

This command determines whether a strong password includes at least a special character.

```
config:#    security strongPasswords enforceAtLeastOneSpecialCharacter <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	At least one special character is required.
disable	No special character is required.

Maximum Password History

This command determines the number of previous passwords that CANNOT be repeated when changing the password.

```
config:#    security strongPasswords passwordHistoryDepth <value>
```

Variables:

- <value> is an integer between 1 and 12.

Role-Based Access Control

In addition to firewall access control based on IP addresses, you can configure other access control rules that are based on both IP addresses and users' roles.

- An IPv4 role-based access control command begins with *security roleBasedAccessControl ipv4.*
- An IPv6 role-based access control command begins with *security roleBasedAccessControl ipv6.*

Modifying Role-Based Access Control Parameters

There are different commands for modifying role-based access control parameters.

- *IPv4 commands*

▶ **Enable or disable the IPv4 role-based access control feature:**

```
config:#    security roleBasedAccessControl ipv4 enabled <option>
```

▶ **Determine the IPv4 role-based access control policy:**

```
config:#    security roleBasedAccessControl ipv4 defaultPolicy <policy>
```

- *IPv6 commands*

▶ **Enable or disable the IPv6 role-based access control feature:**

```
config:#    security roleBasedAccessControl ipv6 enabled <option>
```

▶ **Determine the IPv6 role-based access control policy:**

```
config:#   security roleBasedAccessControl ipv6 defaultPolicy <policy>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	Enables the role-based access control feature.
false	Disables the role-based access control feature.

- <policy> is one of the options: *allow* or *deny*.

Policy	Description
allow	Accepts traffic from all IP addresses regardless of the user's role.
deny	Drops traffic from all IP addresses regardless of the user's role.

Tip: You can combine both commands to modify all role-based access control parameters at a time. See **Multi-Command Syntax** *(on page 381).*

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 Outlet Switching

This section applies to outlet-switching capable models only.

The following CLI commands control whether you can turn on or off an outlet by operating the front panel display.

▶ **To enable the front panel outlet control feature:**

```
config:#    security frontPanelPermissions add switchOutlet
```

▶ **To disable the front panel outlet control feature:**

```
config:#    security frontPanelPermissions remove switchOutlet
```

Enabling or Disabling Front Panel Actuator Control

The following CLI commands control whether you can turn on or off a connected actuator 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 PDU 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 outlet switching functions simultaneously.
security frontPanelPermissions add switchActuator;switchOutlet

---

Examples

This section illustrates several security configuration examples.

Example 1 - IPv4 Firewall Control Configuration

The following command sets up two parameters of the IPv4 access control feature.

```
config:#    security ipAccessControl ipv4 enabled true defaultPolicyIn accept
            defaultPolicyOut accept
```

Results:

- The IPv4 access control feature is enabled.
- The default policy for inbound traffic is set to "accept."
- The default policy for outbound traffic is set to "accept."

Example 2 - Adding an IPv4 Firewall Rule

The following command adds a new IPv4 access control rule and specifies its location in the list.

```
config:#    security ipAccessControl ipv4 rule add 192.168.84.123/24 accept
            insertAbove 5
```

Results:

- A new IPv4 firewall control rule is added to accept all packets sent from the IPv4 address 192.168.84.123.
- The newly-added rule is inserted above the 5th rule. That is, the new rule becomes the 5th rule, and the original 5th rule becomes the 6th rule.

Example 3 - User Blocking

The following command sets up two user blocking parameters.

```
config:#    security userBlocking maximumNumberOfFailedLogins 5 blockTime 30
```

Results:

- The maximum number of failed logins is set to 5.
- The user blocking time is set to 30 minutes.

Example 4 - Adding an IPv4 Role-based Access Control Rule

The following command creates a newIPv4 role-based access control rule and specifies its location in the list.

```
config:#    security roleBasedAccessControl ipv4 rule add 192.168.78.50 192.168.90.100
            admin deny insertAbove 3
```

Results:

- A new IPv4 role-based access control rule is added, dropping all packets from any IPv4 address between 192.168.78.50 and 192.168.90.100 when the user is a member of the role "admin."
- The newly-added IPv4 rule is inserted above the 3rd rule. That is, the new rule becomes the 3rd rule, and the original 3rd rule becomes the 4th rule.

Outlet Configuration Commands

An outlet configuration command begins with *outlet*. Such a command allows you to configure an individual outlet.

Changing the Outlet Name

This command names an outlet.

```
config:#   outlet <n> name "<name>"
```

Variables:

- <n> is the number of the outlet that you want to configure.
- <name> is a string comprising up to 64 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.

Changing an Outlet's Default State

This section applies to outlet-switching capable models only.

This command determines the initial power condition of an outlet after the Legrand PDU powers up.

```
config:#   outlet <n> stateOnDeviceStartup <option>
```

Variables:

- <n> is the number of the outlet that you want to configure.
- <option> is one of the options: *off*, *on, lastKnownState* and *pduDefined.*

Option	Description
off	Turn off the outlet.
on	Turn on the outlet.
lastKnownState	Restore the outlet to the state prior to last PDU power down.
pduDefined	PDU-defined setting.

Note: Setting the outlet's default state to an option other than pduDefined *overrides the PDU-defined default state on that outlet. See* **Setting the PDU-Defined Default Outlet State** *(on page 295).*

Setting an Outlet's Cycling Power-Off Period

This section applies to outlet-switching capable models only.

This command determines the power-off period of the power cycling operation for a specific outlet.

```
config:#    outlet <n> cyclingPowerOffPeriod <timing>
```

Variables:

- <n> is the number of the outlet that you want to configure.
- <timing> is the time of the cycling power-off period in seconds, which is an integer between 0 and 3600, or *pduDefined* for following the PDU-defined timing.

Note: This setting overrides the PDU-defined cycling power-off period on a particular outlet. See **Setting the PDU-Defined Cycling Power-Off Period** *(on page 295).*

Example - Outlet Naming

The following command assigns the name "Win XP" to outlet 8.

```
config:#    outlet 8 name "Win XP"
```

Inlet Configuration Commands

An inlet configuration command begins with *inlet*. You can configure an inlet by using the inlet configuration command.

Changing the Inlet Name

This command syntax names an inlet.

```
config:#    inlet <n> name "<name>"
```

Variables:

- <n> is the number of the inlet that you want to configure. For a single-inlet PDU, <n> is always 1. The value is an integer between 1 and 50.
- <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 an Inlet (for Multi-Inlet PDUs)

> Enabling or disabling an inlet takes effect on a multi-inlet PDU only.

This command enables or disables an inlet.

```
config:#    inlet <n> enabled <option>
```

Variables:

- <n> is the number of the inlet that you want to configure. For a single-inlet PDU, <n> is always 1. The value is an integer between 1 and 50.
- <option> is one of the options: *true* or *false*.

Option	Description
true	The specified inlet is enabled.
false	The specified inlet is disabled.

Note: If performing this command causes all inlets to be disabled, a warning message appears, prompting you to confirm. When this occurs, press y to confirm or n to cancel the operation.

Example - Inlet Naming

The following command assigns the name "AC source" to the inlet 1. If your Legrand PDU contains multiple inlets, this command names the 1st inlet.

```
config:#    inlet 1 name "AC source"
```

Overcurrent Protector Configuration Commands

An overcurrent protector configuration command begins with *ocp.* The command configures an individual circuit breaker or fuse which protects outlets.

Changing the Overcurrent Protector Name

This command names a circuit breaker or a fuse which protects outlets on your Legrand PDU.

```
config:#    ocp <n> name "<name>"
```

Variables:

- <n> is the number of the overcurrent protector that you want to configure. The value is an integer between 1 and 50.
- <name> is a string comprising up to 64 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.

Example - OCP Naming

The command assigns the name "Email servers CB" to the overcurrent protector labeled 2.

```
config:#    ocp 2 name "Email servers CB"
```

June 2018

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 Legrand PDU 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 381).*

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, Legrand PDU 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 293).

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 381).

▶ **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 Legrand PDU only after that user's user profile is enabled.

```
config:#   user modify <name> enabled <option>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option> is one of the options: *true* or *false*.

Option	Description
true	Enables the specified user profile.
false	Disables the specified user profile.

Forcing a Password Change

This command determines whether the password change is forced when a user logs in to the specified user profile next time.

```
config:#   user modify <name> forcePasswordChangeOnNextLogin <option>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option> is one of the options: *true* or *false*.

Option	Description
true	A password change is forced on the user's next login.
false	No password change is forced on the user's next login.

Modifying SNMPv3 Settings

There are different commands to modify the SNMPv3 parameters of a specific user profile. You can combine all of the following commands to modify the SNMPv3 parameters at a time. See **Multi-Command Syntax** (on page 381).

▶ **Enable or disable the SNMP v3 access to Legrand PDU for the specified user:**

```
config:#   user modify <name> snmpV3Access <option1>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option1> is one of the options: *enable* or *disable*.

Option	Description
enable	Enables the SNMP v3 access permission for the specified user.
disable	Disables the SNMP v3 access permission for the specified user.

▶ **Determine the security level:**

```
config:#   user modify <name> securityLevel <option2>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option2> is one of the options: *noAuthNoPriv*, *authNoPriv* or *authPriv*.

Option	Description
noAuthNoPriv	No authentication and no privacy.

Option	Description
authNoPriv	Authentication and no privacy.
authPriv	Authentication and privacy.

▶ **Determine whether the authentication passphrase is identical to the password:**

```
config:#   user modify <name> userPasswordAsAuthenticationPassphrase <option3>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option3> is one of the options: *true* or *false*.

Option	Description
true	Authentication passphrase is identical to the password.
false	Authentication passphrase is different from the password.

▶ **Determine the authentication passphrase:**

```
config:#   user modify <name> authenticationPassPhrase <authentication_passphrase>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <authentication_passphrase> is a string used as an authentication passphrase, comprising 8 to 32 ASCII printable characters.

▶ **Determine whether the privacy passphrase is identical to the authentication passphrase:**

```
config:#   user modify <name> useAuthenticationPassPhraseAsPrivacyPassPhrase <option4>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option4> is one of the options: *true* or *false*.

Option	Description
true	Privacy passphrase is identical to the authentication passphrase.
false	Privacy passphrase is different from the authentication passphrase.

▶ **Determine the privacy passphrase:**

```
config:#   user modify <name> privacyPassPhrase <privacy_passphrase>
```

Variables:

* <name> is the name of the user whose settings you want to change.
* <privacy_passphrase> is a string used as a privacy passphrase, comprising 8 to 32 ASCII printable characters.

▶ **Determine the authentication protocol:**

```
config:#   user modify <name> authenticationProtocol <option5>
```

Variables:

* <name> is the name of the user whose settings you want to change.
* <option5> is one of the options: *MD5* or *SHA-1*.

Option	Description
MD5	MD5 authentication protocol is applied.
SHA-1	SHA-1 authentication protocol is applied.

▶ **Determine the privacy protocol:**

```
config:#   user modify <name> privacyProtocol <option6>
```

Variables:

* <name> is the name of the user whose settings you want to change.
* <option6> is one of the options: *DES* or *AES-128*.

Option	Description
DES	DES privacy protocol is applied.
AES-128	AES-128 privacy protocol is applied.

Changing the Role(s)

This command changes the role(s) of a specific user.

```
config:#   user modify <name> roles <roles>
```

Variables:

* <name> is the name of the user whose settings you want to change.
* <roles> is a role or a list of comma-separated roles assigned to the specified user profile. See ***All Privileges*** (on page 351).

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 381).

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

Tip: To set the default measurement units applied to the Legrand PDU user interfaces for all users via CLI, see **Setting Default Measurement Units** *(on page 349).*

▶ **Set the preferred temperature unit:**

```
config:#    user modify <name> preferredTemperatureUnit <option1>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option1> is one of the options: *C or F.*

Option	Description
C	This option displays the temperature in Celsius.
F	This option displays the temperature in Fahrenheit.

▶ **Set the preferred length unit:**

```
config:#    user modify <name> preferredLengthUnit <option2>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option2> is one of the options: *meter or feet.*

Option	Description
meter	This option displays the length or height in meters.
feet	This option displays the length or height in feet.

▶ **Set the preferred pressure unit:**

```
config:#    user modify <name> preferredPressureUnit <option3>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option3> is one of the options: *pascal or psi.*

Option	Description
pascal	This option displays the pressure value in Pascals (Pa).
psi	This option displays the pressure value in psi.

Specifying the SSH Public Key

If the SSH key-based authentication is enabled, specify the SSH public key for each user profile using the following procedure.

▶ **To specify or change the SSH public key for a specific user:**

1. Type the SSH public key command as shown below and press Enter.

   ```
   config:#   user modify <name> sshPublicKey
   ```

2. The system prompts you to enter the contents of the SSH public key. Do the following to input the contents:
   a. Open your SSH public key with a text editor.
   b. Copy all contents in the text editor.
   c. Paste the contents into the terminal.
   d. Press Enter.

▶ **To remove an existing SSH public key:**

1. Type the same command as shown above.
2. When the system prompts you to input the contents, press Enter without typing or pasting anything.

Example

The following procedure illustrates how to change the SSH public key for the user "assistant."

1. Verify that you have entered the configuration mode. See *Entering Configuration Mode* (on page 293).
2. Type the following command and press Enter.

   ```
   config:#   user modify assistant sshPublicKey
   ```

3. You are prompted to enter a new SSH public key.
4. Type the new key and press Enter.

Deleting a User Profile

This command deletes an existing user profile.

```
config:#   user delete <name>
```

Changing Your Own Password

Every user can change their own password via this command if they have the Change Own Password privilege. Note that this command does not begin with *user*.

```
config:#   password
```

After performing this command, the Legrand PDU 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 293).
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 Legrand PDU 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 381).

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 Legrand PDU user interfaces for a specific user via CLI, see **Changing Measurement Units** (on page 347).*

▶ **Set the default temperature unit:**

`config:#   user defaultpreferences preferredTemperatureUnit <option1>`

Variables:

• <option1> is one of the options: *C* or *F*.

Option	Description
C	This option displays the temperature in Celsius.
F	This option displays the temperature in Fahrenheit.

▶ **Set the default length unit:**

`config:#   user defaultpreferences preferredLengthUnit <option2>`

Variables:

• <option2> is one of the options: *meter* or *feet*.

Option	Description
meter	This option displays the length or height in meters.
feet	This option displays the length or height in feet.

▶ **Set the default pressure unit:**

```
config:#   user defaultpreferences preferredPressureUnit <option3>
```

Variables:

- <option3> is one of the options: *pascal* or *psi.*

Option	Description
pascal	This option displays the pressure value in Pascals (Pa).
psi	This option displays the pressure value in psi.

Examples

This section illustrates several user configuration examples.

Example 1 - Creating a User Profile

The following command creates a new user profile and sets two parameters for the new user.

```
config:#   user create May enable admin
```

Results:

- A new user profile "May" is created.
- The new user profile is enabled.
- The **admin** role is assigned to the new user profile.

Example 2 - Modifying a User's Roles

The following command assigns two roles to the user "May."

```
config:#   user modify May roles admin,tester
```

Results:

- The user May has the union of all privileges of "admin" and "tester."

Example 3 - Default Measurement Units

The following command sets all default measurement units at a time.

```
config:#    user defaultpreferences preferredTemperatureUnit F preferredLengthUnit feet
            preferredPressureUnit psi
```

Results:

- The default temperature unit is set to Fahrenheit.
- The default length unit is set to feet.
- The default pressure unit is set to psi.

Role Configuration Commands

A role configuration command begins with *role*.

Creating a Role

This command creates a new role, with a list of semicolon-separated privileges assigned to the role.

```
config:#    role create <name> <privilege1>;<privilege2>;<privilege3>...
```

If a specific privilege contains any arguments, that privilege should be followed by a colon and the argument(s).

```
config:#    role create <name> <privilege1>:<argument1>,<argument2>...;
            <privilege2>:<argument1>,<argument2>...;
            <privilege3>:<argument1>,<argument2>...;
            ...
```

Variables:

- <name> is a string comprising up to 32 ASCII printable characters.
- <privilege1>, <privilege2>, <privilege3> and the like are names of the privileges assigned to the role. Separate each privilege with a semi-colon. See *All Privileges* (on page 351).
- <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. Note that available privileges vary according to the model you purchased. For example, a PDU without the outlet switching function does not have the privilege "switchOutlet."

Privilege	Description
acknowledgeAlarms	Acknowledge Alarms
adminPrivilege	Administrator Privileges
changeAssetStripConfiguration	Change Asset Strip Configuration
changeAuthSettings	Change Authentication Settings

Privilege	Description
changeDataTimeSettings	Change Date/Time Settings
changeExternalSensorsConfiguration	Change Peripheral Device Configuration
changeLhxConfiguration	Change LHX/SHX Configuration
changeModemConfiguration	Change Modem Configuration
changeNetworkSettings	Change Network Settings
changePassword	Change Own Password
changePduConfiguration	Change Pdu, Inlet, Outlet & Overcurrent Protector Configuration
changeSecuritySettings	Change Security Settings
changeSnmpSettings	Change SNMP Settings
changeUserSettings	Change Local User Management
changeWebcamSettings	Change Webcam Configuration
clearLog	Clear Local Event Log
firmwareUpdate	Firmware Update
performReset	Reset (Warm Start)
switchActuator*	Switch Actuator
switchOutlet**	Switch Outlet
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 Legrand PDU web interface. It is an integer between 1 and 32.

** The "switchOutlet" privilege requires an argument that is separated with a colon. The argument could be:

- All outlets, that is,

  ```
  switchOutlet:all
  ```

- An outlet number. For example:

  ```
  switchOutlet:1
  switchOutlet:2
  switchOutlet:3
  ```

- A list of comma-separated outlets. For example:

  ```
  switchOutlet:1,3,5,7,8,9
  ```

Modifying a Role

You can modify diverse parameters of an existing role, including its privileges.

▶ **Modify a role's description:**

```
config:#   role modify <name> description "<description>"
```

Variables:

- <name> is a string comprising up to 32 ASCII printable characters.
- <description> is a description comprising alphanumeric characters. The <description> variable must be enclosed in quotes when it contains spaces.

▶ **Add more privileges to a specific role:**

```
config:#   role modify <name> addPrivileges
           <privilege1>;<privilege2>;<privilege3>...
```

If a specific privilege contains any arguments, add a colon and the argument(s) after that privilege.

```
config:#    role modify <name> addPrivileges
            <privilege1>:<argument1>,<argument2>...;
            <privilege2>:<argument1>,<argument2>...;
            <privilege3>:<argument1>,<argument2>...;
            ...
```

Variables:

- <name> is a string comprising up to 32 ASCII printable characters.
- <privilege1>, <privilege2>, <privilege3> and the like are names of the privileges assigned to the role. Separate each privilege with a semi-colon. See ***All Privileges*** (on page 351).
- <argument1>, <argument2> and the like are arguments set for a particular privilege. Separate a privilege and its argument(s) with a colon, and separate arguments with a comma if there are more than one argument for a privilege.

▶ **Remove specific privileges from a role:**

```
config:#    role modify <name> removePrivileges
            <privilege1>;<privilege2>;<privilege3>...
```

If a specific privilege contains any arguments, add a colon and the argument(s) after that privilege.

```
config:#    role modify <name> removePrivileges
            <privilege1>:<argument1>,<argument2>...;
            <privilege2>:<argument1>,<argument2>...;
            <privilege3>:<argument1>,<argument2>...;
            ...
```

Note: When removing privileges from a role, make sure the specified privileges and arguments (if any) exactly match those assigned to the role. Otherwise, the command fails to remove specified privileges that are not available.

Variables:

- <name> is a string comprising up to 32 ASCII printable characters.
- <privilege1>, <privilege2>, <privilege3> and the like are names of the privileges assigned to the role. Separate each privilege with a semi-colon. See ***All Privileges*** (on page 351).
- <argument1>, <argument2> and the like are arguments set for a particular privilege. Separate a privilege and its argument(s) with a colon, and separate arguments with a comma if there are more than one argument for a privilege.

Deleting a Role

This command deletes an existing role.

```
config:#    role delete <name>
```

Example - Creating a Role

The following command creates a new role and assigns privileges to the role.

```
config:#   role create tester firmwareUpdate;viewEventSetup
```

Results:

- A new role "tester" is created.
- Two privileges are assigned to the role: firmwareUpdate (Firmware Update) and viewEventSetup (View Event Settings).

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.
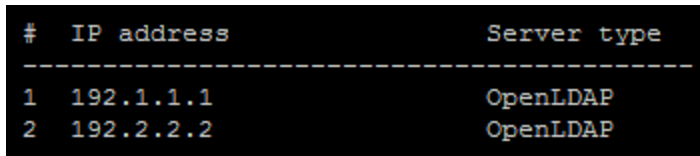
Tip: If any LDAP server's settings are identical to an existing LDAP server's, you can add it by just copying the existing one, instead of using the following command. See **Copying an Existing Server's Settings** *(on page 359).*

▶ **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 357). 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 286).*

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 358).
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 358).
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
```

    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 Legrand PDU. See **Authentication Settings** (on page 286).

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":**

June 2018

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`
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`

June 2018

Parameters	Description
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 356).*

► **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:**

June 2018

```
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.

▶ **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 376).*

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 Legrand PDU web interface or using the command "show externalsensors <n>" in the CLI. It is an integer between 1 and 32.
- <name> is a string comprising up to 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 376).*

Specifying the CC Sensor Type

Raritan's contact closure sensor (DPX-CC2-TR) supports the connection of diverse third-party or Raritan's detectors/switches. You must specify the type of connected detector/switch for proper operation. Use this command when you need to specify the sensor type.

```
config:#   externalsensor <n> sensorSubType <sensor_type>
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is available in the Legrand PDU web interface or using the command "show externalsensors <n>" in the CLI. It is an integer between 1 and 32.
- <sensor_type> is one of these types: *contact*, *smokeDetection*, *waterDetection* or *vibration*.

Type	Description
contact	The connected detector/switch is for detection of door lock or door closed/open status.
smokeDetection	The connected detector/switch is for detection of the smoke presence.
waterDetection	The connected detector/switch is for detection of the water presence.
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 Legrand PDU web interface or using the command "show externalsensors <n>" in the CLI. It is an integer between 1 and 32.
- <coordinate> is a string comprising up to 24 ASCII printable characters, and it must be enclosed in quotes.

Setting the Y Coordinate

This command specifies the Y coordinate of an environmental sensor.

```
config:#   externalsensor <n> ylabel "<coordinate>"
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is available in the Legrand PDU web interface or using the command "`show externalsensors <n>`" in the CLI. It is an integer between 1 and 32.
- <coordinate> is a string comprising up to 24 ASCII printable characters, and it must be enclosed in quotes.

Setting the Z Coordinate

This command specifies the Z coordinate of an environmental sensor.

```
config:#   externalsensor <n> zlabel "<coordinate>"
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is available in the Legrand PDU web interface or using the command "`show externalsensors <n>`" in the CLI. It is an integer between 1 and 32.
- Depending on the Z coordinate format you set, there are two types of values for the <coordinate> variable:

Type	Description
Free form	<coordinate> is a string comprising up to 24 ASCII printable characters, and it must be enclosed in quotes.
Rack units	<coordinate> is an integer number in rack units.

Note: To specify the Z coordinate using the rack units, see **Setting the Z Coordinate Format for Environmental Sensors** *(on page 298).*

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 Legrand PDU web interface or using the command "`show externalsensors <n>`" in the CLI. It is an integer between 1 and 32.
- <description> is a string comprising up to 64 ASCII printable characters, and it must be enclosed in quotes.

Using Default Thresholds

This command determines whether default thresholds, including the deassertion hysteresis and assertion timeout, are applied to a specific environmental sensor.

```
config:#    externalsensor <n> useDefaultThresholds <option>
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is available in the Legrand PDU web interface or using the command "`show externalsensors <n>`" in the CLI. It is an integer between 1 and 32.
- <option> is one of the options: *true* or *false*.

Option	Description
true	Default thresholds are selected as the threshold option for the specified sensor.
false	Sensor-specific thresholds are selected as the threshold option for the specified sensor.

Setting the Alarmed to Normal Delay for DX-PIR

This command determines the value of the Alarmed to Normal Delay setting for a DX-PIR presence detector.

```
config:#    externalsensor <n> alarmedToNormalDelay <time>
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is available in the Legrand PDU web interface or using the command "`show externalsensors <n>`" in the CLI. It is an integer between 1 and 32.
- <time> is an integer number in seconds, ranging between 0 and 300.

Examples

This section illustrates several environmental sensor configuration examples.

Example 1 - Environmental Sensor Naming

The following command assigns the name "Cabinet humidity" to the environmental sensor with the ID number 4.

```
config:#    externalsensor 4 name "Cabinet humidity"
```

Example 2 - Sensor Threshold Selection

The following command sets the environmental sensor #1 to use the default thresholds, including the deassertion hysteresis and assertion timeout, as its threshold settings.

```
config:#    externalsensor 1 useDefaultThresholds true
```

June 2018

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 381).

▶ **Set the Default Upper Critical Threshold for a specific sensor type:**

```
config:#    defaultThresholds <sensor type> upperCritical <value>
```

▶ **Set the Default Upper Warning Threshold for a specific sensor type:**

```
config:#    defaultThresholds <sensor type> upperWarning <value>
```

▶ **Set the Default Lower Critical Threshold for a specific sensor type:**

```
config:#    defaultThresholds <sensor type> lowerCritical <value>
```

▶ **Set the Default Lower Warning Threshold for a specific sensor type:**

```
config:#    defaultThresholds <sensor type> lowerWarning <value>
```

▶ **Set the Default Deassertion Hysteresis for a specific sensor type:**

```
config:#    defaultThresholds <sensor type> hysteresis <hy_value>
```

▶ **Set the Default Assertion Timeout for a specific sensor type:**

```
config:#    defaultThresholds <sensor type> assertionTimeout <as_value>
```

Variables:

- <sensor type> is one of the following numeric sensor types:

Sensor types	Description
absoluteHumidity	Absolute humidity sensors
relativeHumidity	Relative humidity sensors
temperature	Temperature sensors
airPressure	Air pressure sensors
airFlow	Air flow sensors
vibration	Vibration sensors

- <value> is the value for the specified threshold of the specified sensor type. Note that diverse sensor types use different measurement units.

Sensor types	Measurement units
absoluteHumidity	g/m^3 (that is, g/m^3)

Sensor types	Measurement units
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
```

Sensor Threshold Configuration Commands

A sensor configuration command begins with *sensor*. You can use the commands to configure the threshold, hysteresis and assertion timeout values for any sensor associated with the following items:

- Inlets
- Inlet poles (for three-phase PDUs only)
- Overcurrent protectors
- Environmental sensors

It is permitted to assign a new value to the threshold at any time regardless of whether the threshold has been enabled.

Commands for Inlet Sensors

A sensor configuration command for inlets begins with *sensor inlet*.

You can configure various inlet sensor threshold settings at a time by combining multiple commands. See **Multi-Command Syntax** (on page 381).

▶ **Set the Upper Critical threshold for an inlet sensor:**

```
config:#    sensor inlet <n> <sensor type> upperCritical <option>
```

▶ **Set the Upper Warning threshold for an inlet sensor:**

```
config:#    sensor inlet <n> <sensor type> upperWarning <option>
```

▶ **Set the Lower Critical threshold for an inlet sensor:**

```
config:#    sensor inlet <n> <sensor type> lowerCritical <option>
```

▶ **Set the Lower Warning threshold for an inlet sensor:**

```
config:#    sensor inlet <n> <sensor type> lowerWarning <option>
```

▶ **Set the deassertion hysteresis for an inlet sensor:**

```
config:#    sensor inlet <n> <sensor type> hysteresis <hy_value>
```

▶ **Set the assertion timeout for an inlet sensor:**

```
config:#    sensor inlet <n> <sensor type> assertionTimeout <as_value>
```

Variables:

- <n> is the number of the inlet that you want to configure. For a single-inlet PDU, <n> is always 1.
- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor
unbalancedCurrent	Unbalanced load sensor
lineFrequency	Line frequency sensor
phaseAngle	Inlet phase angle sensor

Note: If the requested sensor type is not supported, the "Sensor is not available" message is displayed.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the specified threshold for a specific inlet sensor.
disable	Disables the specified threshold for a specific inlet sensor.

Option	Description
A numeric value	Sets a value for the specified threshold of a specific inlet sensor and enables this threshold at the same time.

- <hy_value> is a numeric value that is assigned to the hysteresis for the specified inlet sensor. See **"To De-assert" and Deassertion Hysteresis** (on page 477).
- <as_value> is a numeric value that is assigned to the assertion timeout for the specified inlet sensor. See **"To Assert" and Assertion Timeout** (on page 475).

▶ **Additional sensors supported by Legrand PDUs:**

The CLI command(s) listed above can be also applied to the following sensors. Note that the measurement unit of current values in CLI is **A**, not mA.

Sensor type	Description
peakCurrent	Peak current sensor
reactivePower	Reactive power sensor
displacementPowerFactor	Displacement power factor sensor
phaseAngle	Inlet phase angle sensor

Commands for Inlet Pole Sensors

A sensor configuration command for inlet poles begins with *sensor inletpole*. This type of command is available on a three-phase PDU only.

You can configure various inlet pole sensor threshold settings at a time by combining multiple commands. See **Multi-Command Syntax** (on page 381).

▶ **Set the Upper Critical Threshold for an Inlet Pole:**

```
config:#   sensor inletpole <n> <p> <sensor type> upperCritical <option>
```

▶ **Set the Upper Warning Threshold for an Inlet Pole:**

```
config:#   sensor inletpole <n> <p> <sensor type> upperWarning <option>
```

▶ **Set the Lower Critical Threshold for an Inlet Pole:**

```
config:#   sensor inletpole <n> <p> <sensor type> lowerCritical <option>
```

▶ **Set the Lower Warning Threshold for an Inlet Pole:**

```
config:#   sensor inletpole <n> <p> <sensor type> lowerWarning <option>
```

▶ **Set the Inlet Pole's Deassertion Hysteresis:**

```
config:#   sensor inletpole <n> <p> <sensor type> hysteresis <hy_value>
```

▶ **Set the Inlet Pole's Assertion Timeout:**

```
config:#   sensor inletpole <n> <p> <sensor type> assertionTimeout <as_value>
```

Variables:

- <n> is the number of the inlet whose pole sensors you want to configure. For a single-inlet PDU, <n> is always 1.
- <p> is the label of the inlet pole that you want to configure.

Pole	Label <p>	Current sensor	Voltage sensor
1	**L1**	L1	L1 - L2
2	**L2**	L2	L2 - L3
3	**L3**	L3	L3 - L1

- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor
unbalancedCurrent	Unbalanced load sensor

Note: If the requested sensor type is not supported, the "Sensor is not available" message is displayed.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the specified threshold for the specified inlet pole sensor.
disable	Disables the specified threshold for the specified inlet pole sensor.
A numeric value	Sets a value for the specified threshold of the specified inlet pole sensor and enables this threshold at the same time.

- <hy_value> is a numeric value that is assigned to the hysteresis for the specified inlet pole sensor. See *"To De-assert" and Deassertion Hysteresis* (on page 477).
- <as_value> is a number in samples that is assigned to the assertion timeout for the specified inlet pole sensor. See *"To Assert" and Assertion Timeout* (on page 475).

▶ **Additional sensors supported by Legrand PDUs:**

The CLI command(s) listed above can be also applied to the following sensors. Note that the measurement unit of current values in CLI is **A**, not mA.

Sensor type	Description
peakCurrent	Peak current sensor
reactivePower	Reactive power sensor
displacementPowerFactor	Displacement power factor sensor
phaseAngle	Inlet phase angle sensor

Commands for Overcurrent Protector Sensors

A sensor configuration command for overcurrent protectors begins with *sensor ocp*.

You can configure various overcurrent protector threshold settings at a time by combining multiple commands. See *Multi-Command Syntax* (on page 381).

▶ **Set the Upper Critical threshold for an overcurrent protector:**

```
config:#   sensor ocp <n> <sensor type> upperCritical <option>
```

▶ **Set the Upper Warning threshold for an overcurrent protector:**

```
config:#   sensor ocp <n> <sensor type> upperWarning <option>
```

▶ **Set the Lower Critical threshold for an overcurrent protector:**

```
config:#   sensor ocp <n> <sensor type> lowerCritical <option>
```

▶ **Set the Lower Warning threshold for an overcurrent protector:**

```
config:#   sensor ocp <n> <sensor type> lowerWarning <option>
```

▶ **Set the deassertion hysteresis for an overcurrent protector:**

```
config:#   sensor ocp <n> <sensor type> hysteresis <hy_value>
```

▶ **Set the assertion timeout for an overcurrent protector:**

```
config:#    sensor ocp <n> <sensor type> assertionTimeout <as_value>
```

Variables:

- <n> is the number of the overcurrent protector that you want to configure.
- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor

Note: If the requested sensor type is not supported, the "Sensor is not available" message is displayed.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the specified threshold for the overcurrent protector sensor.
disable	Disables the specified threshold for the overcurrent protector sensor.
A numeric value	Sets a value for the specified threshold of the overcurrent protector sensor and enables this threshold at the same time.

- <hy_value> is a numeric value that is assigned to the hysteresis for the specified overcurrent protector sensor. See **"To De-assert" and Deassertion Hysteresis** (on page 477).
- <as_value> is a number in samples that is assigned to the assertion timeout for the specified overcurrent protector sensor. See **"To Assert" and Assertion Timeout** (on page 475).

Commands for Environmental Sensors

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 381).

▶ **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 Legrand PDU web interface or using the command "show externalsensors <n>" in the CLI. It is an integer between 1 and 32.
- <sensor type> is one of these sensor types: *temperature, absoluteHumidity, relativeHumidity, airPressure, airFlow* or *vibration.*

  Note: If the specified sensor type does not match the type of the specified environmental sensor, this error message appears: "Specified sensor type 'XXX' does not match the sensor's type (<sensortype>)," where XXX is the specified sensor type, and <sensortype> is the correct sensor type.

- <option> is one of the options: *enable, disable* or a numeric value.

Option	Description
enable	Enables the specified threshold for a specific environmental sensor.
disable	Disables the specified threshold for a specific environmental sensor.
A numeric value	Sets a value for the specified threshold of a specific environmental sensor and enables this threshold at the same time.

- <hy_value> is a numeric value that is assigned to the hysteresis for the specified environmental sensor. See ***"To De-assert" and Deassertion Hysteresis*** (on page 477).
- <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 475).

Examples

This section illustrates several environmental sensor threshold configuration examples.

Example 1 - Upper Critical Threshold for a Temperature Sensor

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
```

Example 2 - Warning Thresholds for Inlet Sensors

The following command sets both the Upper Warning and Lower Warning thresholds for the inlet 1 RMS current.

```
config:#   sensor inlet 1 current upperWarning 20 lowerWarning 12
```

Results:

- The Upper Warning threshold for the inlet 1 RMS current is set to 20A. It also enables the upper warning threshold if this threshold has not been enabled yet.
- The Lower Warning threshold for the inlet 1 RMS current is set to 12A. It also enables the lower warning threshold if this threshold has not been enabled yet.

Example 3 - Upper Thresholds for Overcurrent Protector Sensors

The following command sets both the Upper Critical and Upper Warning thresholds for the 2nd overcurrent protector.

```
config:#   sensor ocp 2 current upperWarning enable upperCritical 16
```

Results:

- The Upper Critical threshold for the 2nd overcurrent protector's RMS current is set to 16A. It also enables the upper critical threshold if this threshold has not been enabled yet.
- The Upper Warning threshold for the 2nd overcurrent protector's RMS current is enabled.

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 381).

▶ **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 Legrand PDU 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 298).*

- <description> is a sentence or paragraph comprising up to 64 ASCII printable characters, and it must be enclosed in quotes.

Example - Actuator Naming

The following command assigns the name "Door lock" to the actuator whose ID number is 9.

```
config:#   actuator 9 name "Door lock"
```

Server Reachability Configuration Commands

You can use the CLI to add or delete an IT device, such as a server, from the server reachability list, or modify the settings for a monitored IT device. A server reachability configuration command begins with *serverReachability*.

Adding a Monitored Device

This command adds a new IT device to the server reachability list.

```
config:#    serverReachability add <IP_host> <enable> <succ_ping>
            <fail_ping> <succ_wait> <fail_wait> <resume> <disable_count>
```

Variables:

- <IP_host> is the IP address or host name of the IT device that you want to add.
- <enable> is one of the options: *true* or *false*.

Option	Description
true	Enables the ping monitoring feature for the newly added device.
false	Disables the ping monitoring feature for the newly added device.

- <succ_ping> is the number of successful pings for declaring the monitored device "Reachable." Valid range is 0 to 200.
- <fail_ping> is the number of consecutive unsuccessful pings for declaring the monitored device "Unreachable." Valid range is 1 to 100.
- <succ_wait> is the wait time to send the next ping after a successful ping. Valid range is 5 to 600 (seconds).
- <fail_wait> is the wait time to send the next ping after a unsuccessful ping. Valid range is 3 to 600 (seconds).
- <resume> is the wait time before the Legrand PDU 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 Legrand PDU 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 381).

▶ **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.

![Legrand logo](logo)

- <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 Legrand PDU 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 Legrand PDU 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
```

EnergyWise Configuration Commands

An EnergyWise configuration command begins with *energywise.*

Enabling or Disabling EnergyWise

This command syntax determines whether the Cisco® EnergyWise endpoint implemented on the Legrand PDU is enabled.

```
config:#    energywise enabled <option>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	The Cisco EnergyWise feature is enabled.
false	The Cisco EnergyWise feature is disabled.

June 2018

Legrand PDU User Guide   379

Specifying the EnergyWise Domain

This command syntax specifies to which Cisco® EnergyWise domain the Legrand PDU belongs.

```
config:#   energywise domain <name>
```

Variables:

- <name> is a string comprising up to 127 ASCII printable characters. Spaces and asterisks are NOT acceptable.

Specifying the EnergyWise Secret

This command syntax specifies the password (secret) to enter the Cisco® EnergyWise domain.

```
config:#   energywise secret <password>
```

Variables:

- <password> is a string comprising up to 127 ASCII printable characters. Spaces and asterisks are NOT acceptable.

Changing the UDP Port

This command syntax specifies the UDP port for communications in the Cisco® EnergyWise domain.

```
config:#   energywise port <port>
```

Variables:

- <port> is the UDP port number ranging between 1 and 65535.

Setting the Polling Interval

This command syntax determines the polling interval at which the Cisco® EnergyWise domain queries the Legrand PDU.

```
config:#   energywise polling <timing>
```

Variables:

- <timing> is an integer number in seconds. It ranges between 30 and 600 seconds.

Example - Setting Up EnergyWise

The following command sets up two Cisco® EnergyWise-related features.

```
config:#   energywise enabled true port 10288
```

Results:

- The EnergyWise feature implemented on the Legrand PDU is enabled.
- The UDP port is set to 10288.

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 on the Legrand PDU device. Change the baud rate before connecting it to the desired device, such as a computer, a Raritan's P2CIM-SER, 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 Legrand PDU or power cycle the connected device for proper communications.

▶ **Determine the CONSOLE baud rate:**

```
config:#   serial consoleBaudRate <baud_rate>
```

Variables:

- <baud_rate> is one of the baud rate options: *1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200.*

Example

The following command sets the CONSOLE baud rate of the Legrand PDU 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 IP, Subnet Mask and Gateway Parameters

The following multi-command syntax configures IPv4 address, subnet mask and gateway for the network connectivity simultaneously.

```
config:#   network ipv4 ipAddress 192.168.84.225 subnetMask 255.255.255.0
           gateway 192.168.84.0
```

Results:

- The IP address is set to 192.168.84.225.
- The subnet mask is set to 255.255.255.0.
- The gateway is set to 192.168.84.0.

Example 2 - Combination of Upper Critical and Upper Warning Settings

The following multi-command syntax simultaneously configures Upper Critical and Upper Warning thresholds for the RMS current of the 2nd overcurrent protector.

```
config:#    sensor ocp 2 current upperCritical disable upperWarning 15
```

Results:

- The Upper Critical threshold of the 2nd overcurrent protector's RMS current is disabled.
- The Upper Warning threshold of the 2nd overcurrent protector's RMS current is set to 15A and enabled at the same time.

Example 3 - 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.

Example 4 - Combination of Upper Critical, Upper Warning and Lower Warning Settings

The following multi-command syntax configures Upper Critical, Upper Warning and Lower Warning thresholds for the outlet 5 RMS current simultaneously.

```
config:#    sensor outlet 5 current upperCritical disable upperWarning enable
            lowerWarning 1.0
```

Results:

- The Upper Critical threshold of outlet 5 RMS current is disabled.
- The Upper Warning threshold of outlet 5 RMS current is enabled.
- The Lower Warning threshold of outlet 5 RMS current is set to 1.0A and enabled at the same time.

Load Shedding Configuration Commands

This section applies to outlet-switching capable models only.

A load shedding configuration command begins with *loadshedding*.

Unlike other CLI configuration commands, the load shedding configuration command is performed in the *administrator mode* rather than the configuration mode. See **Different CLI Modes and Prompts** (on page 271).

Enabling or Disabling Load Shedding

This section applies to outlet-switching capable models only.

This command determines whether to enter or exit from the load shedding mode.

```
#        loadshedding <option>
```

After performing the above command, Legrand PDU prompts you to confirm the operation. Press y to confirm or n to abort the operation.

To skip the confirmation step, you can add the "/y" parameter to the end of the command so that the operation is executed immediately.

```
#        loadshedding <option> /y
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
start	Enter the load shedding mode.
stop	Quit the load shedding mode.

Example

The following command has the Legrand PDU enter the load shedding mode.

```
config:#  loadshedding start
```

Power Control Operations

This section applies to outlet-switching capable models only.

Outlets on the Legrand PDU can be turned on or off or power cycled through the CLI.

Besides, you can cancel the power-on process while the Legrand PDU is powering on ALL outlets.

You must perform this operation in the *administrator mode*. See **Different CLI Modes and Prompts** .

![Legrand logo]

Turning On the Outlet(s)

This section applies to outlet-switching capable models only.

This command turns on one or multiple outlets.

```
#        power outlets <numbers> on
```

To quicken the operation, you can add the parameter "/y" to the end of the command, which confirms the operation.

```
#        power outlets <numbers> on /y
```

Variables:

- <numbers> is one of the options: *all*, an outlet number, a list or a range of outlets.

Option	Description
all	Switches ON all outlets.
A specific outlet number	Switches ON the specified outlet.
A comma-separated list of outlets	Switches ON multiple, inconsecutive or consecutive outlets. For example, to specify 7 outlets -- 2, 4, 9, 11, 12, 13 and 15, type `outlets 2,4,9,11-13,15`.
A range of outlets with an en dash in between	Switches ON multiple, consecutive outlets. For example, to specify 6 consecutive outlets -- 3, 4, 5, 6, 7, 8, type `outlets 3-8`.

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

Turning Off the Outlet(s)

This section applies to outlet-switching capable models only.

This command turns off one or multiple outlets.

```
#        power outlets <numbers> off
```

To quicken the operation, you can add the parameter "/y" to the end of the command, which confirms the operation.

```
#        power outlets <numbers> off /y
```

Variables:

- <numbers> is one of the options: *all*, an outlet number, a list or a range of outlets.

Option	Description
all	Switches OFF all outlets.
A specific outlet number	Switches OFF the specified outlet.
A comma-separated list of outlets	Switches OFF multiple, inconsecutive or consecutive outlets. For example, to specify 7 outlets -- 2, 4, 9, 11, 12, 13 and 15, type `outlets 2,4,9,11-13,15`.
A range of outlets with an en dash in between	Switches OFF multiple, consecutive outlets. For example, to specify 6 consecutive outlets -- 3, 4, 5, 6, 7, 8, type `outlets 3-8`.

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

Power Cycling the Outlet(s)

This section applies to outlet-switching capable models only.

This command power cycles one or multiple outlets.

```
#       power outlets <numbers> cycle
```

To quicken the operation, you can add the parameter "/y" to the end of the command, which confirms the operation.

```
#       power outlets <numbers> cycle /y
```

Variables:

- <numbers> is one of the options: *all*, an outlet number, a list or a range of outlets.

Option	Description
all	Power cycles all outlets.
A specific outlet number	Power cycles the specified outlet.
A comma-separated list of outlets	Power cycles multiple, inconsecutive or consecutive outlets. For example, to specify 7 outlets -- 2, 4, 9, 11, 12, 13 and 15, type `outlets 2,4,9,11-13,15`.
A range of outlets with an en dash in between	Power cycles multiple, consecutive outlets. For example, to specify 6 consecutive outlets -- 3, 4, 5, 6, 7, 8, type `outlets 3-8`.

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

Canceling the Power-On Process

This section applies to outlet-switching capable models only.

After issuing the command to power on ALL outlets, you can use the following command to stop the power-on process.

```
#       power cancelSequence
```

To quicken the operation, you can add the parameter "/y" to the end of the command, which confirms the operation.

```
#       power cancelSequence /y
```

Example - Power Cycling Specific Outlets

The following command power cycles these outlets: 2, 6, 7, 8, 10, 13, 14, 15 and 16.

```
#      power outlets 2,6-8,10,13-16 cycle
```

Actuator Control Operations

An actuator, which is connected to a dry contact signal channel of a DX sensor, can control a mechanism or system. You can switch on or off that mechanism or system through the actuator control command in the CLI.

Perform these commands in the administrator or user mode. See *Different CLI Modes and Prompts* (on page 271).

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 Legrand PDU web interface or using the show command in the CLI. It is an integer between 1 and 32.

If you entered the command without "/y", a message appears, prompting you to confirm the operation. Then:

- Type y to confirm the operation, OR
- Type n to abort the operation

Switching Off an Actuator

This command syntax turns off one actuator.

```
#      control actuator <n> off
```

To quicken the operation, you can add the parameter "/y" to the end of the command, which confirms the operation.

```
#      control actuator <n> off /y
```

Variables:

- <n> is an actuator's ID number.

  The ID number is available in the Legrand PDU web interface or using the show command in the CLI. It is an integer between 1 and 32.

If you entered the command without "/y", a message appears, prompting you to confirm the operation. Then:

- Type `y` to confirm the operation, OR
- Type `n` to abort the operation

Example - Turning On a Specific Actuator

The following command turns on the actuator whose ID number is 8.

```
#      control actuator 8 on
```

Unblocking a User

If any user is blocked from accessing the Legrand PDU, you can unblock them at the local console.

▶ **To unblock a user:**

1. Log in to the CLI interface using any terminal program via a local connection. See ***With HyperTerminal*** (on page 270).
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 Legrand PDU

You can reset the Legrand PDU to factory defaults or simply restart it using the CLI commands.

Restarting the PDU

This command restarts the Legrand PDU. It is not a factory default reset.

▶ **To restart the Legrand PDU:**

1. Ensure you have entered administrator mode and the # prompt is displayed.
2. Type either of the following commands to restart the Legrand PDU.

```
#      reset unit
```

     -- OR --

```
#      reset unit /y
```

3. If you entered the command without "/y" in Step 2, a message appears prompting you to confirm the operation. Type y to confirm the reset.
4. Wait until the Username prompt appears, indicating the reset is complete.

Note: If you are performing this command over a USB connection, re-connect the USB cable after the reset is completed, or the CLI communications are lost.

Resetting Active Energy Readings

You can reset either one active energy sensor or all active energy sensors at a time to restart the energy accumulation process.

Only users with the "Admin" role assigned can reset active energy readings.

▶ **To reset all active energy readings of the Legrand PDU:**

    #   reset activeEnergy pdu

            -- OR --

    #   reset activeEnergy pdu /y

▶ **To reset one inlet's active energy readings:**

    #   reset activeEnergy inlet <n>

            -- OR --

    #   reset activeEnergy inlet <n> /y

▶ **To reset one outlet's active energy readings:**

    #   reset activeEnergy outlet <outlet_n>

            -- OR --

    #   reset activeEnergy outlet <outlet_n> /y

If you entered the command without "/y", a message appears prompting you to confirm the operation. Type y to confirm the reset or n to abort it.

Variables:

- <n> is the inlet number.
- <outlet_n> is an outlet number.

Resetting to Factory Defaults

The following commands restore all settings of the Legrand PDU to factory defaults.

▶ **To reset Legrand PDU settings after login, use either command:**

    #   reset factorydefaults

            -- OR --

    #   reset factorydefaults /y

▶ **To reset Legrand PDU settings before login:**

    Username: factorydefaults

See ***Using the CLI Command*** for details.

Network Troubleshooting

The Legrand PDU 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 271).

Diagnostic Commands

The diagnostic command syntax varies from command to command.

Querying DNS Servers

This command syntax queries Internet domain name server (DNS) information of a network host.

```
diag>          nslookup <host>
```

Variables:

- <host> is the name or IP address of the host whose DNS information you want to query.

Showing Network Connections

This command syntax displays network connections and/or status of ports.

```
diag>          netstat <option>
```

Variables:

- <option> is one of the options: *ports* or *connections*.

Option	Description
ports	Shows TCP/UDP ports.
connections	Shows network connections.

Testing the Network Connectivity

This ping command sends the ICMP ECHO_REQUEST message to a network host for checking its network connectivity. If the output shows the host is responding properly, the network connectivity is good. If not, either the host is shut down or it is not being properly connected to the network.

```
diag>      ping <host>
```

Variables:

- <host> is the host name or IP address whose networking connectivity you want to check.

Options:

- You can include any or all of additional options listed below in the ping command.

Options	Description
count <number1>	Determines the number of messages to be sent. <number1> is an integer number between 1 and 100.
size <number2>	Determines the packet size. <number2> is an integer number in bytes between 1 and 65468.
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 Legrand PDU and a network host.

```
diag>      traceroute <host>
```

Variables:

- <host> is the name or IP address of the host you want to trace.

Example - Ping Command

The following command checks the network connectivity of the host 192.168.84.222 by sending the ICMP ECHO_REQUEST message to the host for 5 times.

```
diag>      ping 192.168.84.222 count 5
```

June 2018

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.

▶ **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 enforceHttpsForWebAccess`" command -- that is, `security enf`.
  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.

Using SCP Commands

You can perform a Secure Copy (SCP) command to update the Legrand PDU firmware, do bulk configuration, or back up and restore the configuration.

In This Chapter

Firmware Update via SCP

Same as any Legrand PDU firmware update, all user management operations are suspended and all login attempts fail during the SCP firmware update. For details, see *Updating the Legrand PDU Firmware* (on page 237).

> 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 Legrand PDU firmware's filename. If the firmware file is not in the current directory, you must include the path in the filename.
   - *<user name>* is the "admin" or any user profile with the Firmware Update permission.
   - *<device ip>* is the IP address of the Legrand PDU that you want to update.

2. When the system prompts you to enter the password for the specified user profile, type it and press Enter.
3. The system transmits the specified firmware file to the Legrand PDU, and shows the transmission speed and percentage.
4. When the transmission is complete, it shows the following message, indicating that the Legrand PDU 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 Legrand PDU.
b. Copy the configuration file to one or multiple destination Legrand PDU.

For detailed information on the bulk configuration requirements, see ***Bulk Configuration*** (on page 239).

► **To save the configuration via SCP:**

1. Type the following SCP command and press Enter.

   ```
   scp <user name>@<device ip>:/bulk_config.txt
   ```

   - *<user name>* is the "admin" or any user profile with the administrator privileges.
   - *<device ip>* is the IP address of the Legrand PDU whose configuration you want to save.

2. Type the user password when prompted.
3. The system saves the configuration from the Legrand PDU 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 the administrator privileges.
   - *<device ip>* is the IP address of the Legrand PDU 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 Legrand PDU, 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
  ```

- Copy operation:

  ```
  scp  bulk_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
  ```

- Copy operation:

  ```
  pscp bulk_config.txt <user name>@<device ip>:/bulk_restore
  ```

Backup and Restore via SCP

To back up ALL settings of a Legrand PDU, 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 the administrator privileges.
   - *<device ip>* is the IP address of the Legrand PDU whose settings you want to back up.

2. Type the user password when prompted.
3. The system saves the settings from the Legrand PDU to a file named "backup_settings.txt."

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 the administrator privileges.
   - *<device ip>* is the IP address of the Legrand PDU 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 Legrand PDU, 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 Legrand PDU 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 Legrand PDU 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 Legrand PDU is a standalone device.
- Renaming the diagnostic file is wanted.

```
scp @<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 Legrand PDU 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 the Administrator or "Unrestricted View Privileges" privileges.
- *<device ip>* is the IP address of the Legrand PDU whose diagnostic 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 diagnostic file.

2. Type the password when the system prompts you to type it.
3. The system downloads the diagnostic data from the Legrand PDU onto your computer.
   - If you do NOT specify a new filename in the command, such as Scenario 1 or 2, the downloaded file's default name is "diag-data.zip."
   - If you specify a new filename in the command, such as Scenario 3 or 4, the downloaded file is renamed accordingly.

▶ **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>
  ```

June 2018

Specifications

In This Chapter

Maximum Ambient Operating Temperature

Make sure the environment does NOT exceed the maximum ambient operating temperature (TMA) when operating your Legrand PDU. If necessary, contact Legrand Technical Support for this information of your model.

Specification	Measure
Max Ambient Temperature	45 degrees Celsius

Serial RS-232 "RJ-45" Port Pinouts

RJ-45 Pin/signal definition			
Pin No.	Signal	Direction	Description
1	N/A	—	No signal
2	N/A	—	No signal
3	TxD	Output	Transmit data
4	GND	—	Signal ground
5	N/A	—	No signal
6	RxD	Input	Receive data (data in)
7	N/A	—	No signal
8	N/A	—	No signal

Sensor RJ-45 Port Pinouts

RJ-45 Pin/signal definition			
Pin No.	Signal	Direction	Description
1	+12V	—	Power (fuse protected)
2	+12V	—	Power (fuse protected)

RJ-45 Pin/signal definition			
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.

Equipment Setup Worksheet

Legrand PDU Series Model   _____

Legrand PDU Series Serial Number   _____

OUTLET 1	OUTLET 2	OUTLET 3
MODEL	MODEL	**MODEL**
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE
OUTLET 4	OUTLET 5	OUTLET 6
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE

OUTLET 7	OUTLET 8	OUTLET 9
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE
OUTLET 10	OUTLET 11	OUTLET 12
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE
OUTLET 13	OUTLET 14	OUTLET 15
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE

OUTLET 16	OUTLET 17	OUTLET 18
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE
OUTLET 19	OUTLET 20	OUTLET 21
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE
OUTLET 22	OUTLET 23	OUTLET 24
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE

Types of adapters

_____

Types of cables

_____

Name of software program

_____

June 2018

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 Legrand PDU.

- Configuration changes
- Firmware upgrade
- Downloading diagnostic data

Tip: You can also accomplish the same tasks via the TFTP server in a DHCP network. See **Bulk Configuration or Firmware Upgrade via DHCP/TFTP** *(on page 411).*

In This Chapter

Device Configuration/Upgrade Procedure

You can use one USB drive to configure or upgrade multiple Legrand PDUs one by one as long it contains valid configuration files.

▶ **To use a USB drive to configure the Legrand PDU or upgrade firmware:**

1. Verify that both the USB drive and your Legrand PDU meet the requirements. See *System and USB Requirements* (on page 403).
2. Prepare required configuration files. See *Configuration Files* (on page 403).
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 Legrand PDU.
5. The initial message shown on the front panel display depends on the first task performed by the Legrand PDU.
   - If no firmware upgrade task will be performed, a happy smiley is displayed after around 30 seconds. The happy smiley looks like one of the following, depending on your Raritan product.

   - If the USB drive contains the firmware upgrade data, the Legrand PDU:
   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 410).
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 Legrand PDU device for performing the same task(s) once the happy smiley or the firmware upgrade message displays.

7. Wait for several seconds until the Legrand PDU 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.

▶ **Legrand PDU system requirements:**
* There is at least one USB-A port available on your Legrand device.
* Your Legrand PDU must run firmware version 3.4.11 or later.

    Note that the Legrand PDU 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 404).

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 404).

* **config.txt:**

    This file is used for configuring device settings. See ***config.txt*** (on page 406).

* **devices.csv:**

    This file is required only when there are device-specific settings to configure for multiple Legrand PDUs. See ***devices.csv*** (on page 408).

Legrand provides a Mass Deployment Utility, which helps you to quickly generate all configuration files for your Legrand PDU. See ***Creating Configuration Files via Mass Deployment Utility*** (on page 408).

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 Legrand PDU to the latest firmware version.

▶ **user**

- A required option.
- Specify the name of a user account with Administrator Privileges.
- For Legrand PDU with factory default configuration, set this option to `admin`.

▶ **password**

- A required option.
- Specify the password of the specified admin user.
- For Legrand PDU with factory default configuration, set this option to `raritan`.

▶ **logfile**

- Specify the name of a text file where the Legrand PDU will append the log messages when interpreting the USB drive contents.
- If the specified file does not exist in the USB drive, it will be automatically created.
- If this option is not set, no log message are recorded. The disadvantage is that no feedback is available if the Legrand PDU detects a problem with the USB drive contents.

▶ **firmware**

- Specify the name of a firmware binary file used to upgrade your Legrand PDU.
- The specified firmware file must be compatible with your Legrand PDU and have an official Raritan signature.
- If the specified firmware file is the same as the current firmware version of your Legrand PDU, no firmware upgrade is performed.

▶ **config**

- Specify the name of the configuration file containing device settings.
- The suggested filename is *config.txt*. See ***config.txt*** (on page 406).

▶ **device_list**

- Specify the name of the configuration file listing all Legrand PDUs 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 408).

▶ **match**

- Specify a match condition for identifying a line or one Legrand PDU 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 Legrand PDU to search for the MAC address in the 7th column of the "devices.csv" file.

- The default value is `serial:1`, making the Legrand PDU 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 Legrand PDU 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 Legrand PDU.

  Note: See **Bulk Configuration** *(on page 239) 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 Legrand PDU.

  Note: See **Backup and Restore of Device Settings** *(on page 243) 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 Legrand PDU is transmitted to the USB drive.

- The filename of the diagnostic data written into the USB drive is:

  diag_<unit-serial>.zip

▶ **switch_outlets**

- This feature works on outlet-switching capable models only.

- Switch on or off specific outlets.

- The option's value comprises outlet numbers and the setting "on" or "off" as explained below:
  - Each "on" or "off" setting consists of three parts: outlet numbers, a colon, and the word "on" or "off".
  - Each "on" or "off" setting is separated with a semicolon.
  - If all outlets will share the same "on" or "off" setting, replace the outlet numbers with the word "all".

- Examples:
  - Turn on outlets 1 to 3, and 10, and turn off outlets 4 to 9.

```
switch_outlets=1,2,3:on;4-9:off;10:on
```
- ▪ Turn on all outlets.
```
switch_outlets=all:on
```

▶ **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 Legrand PDU.
- 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 Legrand PDU.
- 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.

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 404).

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 Legrand PDU model.

You can use Legrand's Mass Deployment Utility to create this file by yourself, or contact Legrand to get a device configuration file specific to your Legrand PDU 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 409).*

▶ **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.

▶ **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 PDU2. See ***devices.csv*** (on page 408)
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
```

June 2018

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 Legrand PDU device.

This file must be:

- A CSV (comma-separated values) format file exported from a spreadsheet application like Excel.
- Copied to the root directory.
- Referenced in the *device_list* option of the "fwupdate.cfg" file. See ***fwupdate.cfg*** (on page 404).

Every Legrand PDU identifies its entry in the "devicelist.csv" file by comparing its serial number or MAC address to one of the columns in the file.

▶ **Determine the column to identify Legrand PDUs:**

- By default, the Legrand PDU searches for its serial number in the 1st column.
- To override the default, set the *match* option in the "fwupdate.cfg" file to a different column.

▶ **Syntax:**

- 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",Value-3


Value-1,"Value-2
with a line break", Value-3
```

Creating Configuration Files via Mass Deployment Utility

The Mass Deployment Utility is an Excel file that lets you fill in basic information required for the three configuration files, such as the admin account and password.

After entering required information, you can generate all configuration files with only one click, including *fwupdate.cfg*, *config.txt* and *devices.csv*.

▶ **To use the Mass Deployment Utility:**

1. Download the Mass Deployment Utility from the Legrand PDU section of the Raritan website.
   - The utility is named *mass_deployment-xxx* (where xxx is the firmware version number).
   - It is available on the Legrand PDU 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.

Target Directory:

C:\temp   Browse...

Export Lists
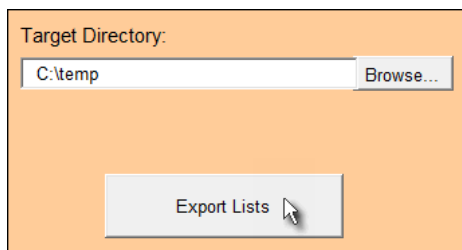
6. Verify that at least 3 configuration files are created - *fwupdate.cfg*, *config.txt* and *devices.csv*. You are ready to configure or upgrade any Legrand PDU with these files. See **Configuration or Firmware Upgrade with a USB Drive** (on page 402).

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 Legrand PDU running firmware version 3.4.11 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 408).
2. Launch a terminal to log in to the CLI of any Legrand PDU running version 3.4.11 or later. See **Logging in to CLI** (on page 269).
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 Legrand PDU running version 3.4.11 or later. See **Configuration or Firmware Upgrade with a USB Drive** (on page 402).

▶ **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 the Legrand PDU section of 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 Legrand PDU, 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 404).

▶ **To use a USB drive to upgrade the Legrand PDU:**

1. Copy the configuration file "fwupdate.cfg" and an appropriate firmware file to the root directory of the USB drive.
2. Reference the firmware file in the *image* option of the "fwupdate.cfg" file.
3. Plug the USB drive into the USB-A port on the Legrand PDU.
4. The Legrand PDU 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 Legrand PDU 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 Legrand Technical Support to look into the failure cause.

   ☹

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 Legrand PDUs 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 Legrand PDUs to configure or upgrade.

> Warning: The feature of bulk configuration or firmware upgrade via DHCP/TFTP only works on standalone Legrand PDUs directly connected to the network. This feature does NOT work for slave devices in the cascading configuration.

Tip: For the other alternative, see **Configuration or Firmware Upgrade with a USB Drive** *(on page 402).*

In This Chapter

Bulk Configuration/Upgrade Procedure

▶ **Steps of using DHCP/TFTP for bulk configuration/upgrade:**

1. Create configuration files specific to your Legrand PDU models and firmware versions. See **Configuration Files** (on page 403) or contact Legrand 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 Legrand Technical Support for the correctness of these files prior to using this feature.

2. Configure your TFTP server properly. See **TFTP Requirements** (on page 412).

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 Legrand PDU.

L1 legrand®

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 412)
- **DHCP IPv6 Configuration in Windows** (on page 420)
- **DHCP IPv4 Configuration in Linux** (on page 426)
- **DHCP IPv6 Configuration in Linux** (on page 427)

5. Make sure all of the desired Legrand PDUs use DHCP as the IP configuration method and have been *directly* connected to the network.

6. Re-boot these Legrand PDUs. The DHCP server will execute the commands in the "fwupdate.cfg" file on the TFTP server to configure or upgrade those Legrand PDUs 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 411).

If you are going to upload any Legrand PDU 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 Legrand PDUs 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 Legrand PDU under IPv4.
   a. Right-click the IPv4 node in DHCP to select Define Vendor Classes.

b. Click Add to add a new vendor class.
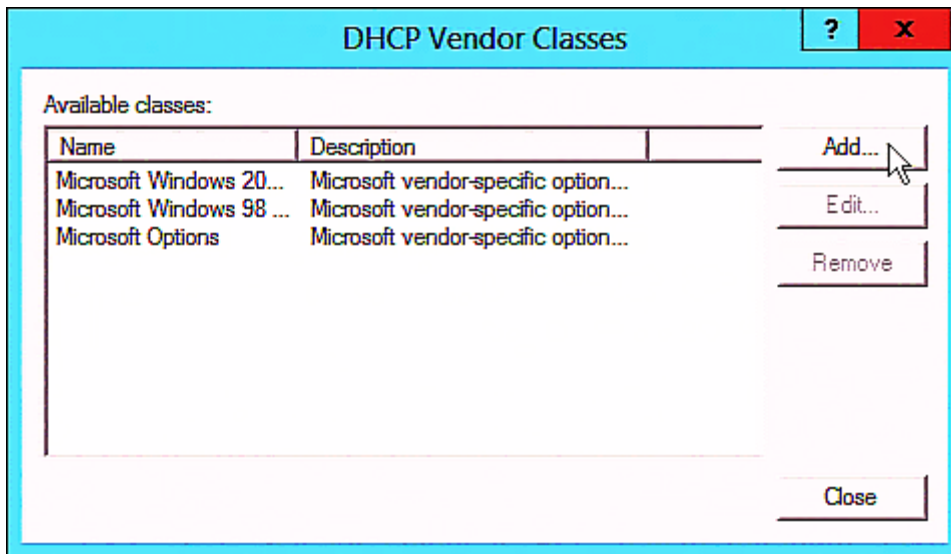
c. Specify a unique name for this vendor class and type the binary codes of "Raritan PDU 1.0" in the New Class dialog.

The vendor class is named "Raritan PDU" in this illustration.
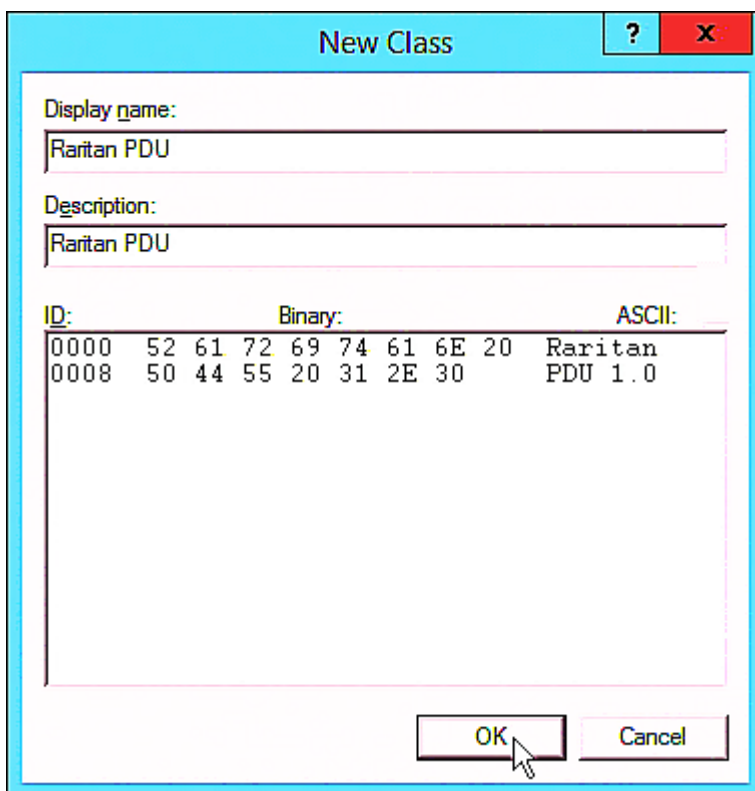
2. Define one DHCP standard option - Vendor Class Identifier.

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.
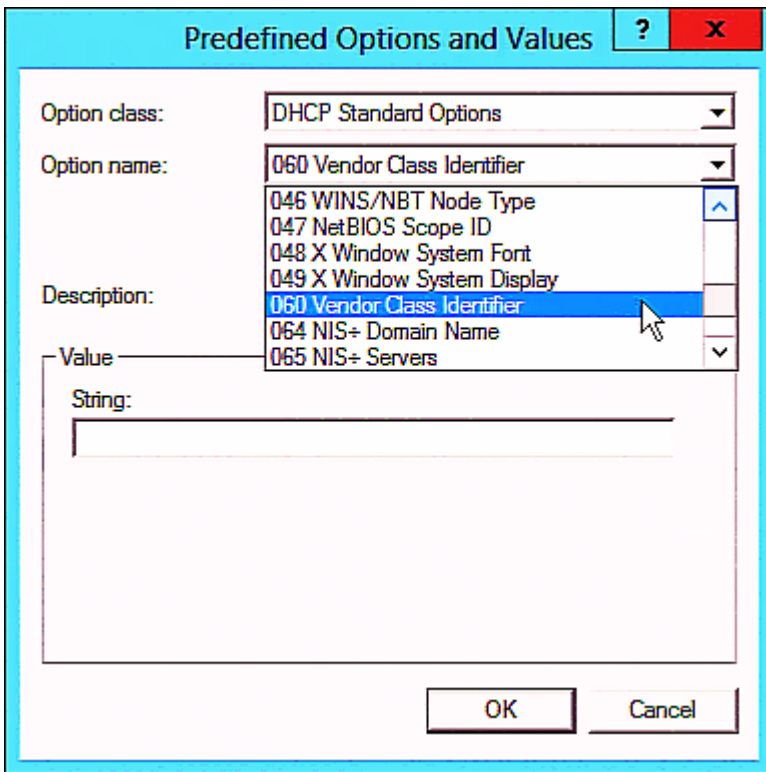
3. Add three options to the new vendor class "Raritan PDU" in the same dialog.

   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.

![Legrand logo]

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.

![Legrand logo]
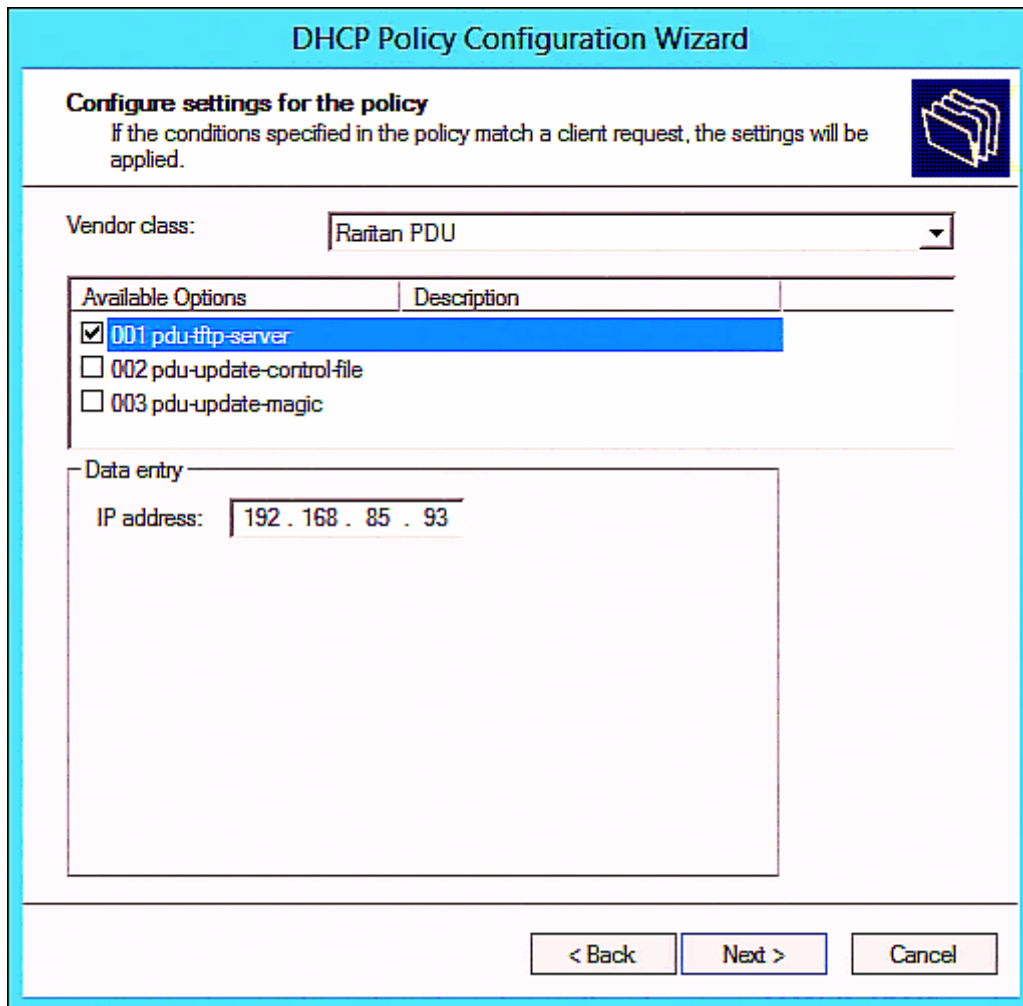
g. Select the "Raritan PDU" in the "Vendor class" field, select "001 pdu-tftp-server" from the Available
    Options list, and type your TFTP server's IPv4 address in the "IP address" field.
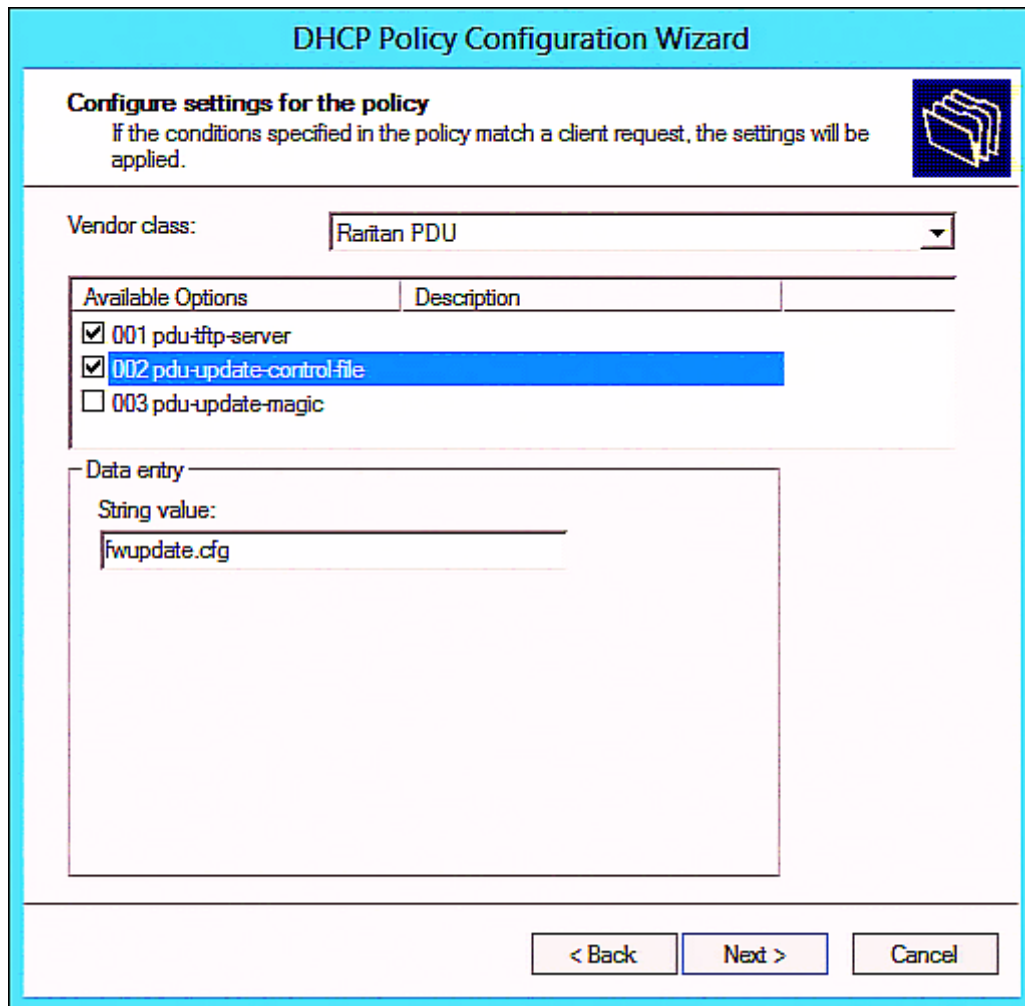
h. Select "002 pdu-update-control-file" from the Available Options list, and type the filename "fwupdate.cfg" in the "String value" field.

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.

June 2018

Important: The magic cookie is transmitted to and stored in Legrand PDU 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 Legrand PDU. 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 Legrand PDUs 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 Legrand PDU under IPv6.
    a. Right-click the IPv6 node in DHCP to select Define Vendor Classes.

b. Click Add to add a new vendor class.
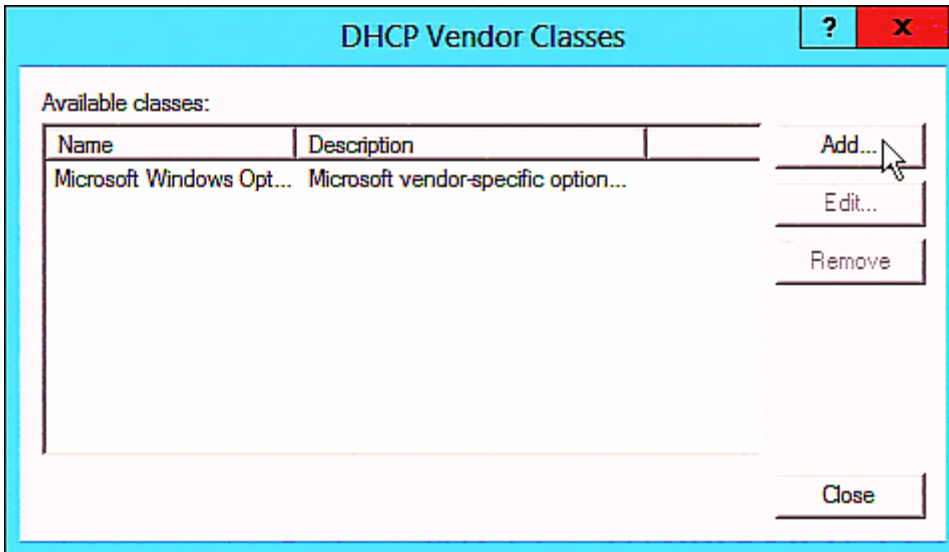
c. Specify a unique name for the vendor class, type "13742" in the "Vendor ID (IANA)" field, and type the binary codes of "Raritan PDU 1.0" in the New Class dialog.

The vendor class is named "Raritan PDU 1.0" in this illustration.
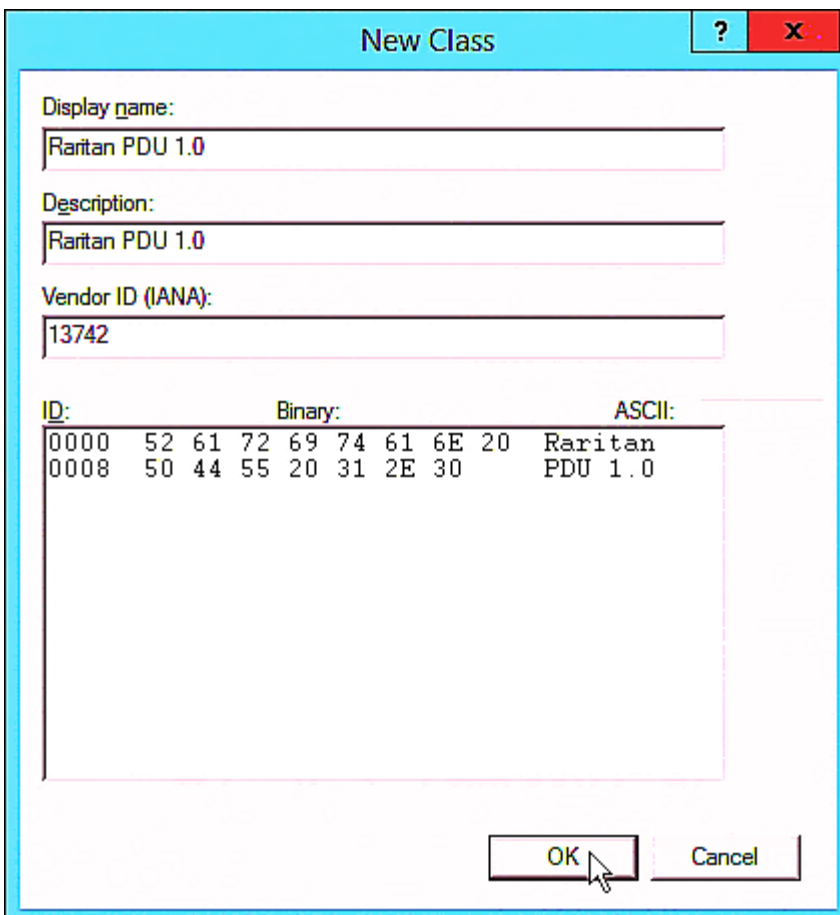
2. Add three options to the "Raritan PDU 1.0" vendor class.

a. Right-click the IPv6 node in DHCP to select Set Predefined Options.

b. Select Raritan PDU 1.0 in the "Option class" field.

c. Click Add to add the first option. Type "pdu-tftp-server" in the Name field, select IP Address as the data type, and type 1 in the Code field.

d. Click Add to add the second option. Type "pdu-update-control-file" in the Name field, select String as the data type, and type 2 in the Code field.

e. Click Add to add the third one. Type "pdu-update-magic" in the Name field, select String as the data type, and type 3 in the Code field.

3. Configure server options associated with the "Raritan PDU 1.0" vendor class.

    a. Right-click the Server Options node under IPv6 to select Configure Options.

    b. Click the Advanced tab.

c. Select "Raritan PDU 1.0" in the "Vendor class" field, select "00001 pdu-tftp-server" from the Available Options list, and type your TFTP server's IPv6 address in the "IPv6 address" field.
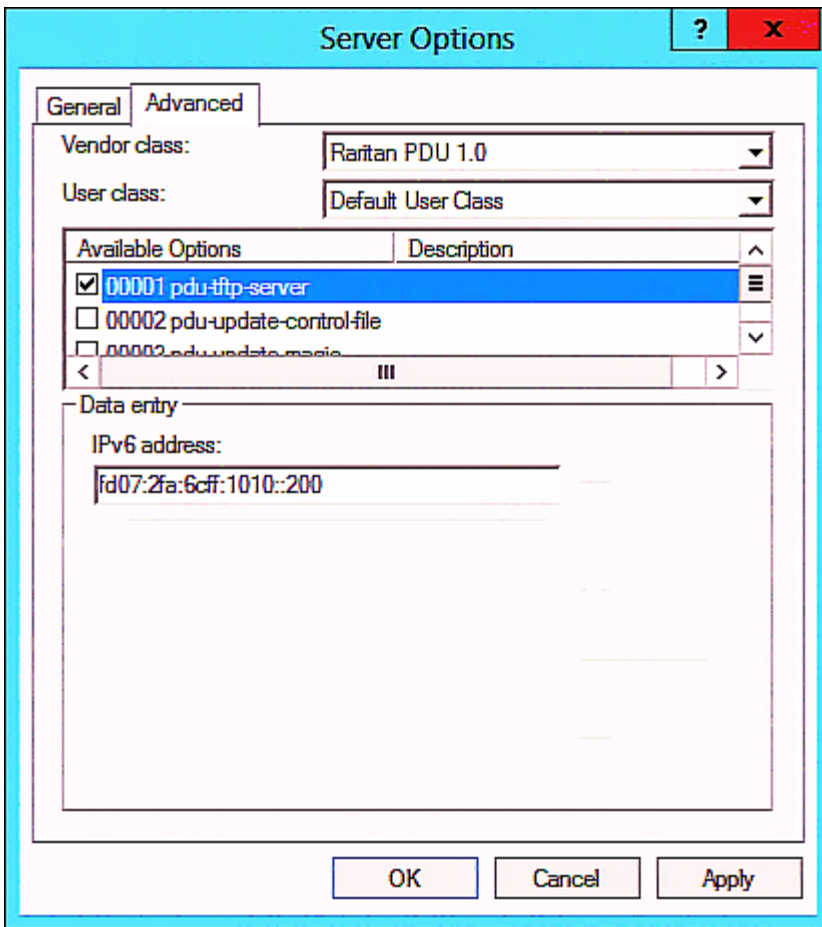
d. Select "00002 pdu-update-control-file" from the Available Options list, and type the filename "fwupdate.cfg" in the "String value" field.
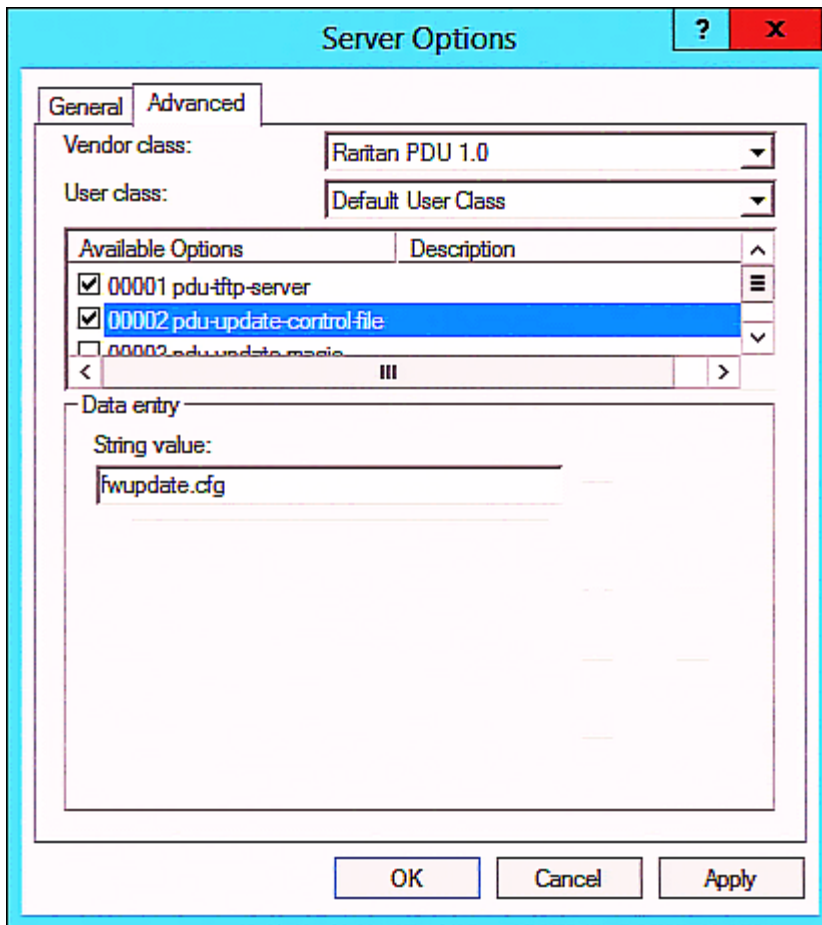
e. Select "00003 pdu-update-magic" from the Available Options list, and type any string in the "String value" field. This third option/code is the magic cookie to prevent the *fwupdate.cfg* commands from being executed repeatedly. It does NOT matter whether the IPv6 magic cookie is identical to or different from the IPv4 magic cookie.

The magic cookie is a string comprising numerical and/or alphabetical digits in any format. In the following illustration diagram, it is a combination of a date and a serial number.

June 2018

Important: The magic cookie is transmitted to and stored in Legrand PDU 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 Legrand PDU. 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 Legrand PDU 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 Legrand PDU 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 Legrand PDU 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 Legrand PDU. 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 Legrand PDU 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 Legrand PDU 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 Legrand PDU. 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";
[...]


}
```

Resetting to Factory Defaults

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

Important: Exercise caution before resetting the Legrand PDU to its factory defaults. This erases existing information and customized settings, such as user profiles, threshold values, and so on. Only active energy data and firmware upgrade history are 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 246).

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 Legrand PDU. See **Connecting the Legrand PDU to a Computer** (on page 30).
2. Launch a terminal emulation program such as Kermit or PuTTY, and open a window on the Legrand PDU. For information on the serial port configuration, see Step 2 of **Initial Network Configuration via CLI** (on page 486).

   Note: PuTTY is a free program you can download from the Internet. See PuTTY's documentation for details on configuration.

3. Press (and release) the Reset button of the Legrand PDU 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 Legrand PDU to its factory defaults.
5. Wait until the Username prompt appears, indicating the reset is complete.

   This diagram illustrates the reset button on Zero U models so it may look slightly different from your model's front panel.
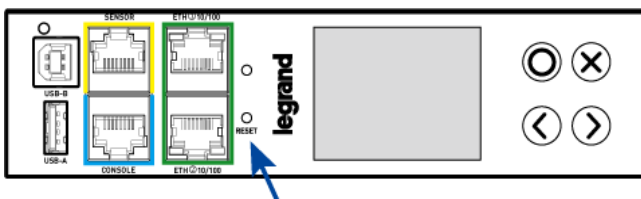
Using the CLI Command

The Command Line Interface (CLI) provides a reset command for restoring the Legrand PDU to factory defaults. For information on CLI, see **Using the Command Line Interface** (on page 269).

▶ **To reset to factory defaults after logging in to the CLI:**

1. Connect to the Legrand PDU. See **Logging in to CLI** (on page 269) or **Connecting the Legrand PDU to a Computer** (on page 30).

2. Launch a terminal emulation program such as HyperTerminal, Kermit, or PuTTY, and open a window on the Legrand PDU. For information on the serial port configuration, see Step 2 of ***Initial Network Configuration via CLI*** (on page 486).

3. Log in to the CLI by typing the user name "admin" and its password.

4. After the # system prompt appears, type either of the following commands and press Enter.

       `#      reset factorydefaults`

         -- OR --

       `#      reset factorydefaults /y`

5. If you entered the command without "`/y`" in Step 4, a message appears prompting you to confirm the operation. Type y to confirm the reset.

6. Wait until the Username prompt appears, indicating the reset is complete.

▶ **To reset to factory defaults without logging in to the CLI:**

The Legrand PDU provides an easier way to reset the product to factory defaults in the CLI prior to login.

1. Connect to the Legrand PDU 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.

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 Legrand PDU
b. Create user groups for the Legrand PDU on the AD server
c. Configure LDAP authentication on the Legrand PDU
d. Configure roles on the Legrand PDU

Important: Legrand 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 Legrand PDU. 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)
PX_User	usera
	pxuser2
PX_Admin	userb
	pxuser

Group permissions:

*   The PX_User role will have neither system permissions nor outlet permissions.
*   The PX_Admin role will have full system and outlet permissions.

Step B. Configure User Groups on the AD Server

You must create the groups (roles) for the Legrand PDU on the AD server, and then make appropriate users members of these groups.

In this illustration, we assume:

*   The groups (roles) for the Legrand PDU are named *PX_Admin* and *PX_User*.
*   User accounts *pxuser*, *pxuser2*, *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 -- *PX_Admin* and *PX_User*.

Note: Refer to the documentation or online help accompanying Microsoft AD for detailed instructions.

---

2. Add the *pxuser2* and *usera* accounts to the PX_User group.
3. Add the *pxuser* and *userb* accounts to the PX_Admin group.
4. Verify whether each group comprises correct users.

PX_Admin Properties ?|X|

General | Members | Member Of | Managed By |

Members:

Name	Active Directory Folder
pxuser	techadssl.com/Users
userb	techadssl.com/ServicesApps/raritan

PX_User Properties ?|X|

General | Members | Member Of | Managed By |

Members:

Name	Active Directory Folder
pxuser2	techadssl.com/Users
usera	techadssl.com/ServicesApps/raritan

Step C. Configure LDAP Authentication on the Legrand PDU

You must enable and set up LDAP authentication properly on the Legrand PDU to use external authentication.

In the illustration, we assume:

- The DNS server settings have been configured properly. See **Wired Network Settings** (on page 141) and **Role of a DNS Server** (on page 482).
- 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 Legrand PDU 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."

Field/setting	Do this...
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.
Login Name Attribute	Ensure the field is set to `sAMAccountName` because the LDAP server is Microsoft Active Directory.
User Entry Object Class	Ensure the field is set to `user` because the LDAP server is Microsoft Active Directory.
User Search Subfilter	The field is optional. The subfilter information is also useful for filtering out additional objects in a large directory structure. In this example, we leave it blank.
Active Directory Domain	Type `techadssl.com`.

4. Click Add Server.The LDAP server is saved.
5. In the Authentication Type field, select LDAP.
6. Click Save. The LDAP authentication is activated.

Note: If the Legrand PDU 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 Legrand PDU and the LDAP server to use the same NTP server(s).

Step D. Configure Roles on the Legrand PDU

A role on the Legrand PDU determines the system and outlet permissions. You must create the roles whose names are identical to the user groups created for the Legrand PDU on the AD server or authorization will fail. Therefore, we will create the roles named *PX_User* and *PX_Admin* on the PDU.

In this illustration, we assume:

- Users assigned to the *PX_User* role can view settings only, but they can neither configure Legrand PDU nor access the outlets.
- Users assigned to the *PX_Admin* role have the Administrator Privileges so they can both configure Legrand PDU and access the outlets.

▶ **To create the PX_User role with appropriate permissions assigned:**

1. Choose User Management > Roles.
2. Click 👤➕ to add a new role.
   a. Type `PX_User` in the Role Name field.
   b. Type a description for the PX_User role in the Description field. In this example, we type "View PX settings" to describe the role.

c. In the Privileges list, select Unrestricted View Privileges, which includes all View permissions. The Unrestricted View Privileges permission lets users view all settings without the capability to configure or change them.

✔	Unrestricted View Privileges
☐	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 PX_User role is created.

Role Name ▲	Description	
Admin	System defined administrator role including all privileges.	🔒
Operator	Predefined operator role.	
PX_User	View PX settings	

4. Keep the Roles page open to create the PX_Admin role.

▶ **To create the PX_Admin role with full permissions assigned:**

1. Click 👤➕ to add another role.

   a. Type `PX_Admin` in the Role Name field.

   b. Type a description for the PX_Admin role in the Description field. In this example, we type "Includes all PX privileges" to describe the role.

June 2018

c. In the Privileges list, select Administrator Privileges. The Administrator Privileges allows users to configure or change all Legrand PDU settings.

Privileges	^
Select privilege to add to role. Be aware some privileges may require additional arguments.	
☐ Acknowledge Alarms	
☑ Administrator Privileges	
☐ Change Asset Strip Configuration	
☐ Change Authentication Settings	

d. Click Save.

2. The PX_Admin role is created.

Role Name ▲	Description	
Admin	System defined administrator role including all privileges.	🔒
Operator	Predefined operator role.	
PX_Admin	Includes all PX privileges	
PX_User	View PX settings	

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 Legrand PDU 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.
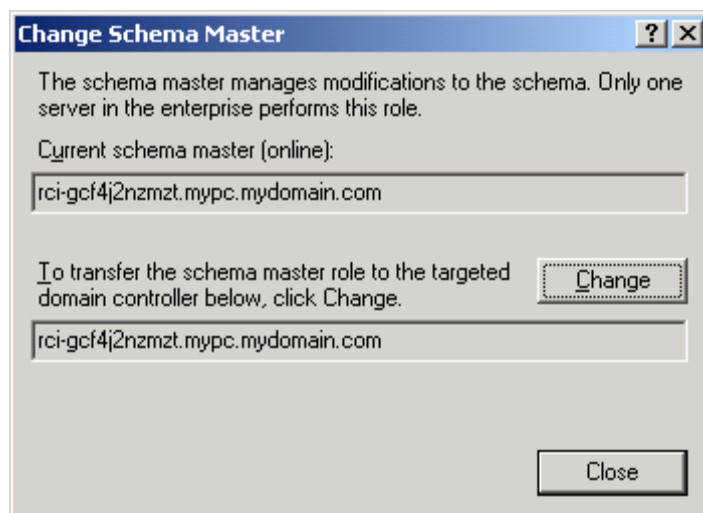
2. Select the "Schema can be modified on this Domain Controller" checkbox. **Optional**
3. Click OK.

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.
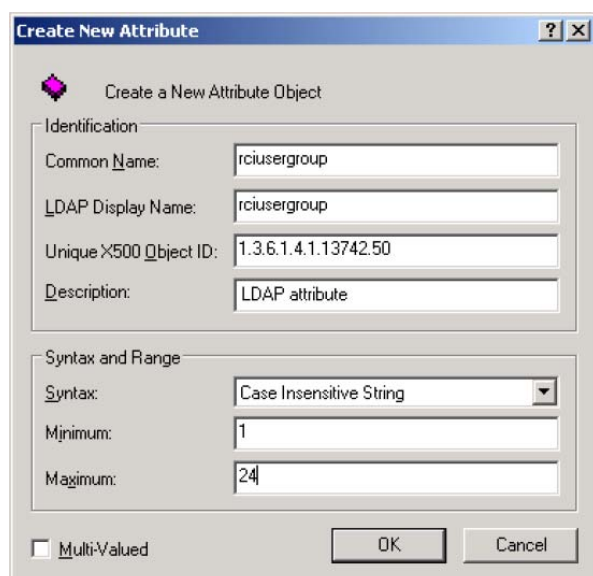
4. Type *rciusergroup* in the Common Name field.

June 2018

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.
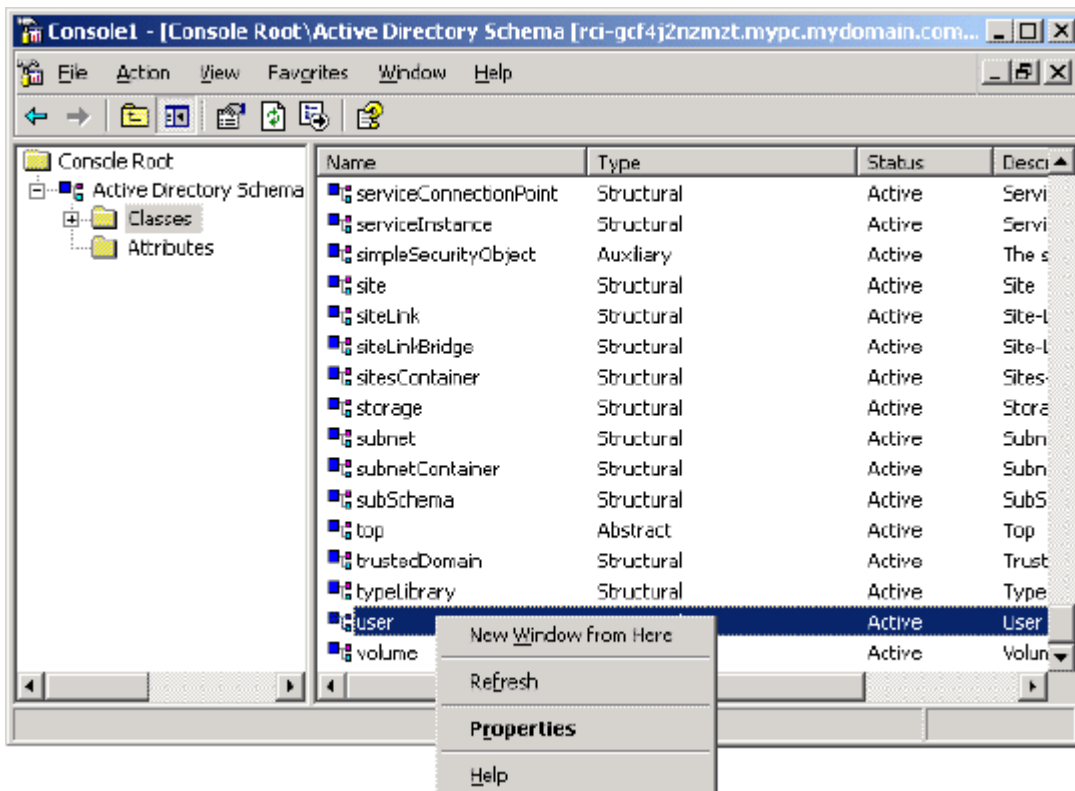
3. Choose Properties from the menu. The user Properties dialog appears.
4. Click the Attributes tab to open it.
5. Click Add.

6. Choose rciusergroup from the Select Schema Object list.
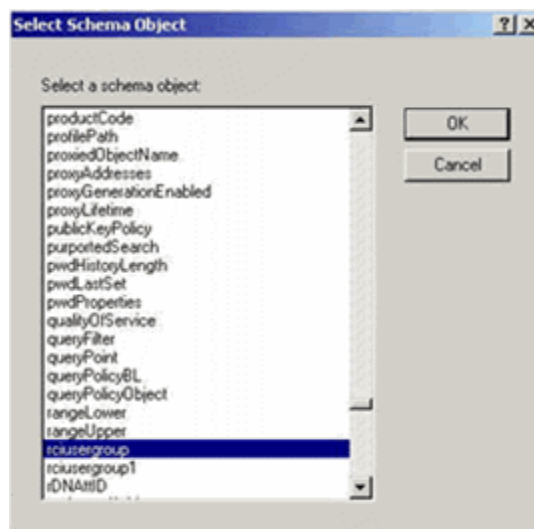
7. Click OK in the Select Schema Object dialog.
8. Click OK in the User Properties dialog.

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.

June 2018

3. Go to the directory where the support tools were installed. Run adsiedit.msc. The ADSI Edit window opens.
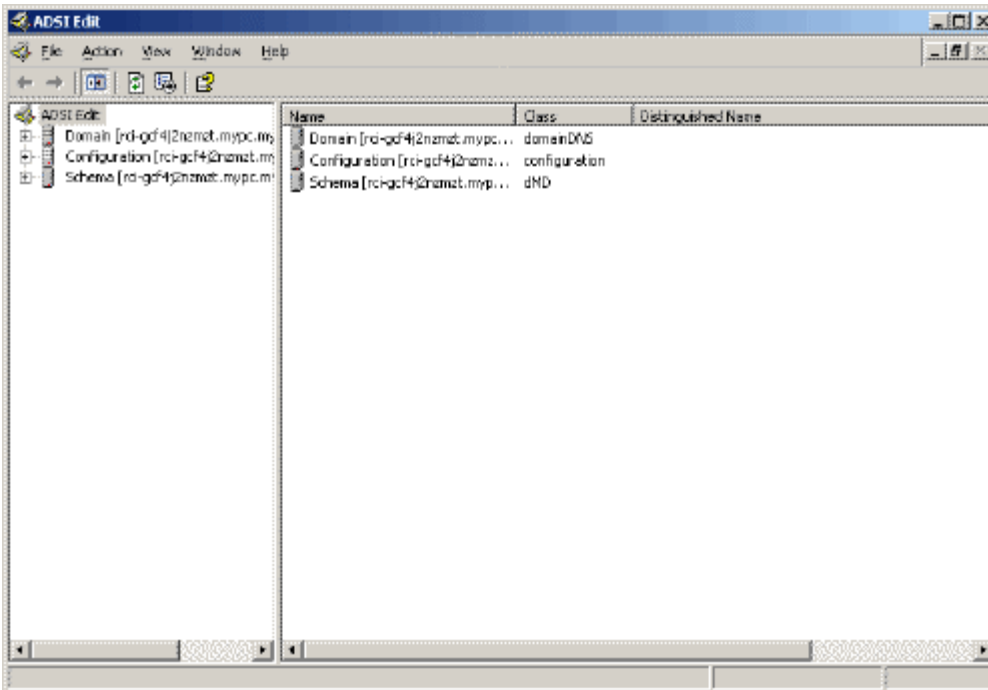
4. Open the Domain.

5. In the left pane of the window, select the CN=Users folder.
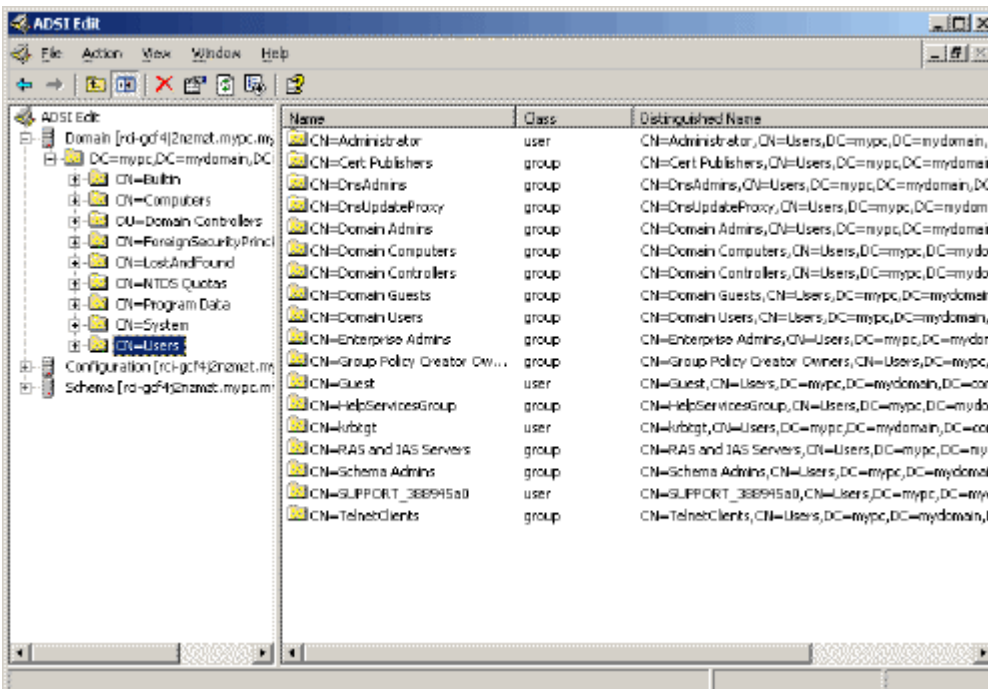
6. Locate the user name whose properties you want to adjust in the right pane. Right-click the user name and select Properties.

7. Click the Attribute Editor tab if it is not already open. Choose rciusergroup from the Attributes list.
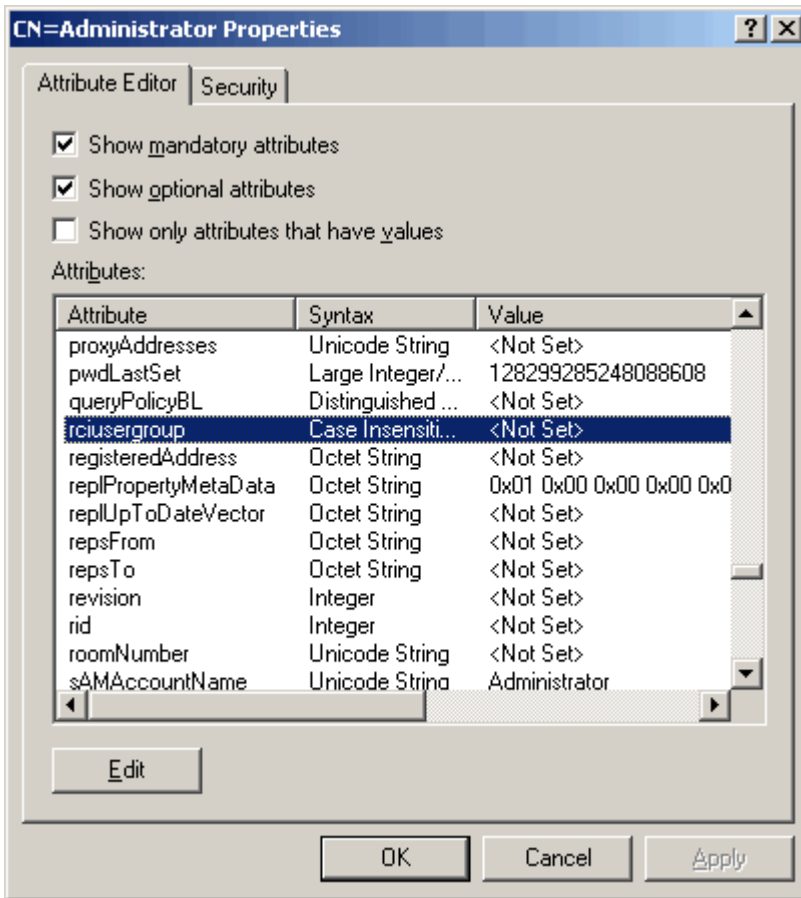
8. Click Edit. The String Attribute Editor dialog appears.
9. Type the user role (created in the Legrand PDU) in the Edit Attribute field. Click OK.
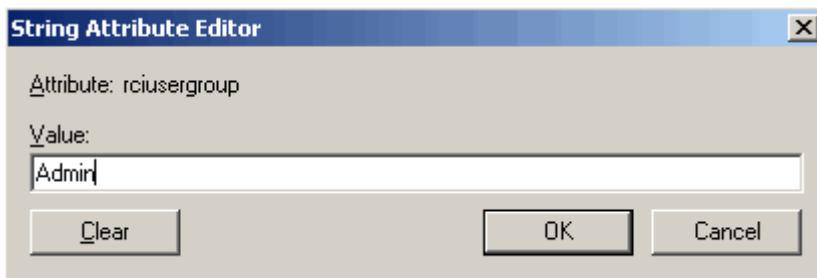
RADIUS Configuration Illustration

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 Legrand PDU. See **Adding Radius Servers** (on page 177).
2. Configure roles on the Legrand PDU. See **Creating Roles** (on page 135).
3. Configure Legrand PDU user credentials and roles on your RADIUS server.
    - To configure using standard attributes, see **Standard Attributes** (on page 442).
    - To configure using vendor-specific attributes, see **Vendor-Specific Attributes** (on page 455).

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 442).

For configuration on FreeRADIUS, see **FreeRADIUS Standard Attribute Illustration** (on page 455).

NPS Standard Attribute Illustration

To configure Windows 2008 NPS with the *standard attribute*, you must:

a. Add your Legrand PDU to NPS. See **Step A: Add Your Legrand PDU as a RADIUS Client** (on page 443).
b. On the NPS, configure Connection Request Policies and the standard attribute. See **Step B: Configure Connection Policies and Standard Attributes** (on page 446).

Some configuration associated with Microsoft Active Directory (AD) is also required for RADIUS authentication. See **AD-Related Configuration** (on page 466).

Step A: Add Your Legrand PDU as a RADIUS Client

The RADIUS implementation on a Legrand PDU 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 Legrand PDU = `192.168.56.29`
- RADIUS authentication port specified for Legrand PDU: *1812*
- RADIUS accounting port specified for Legrand PDU: *1813*

► **To add your Legrand PDU 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.

June 2018

Verify the authentication and accounting port numbers shown in the properties dialog are the same as those specified on your Legrand PDU. In this example, they are 1812 and 1813. Then close this dialog.

Network Policy Server (Local) Properties

General | Ports

Enter the RADIUS authentication and accounting port numbers.

Authentication:

1812,1645

Authentication default ports 1812,1645

Accounting:

1813,1646

Accounting default ports 1813,1646

3. Under "RADIUS Clients and Servers," right-click RADIUS Client and select New RADIUS Client. The New RADIUS Client dialog appears.

Network Policy Server

File   Action   View   Help

NPS (Local)
  RADIUS Clients and Servers
      RADIUS C...   New RADIUS Client
      Remote R...   Export List
  Policies
  Network Acce...   View   ▶
  Accounting
                          Refresh

                          Help

4. Do the following to add your Legrand PDU to NPS:
   a. Verify the "Enable this RADIUS client" checkbox is selected.
   b. Type a name for identifying your Legrand PDU 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 Legrand PDU.

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 Legrand PDU
- Connection request forwarding method
- Authentication method(s)
- Standard RADIUS attributes

▶ **Presumptions in the illustration:**

- IP address of your Legrand PDU = `192.168.56.29`
- *Local* NPS server is used
- RADIUS protocol selected on your Legrand PDU = `CHAP`
- Existing role of your Legrand PDU = `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 Legrand PDU 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 Legrand PDU uses "CHAP" in this example

Note: If your Legrand PDU 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.
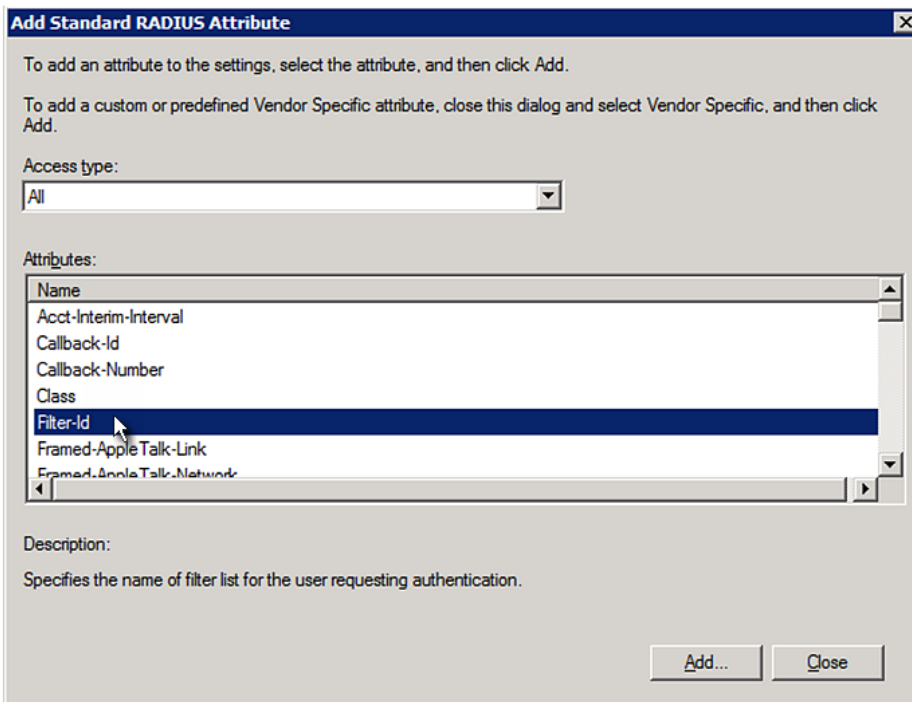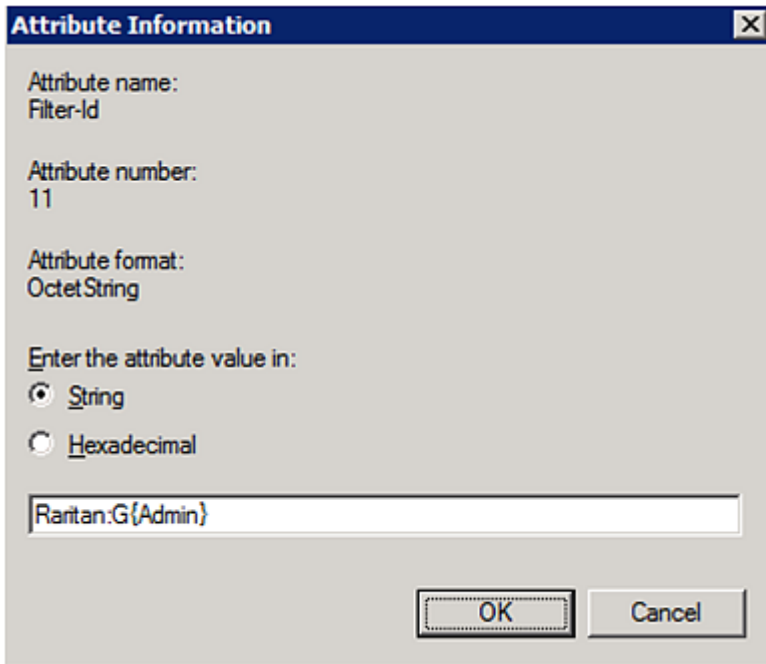
12. In the Attribute Information dialog, click Add.
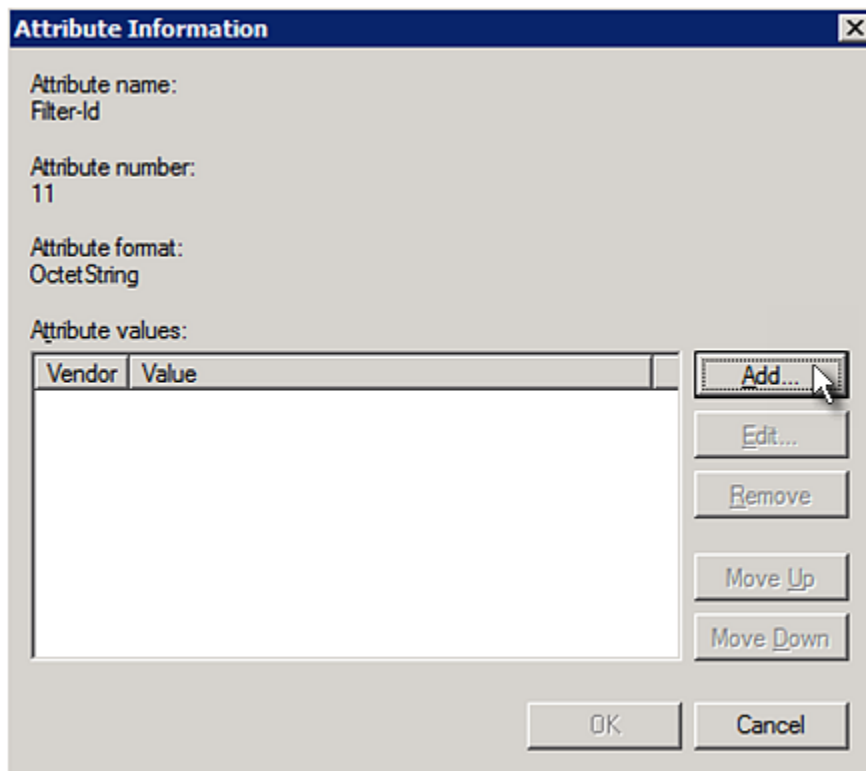
13. Select String, type *Raritan:G{Admin}* in the text box, and then click OK.

Admin inside the curved brackets {} is the existing role on the Legrand PDU. It is recommended to use the Admin role to test this configuration. The role name is case sensitive.
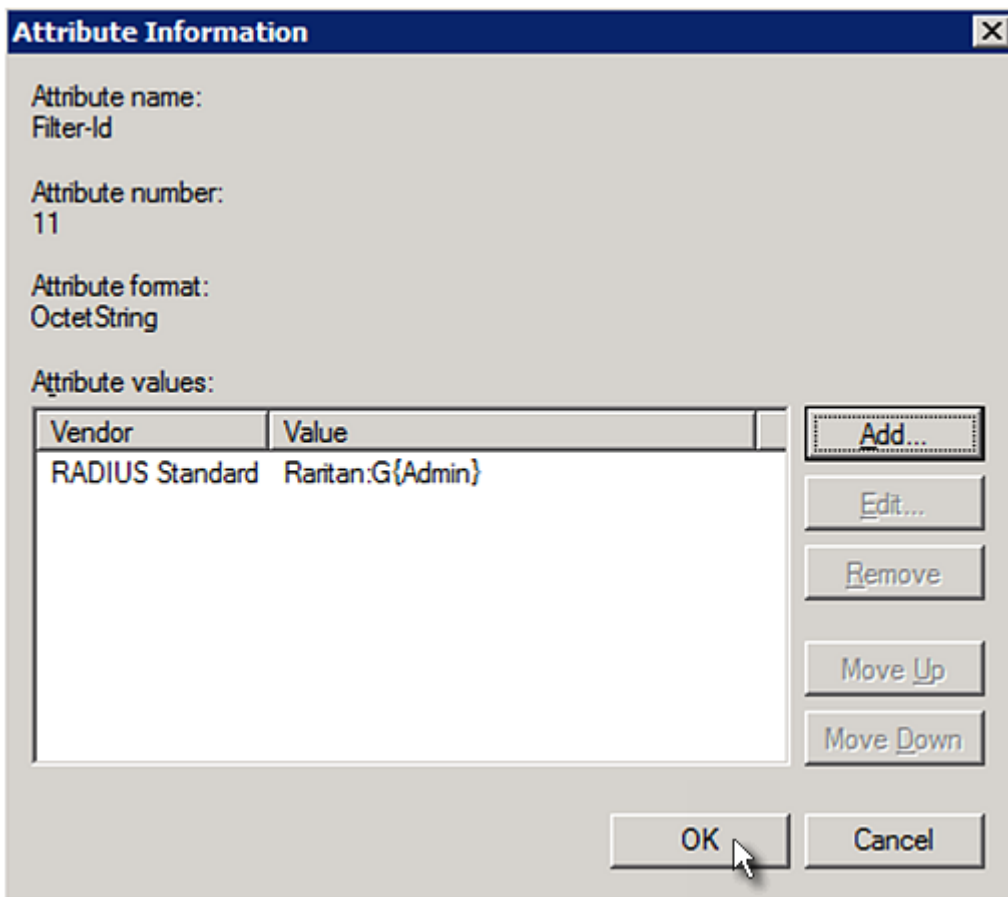
14. The new attribute is added. Click OK.

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 455).

For configuration on FreeRADIUS, see *FreeRADIUS VSA Illustration* (on page 465).

NPS VSA Illustration

To configure Windows 2008 NPS with the *vendor-specific attribute*, you must:

a. Add your Legrand PDU to NPS. See *Step A: Add Your Legrand PDU as a RADIUS Client* (on page 443).
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 459).

Some configuration associated with Microsoft Active Directory (AD) is also required for RADIUS authentication. See *AD-Related Configuration* (on page 466).

Step A: Add Your Legrand PDU as a RADIUS Client

The RADIUS implementation on a Legrand PDU 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 Legrand PDU = `192.168.56.29`
* RADIUS authentication port specified for Legrand PDU: *1812*
* RADIUS accounting port specified for Legrand PDU: *1813*

▶ **To add your Legrand PDU 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 Legrand PDU. 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 Legrand PDU to NPS:
    a. Verify the "Enable this RADIUS client" checkbox is selected.
    b. Type a name for identifying your Legrand PDU 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 Legrand PDU.

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 Legrand PDU
- Connection request forwarding method
- Authentication method(s)
- Standard RADIUS attributes

▶ **Presumptions in the illustration:**

- IP address of your Legrand PDU = `192.168.56.29`
- *Local* NPS server is used
- RADIUS protocol selected on your Legrand PDU = `CHAP`
- Existing roles of your Legrand PDU = `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 Legrand PDU IP address -- *192.168.56.29*, and click OK.

NAS IPv4 Address   ☒

Specify the IPv4 address of the network access server sending the access request message. You can use pattern matching syntax.

| 192.168.56.29 |

                                    [OK]   [Cancel]

7. Click Next in the New Connection Request Policy dialog.

New Connection Request Policy

Specify Conditions

Specify the conditions that determine whether t
A minimum of one condition is required.

Conditions:

Condition	Value
🖧 NAS IPv4 Address	192.168.56.29

8. Select "Authenticate requests on this server" because a local NPS server is used in this example. Then click Next.

Note: Connection Request Forwarding options must match your environment.

9. When the system prompts you to select the authentication method, select the following two options:
   - Override network policy authentication settings
   - CHAP -- the Legrand PDU uses "CHAP" in this example

New Connection Request Policy

Specify Authentication Methods

Configure one or more authentication methods required
authentication, you must configure an EAP type. If you d
Protected EAP.

☑ Override network policy authentication settings

These authentication settings are used rather than the constraints and auth
connections with NAP, you must configure PEAP authentication here.

EAP types are negotiated between NPS and the client in the order in which

EAP Types:

[Add...] [Edit...] [Remove]

Less secure authentication methods:

☐ Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
   ☐ User can change password after it has expired
☐ Microsoft Encrypted Authentication (MS-CHAP)
   ☐ User can change password after it has expired
☑ Encrypted authentication (CHAP)
☐ Unencrypted authentication (PAP, SPAP)
☐ Allow clients to connect without negotiating an authentication method.

10. Select Vendor Specific to the left of the dialog, and click Add. The Add Vendor Specific Attribute dialog appears.

11. Select Custom in the Vendor field, and click Add. The Attribute Information dialog appears.

12. Click Add, and the Vendor-Specific Attribute Information dialog appears.

13. Click "Enter Vendor Code" and type *13742*.

14. Select "Yes, it conforms" to indicate that the custom attribute conforms to the RADIUS Request For Comment (RFC).

15. Click Configure Attribute, and then:

   a. Type *26* in the "Vendor-assigned attribute number" field.

   b. Select String in the "Attribute format" field.

   c. Type *Raritan:G{Admin User SystemTester}* in the "Attribute value" field. In this example, three roles 'Admin,' 'User' and 'SystemTester' are specified inside the curved brackets {}.

Note that multiple roles are separated with a space.
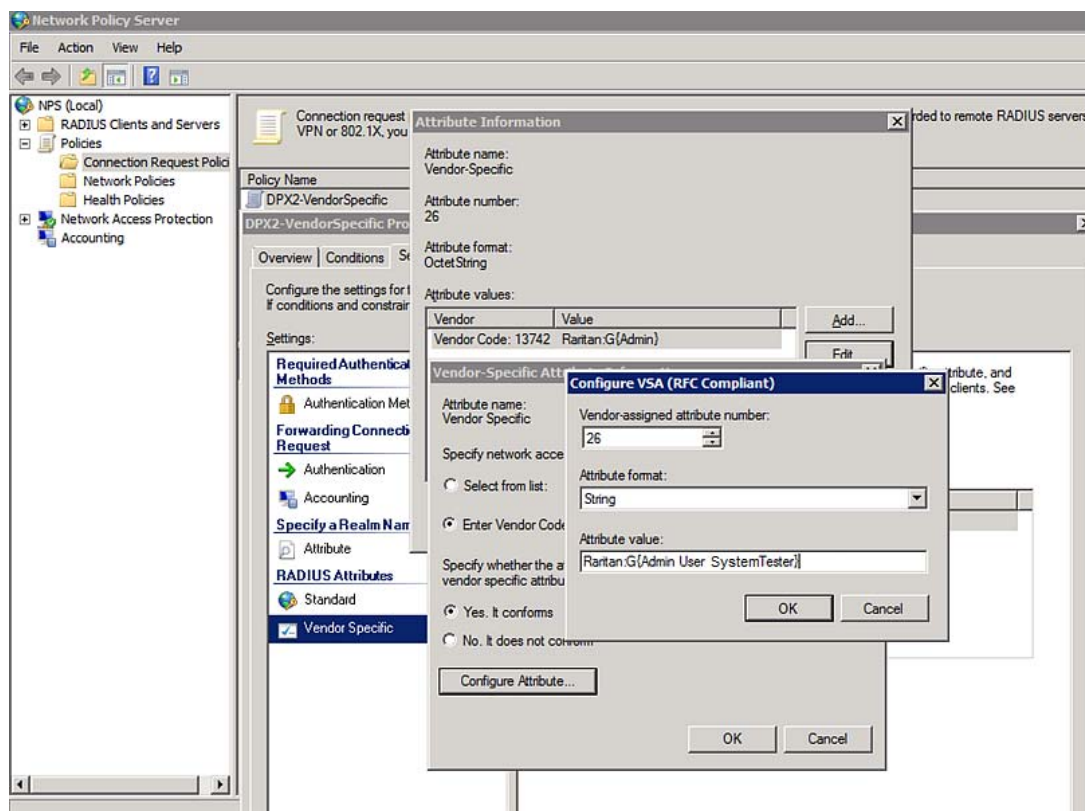
16. Click OK.

FreeRADIUS VSA Illustration

A vendor-specific dictionary file is required for the vendor-specific-attribute configuration on FreeRADIUS. Therefore, there are two major configuration steps.

a. Use a dictionary to define the Raritan vendor-specific attribute

b. Add all user data, including user names, passwords, and roles

► **Presumptions in the illustration:**

- Raritan attribute = `Raritan-User-Roles`
- User name = `steve`
- Steve's password = `test123`
- Steve's roles = `Admin`, `User` and `SystemTester`

► **Step A -- define the vendor-specific attribute in FreeRADIUS:**

1. Go to this location: `/etc/raddb/dictionary`.
2. Type the following in the Raritan dictionary file.

```
VENDOR Raritan 13742
BEGIN-VENDOR Raritan
ATTRIBUTE Raritan-User-Roles 26 string
END-VENDOR Raritan
```

► **Step B -- create a user profile for "steve" in FreeRADIUS:**

1. Go to this location: `/etc/raddb/users`.

2. Add the data of the user "steve" by typing the following. Note that the values after the equal sign (=) must be enclosed in double quotes (").

```
steve Cleartext-Password := "test123"
Raritan-PDU-User-Roles = "Raritan:G{Admin User SystemTester}"
```

AD-Related Configuration

When RADIUS authentication is intended, make sure you also configure the following settings related to Microsoft Active Directory (AD):

• Register the NPS server in AD

• Configure remote access permission for users in AD

The NPS server is registered in AD only when NPS is configured for the FIRST time and user accounts are created in AD.

If CHAP authentication is used, you must enable the following feature for user accounts created in AD:

• Store password using reversible encryption

Important: Reset the user password if the password is set before you enable the "Store password using reversible encryption" feature.

▶ **To register NPS:**

1. Open the NPS console.

2. Right-click NPS (Local) and select "Register server in Active Directory."
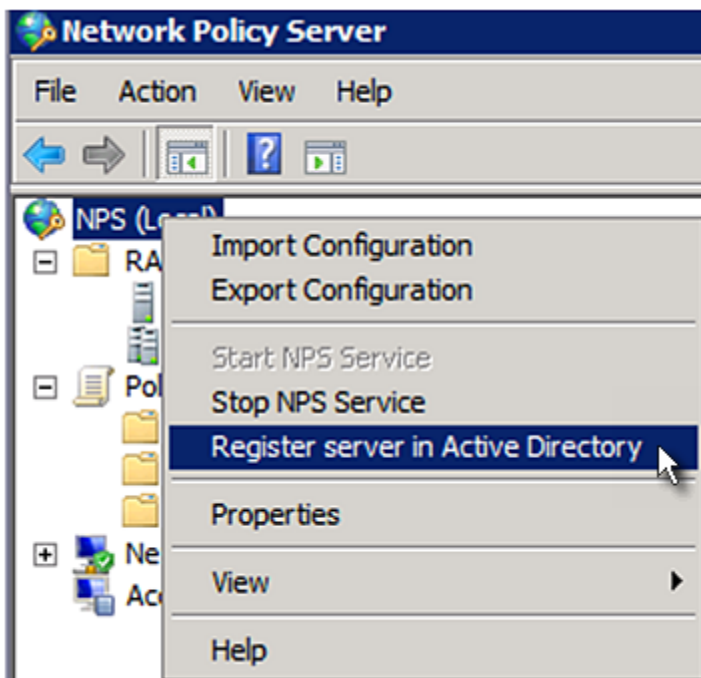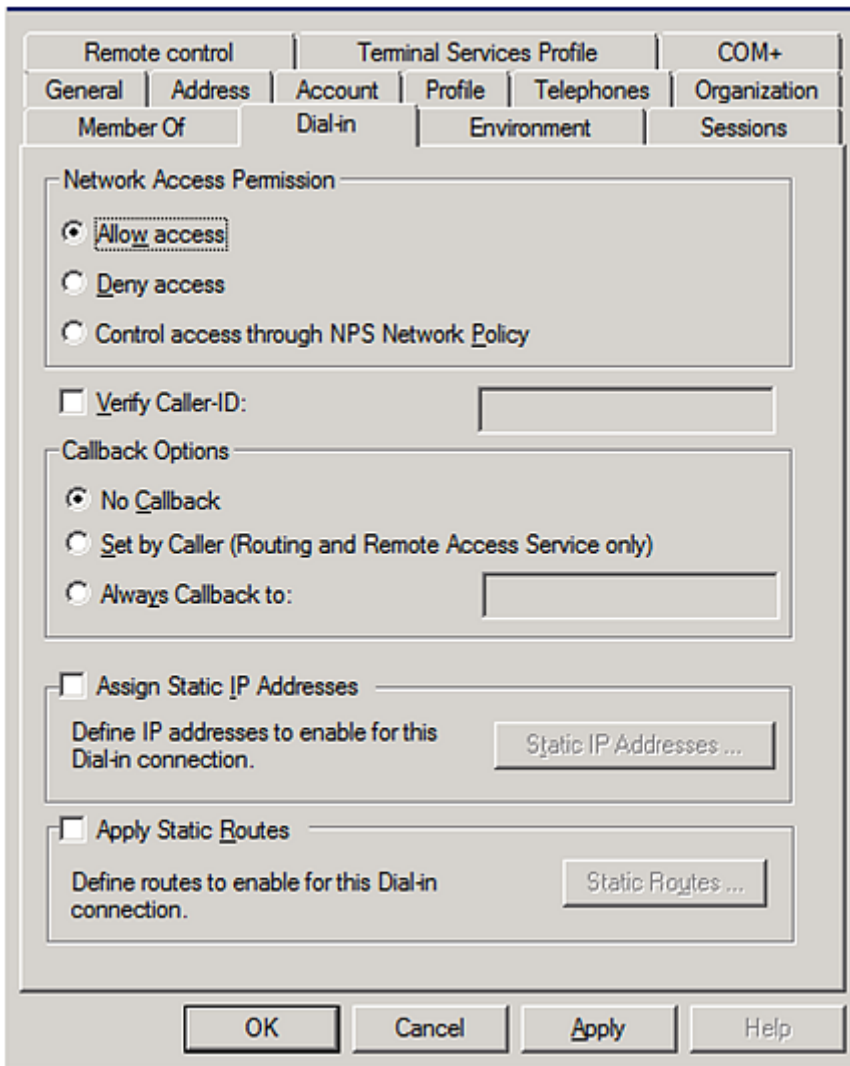
3. Click OK, and then OK again.
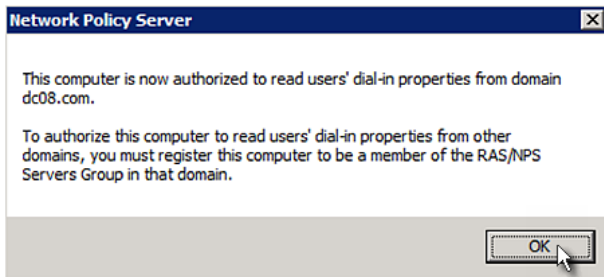
▶ **To grant Legrand PDU users remote access permission:**

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.

Additional Legrand PDU Information

In This Chapter

Reserving IP Addresses in DHCP Servers

The Legrand PDU uses its serial number as the client identifier in the DHCP request. Therefore, to successfully reserve an IP address for the Legrand PDU in a DHCP server, use the Legrand PDU device's serial number as the unique ID instead of the MAC address.

Since all network interfaces of the Legrand PDU 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 Legrand PDU 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 470).

In the following illustration, it is assumed that the Legrand PDU 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

1. In your DHCP server, bring up the New Reservation dialog, and separate the converted ASCII codes with spaces.

   For example, to reserve the IP address of the ETH1 interface, enter the following data in the dialog.

Field	Data entered
IP address	The IP address you want to reserve.
MAC address	The following ASCII codes. `50 45 47 31 41 30 30 30 30 33`
Other fields	Configure as needed.
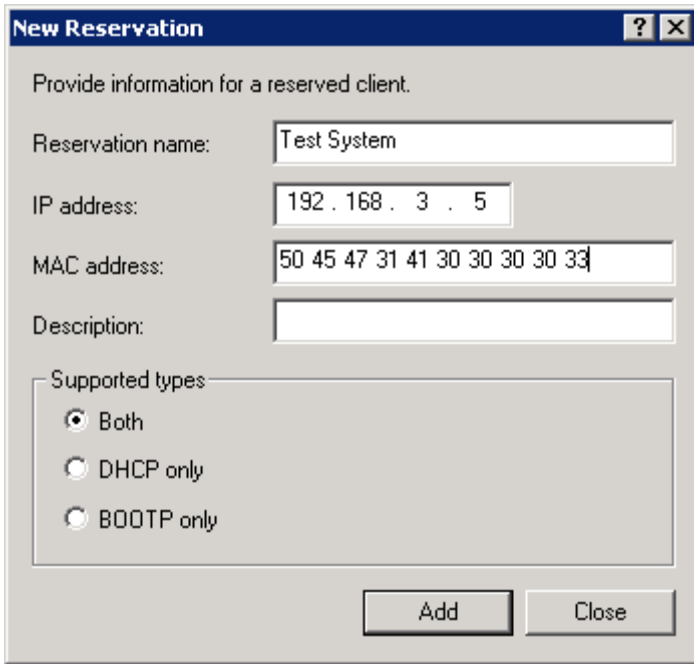
Reserving IP in Linux

There are two methods to reserve the IP address of any network interface in the standard Linux DHCP server (ISC DHCP server):

- Convert an interface's client identifier into *hexadecimal* ASCII codes.
- Use an interface's original client identifier without converting it into ASCII codes.

For each interface's client identifier, see ***Reserving IP Addresses in DHCP Servers*** (on page 470).

In the following illustrations, it is assumed that the Legrand PDU 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

1. 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
   ```

2. 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:
    `\000PEG1A00003`
3. Now enter the original client identifier with the following syntax. The client identifier is enclosed in quotation marks.

```
host mypx {
option dhcp-client-identifier = "\000PEG1A00003";
fixed-address 192.168.20.1;
}
```

Sensor Threshold Settings

This section explains the thresholds settings for a numeric sensor.

Lower Critical	✔	0	
Lower Warning	✔	0	
Upper Warning	✔	0	
Upper Critical	✔	0	
Deassertion Hysteresis		0	
Assertion Timeout		0	Samples

✖ Cancel   ✔ Save

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.

abo ve upper critical
Upper Critical
abo ve upper warning
Upper Warning
normal
Lower Warning
belo w lower warning
Lower Critical
belo w lower critical
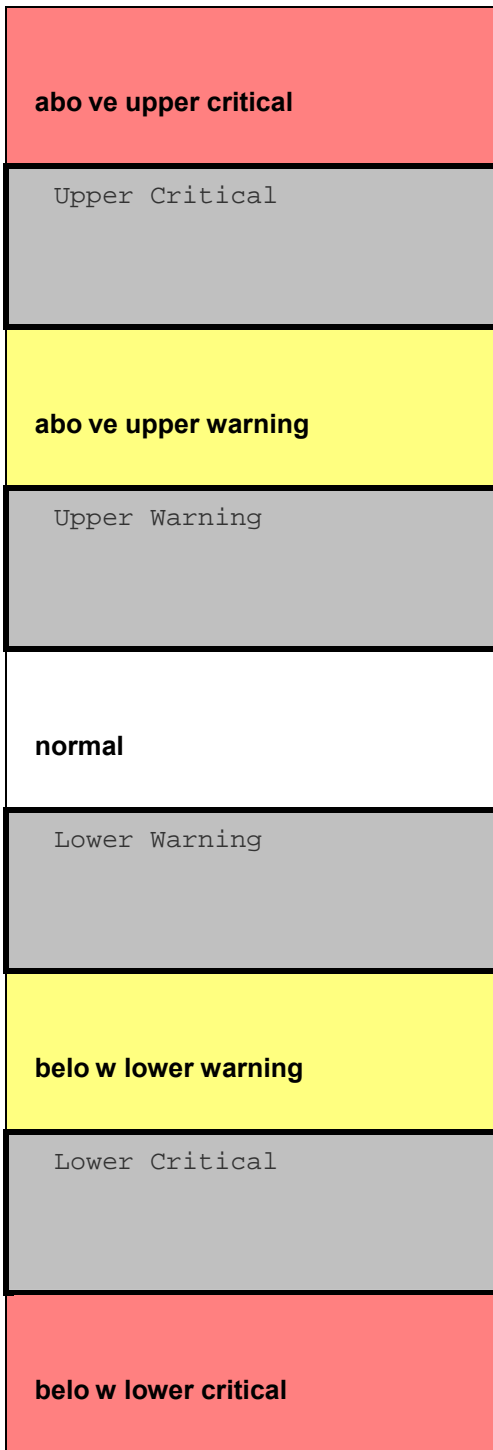
▶ **Available sensor states:**

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 120).

"To Assert" and Assertion Timeout

If multiple sensor states are available for a specific sensor, the Legrand PDU 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 Legrand PDU to assert.
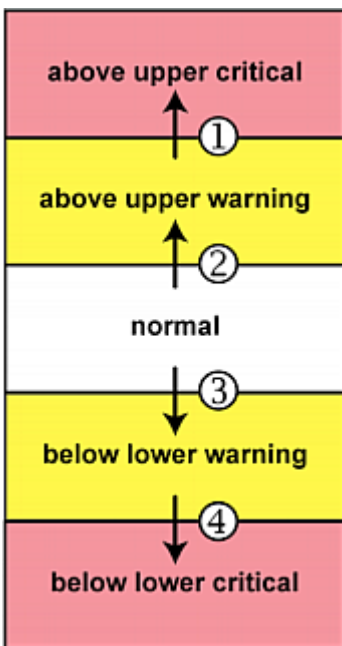
1. above upper warning --> above upper critical
2. normal --> above upper warning
3. normal --> below lower warning
4. below lower warning --> below lower critical

▶ **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 Legrand PDU triggers the "assertion" action. If that sensor changes its state again within the specified wait time, the Legrand PDU 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 Legrand PDU 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 Legrand PDU 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 Legrand PDU performs the "assertion" action to announce the "above upper warning" state.

- If the temperature drops below 25 degrees Celsius within 5 seconds, the Legrand PDU does NOT perform the "assertion" action.

"To De-assert" and Deassertion Hysteresis

After the Legrand PDU 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 Legrand PDU to de-assert the previous state.
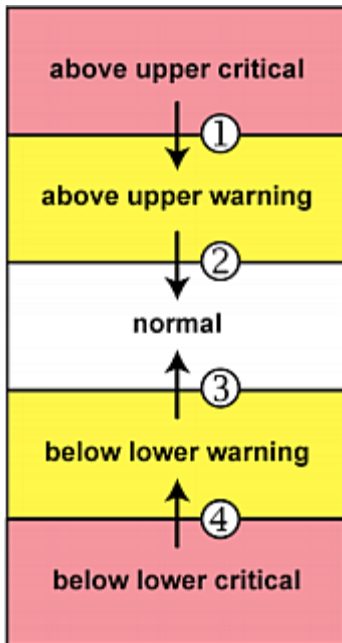
1. above upper critical --> above upper warning
2. above upper warning --> normal
3. below lower warning --> normal
4. below lower critical --> below lower warning

▶ **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 Legrand PDU 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).

▶ **How "Deassertion Hysteresis" is helpful:**

If you have created an event rule that instructs the Legrand PDU 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 Legrand PDU 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 Legrand PDU does NOT perform the "deassertion" action.
- If the temperature drops to 17 degrees Celsius or lower, the Legrand PDU performs the "deassertion" action to announce the end of the "above upper warning" state.

Default Voltage and Current Thresholds

The following are factory-default voltage and current thresholds applied to a Legrand power product. There are no default values set for *lower* current thresholds because lower thresholds are not useful.

Availability of diverse thresholds depends on the capability of the model you purchased.

▶ **Single-phase inlets or outlets:**

- **RMS voltage:**

Threshold	Default value
Lower critical	-6% of minimum rating
Lower warning	-3% of minimum rating
Upper warning	+3% of maximum rating
Upper critical	+6% of maximum rating
Hysteresis	2V

- **RMS current:**

Threshold	Default value
Upper warning	65% of rating
Upper critical	80% of rating
Hysteresis	1A

▶ **Multi-phase inlets or outlets:**

- **Line-Line RMS voltage:**

Threshold	Default value
Lower critical	-6% of minimum rating
Lower warning	-3% of minimum rating
Upper warning	+3% of maximum rating
Upper critical	+6% of maximum rating
Hysteresis	2V

- **Line RMS current:**

Threshold	Default value
Upper warning	65% of rating
Upper critical	80% of rating
Hysteresis	1A

June 2018

- **Unbalanced current:**

Threshold	Default value
Upper critical	10% -- disabled by default
Upper warning	5% -- disabled by default
Hysteresis	2%

▶ **Overcurrent protectors which aims to protect the PDU's outlets:**

- **OCP RMS current:**

Threshold	Default value
Upper critical	80% of OCP rating
Upper warning	65% of OCP rating
Hysteresis	1A

▶ **Total residual current:**

Threshold	Default value
Upper critical	30mA
Hysteresis	15mA

Altitude Correction Factors

If a Legrand 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

Unbalanced Current Calculation

Unbalanced current information is available on 3-phase models only. This section explains how Legrand PDU calculates the unbalanced current percentage.

▶ **Calculation:**

1. Calculate the average current of all 3 lines.

   ```
   Average current = (L1+L2+L3) / 3
   ```

2. Calculate each line's current unbalance by having each line current subtracted and divided with the average current.

   ```
   L1 current unbalance = (L1 - average current) / average current
   L2 current unbalance = (L2 - average current) / average current
   L3 current unbalance = (L3 - average current) / average current
   ```

3. Determine the maximum absolute value among three lines' current unbalance values.

   ```
   Maximum (|L1 current unbalance|, |L2 current unbalance|, |L3 current unbalance|)
   ```

4. Convert the maximum value to a percentage.

   ```
   Unbalanced load percent = 100 * maximum current unbalance
   ```

▶ **Example:**

- Each line's current:
  L1 = 5.5 amps
  L2 = 5.2 amps
  L3 = 4.0 amps

- Average current: (5.5+5.2+4.0) / 3 = 4.9 amps

- L1 current unbalance: (5.5 - 4.9) / 4.9 = 0.1224
- L2 current unbalance: (5.2 - 4.9) / 4.9 = 0.0612
- L3 current unbalance: (4.0 - 4.9) / 4.9 = -0.1837

- Maximum current unbalance:
  Maximum (|0.1224|, |0.0612|, |-0.1837|) = 0.1837

- Current unbalance converted to a percentage:
  100 * (0.1837) = 18%

Ways to Probe Existing User Profiles

This section indicates available ways to query existing user accounts on the Legrand PDU.

- 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.

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 Legrand PDU may fail to connect to the given host.

Therefore, DNS server settings are important for external authentication. With appropriate DNS settings, the Legrand PDU 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 173).

Cascading Troubleshooting

Any accessibility problem occurred on one of the devices in the cascading chain may result in failure to access all downstream slave devices that are connected to it.

Possible Root Causes

The following lists the network accessibility issues and possible root causes.

You can always troubleshoot the software settings by connecting the Legrand PDU to a computer if network access to that Legrand PDU fails. See **Connecting the Legrand PDU to a Computer** (on page 30).

Symptom	Probable cause
Failure to access the master device	• Anything below is lost 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 24). ▪ The wireless LAN configuration is not supported. See **Supported Wireless LAN Configuration** (on page 24). ▪ 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.
	  ▪ 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 153).
	  ▪ 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.

Tip: To determine which Legrand PDU may be the failure point of network, you may ping each Legrand PDU in the cascading chain, or check the slave-related events in the event log of each Legrand PDU. See **The Ping Tool** *(on page 485) and* **Slave Device Events in the Log** *(on page 484).*

▶ **For a pure Legrand PDU cascading chain, 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 if it is set to the Port Forwarding mode. See *Restrictions of Port-Forwarding Connections* (on page 37).

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 Legrand PDUs 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 Legrand 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 Legrand 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 Legrand PDU at the USB-A end of the USB cable logs it in the internal log. Note that the Legrand PDU 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 Legrand PDU 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 Legrand PDU provides a ping tool in the web interface and CLI so you can ping any host or Legrand PDU in your data center.

▶ **Ping via the Web Interface:**

To log in to the web interface, see *Login* (on page 79).

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 Legrand PDU or using SSH/Telnet. See *With SSH or Telnet* (on page 270).

1. You must perform the ping command in the diagnostic mode. See *Entering Diagnostic Mode* (on page 390).
2. Then perform the ping command. See *Testing the Network Connectivity* (on page 391).

Installing the USB-to-Serial Driver (Optional)

The Legrand PDU can emulate a USB-to-serial converter over a USB connection. A USB-to-serial driver named "Dominion PX2 Serial Console" is required for Microsoft® Windows® operating systems.

Download the Windows driver for USB serial console from the Legrand PDU section of 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 Legrand PDU 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 Legrand PDU to the computer via a USB cable. The driver is automatically installed.

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

1. Make sure the Legrand PDU 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 PX2 Serial Console*, and choose Update Driver.
3. Select the option of driver installation from a specific location, and then specify the location where both *dominion-serial.inf* and *dominion-serial.cat* are stored.

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

4. Wait until the installation is complete.

Note: If the Legrand PDU 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 Legrand PDU 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 Legrand PDU 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 140).

▶ **To configure the Legrand PDU:**

1. On the computer connected to the Legrand PDU, 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 PX2 Serial Console" under the Ports group.

2. In the communications program, press Enter to send a carriage return to the Legrand PDU.
3. The Legrand PDU 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

To set	Use this command
IPv4 or IPv6 third DNS server	`network dns thirdServer <ip address>` <ip address> = DNS server's IP address

► **Commands for wireless networking:**

• **General wireless settings**:

To set or enable	Use this command
Wireless interface	`network wireless enabled <option>` <option> = *true*, or *false*
SSID	`network wireless SSID <ssid>` <ssid> = SSID string
BSSID	`network wireless BSSID <bssid>` <bssid> = AP MAC address or *none*
802.11n protocol	`network wireless enableHT <option>` <option> = *true*, or *false*
Authentication method	`network wireless authMethod <method>` <method> = *psk* or *eap*
PSK	`network wireless PSK <psk>` <psk> = PSK string
EAP outer authentication	`network wireless eapOuterAuthentication <outer_auth>` <outer_auth> = *PEAP*
EAP inner authentication	`network wireless eapInnerAuthentication <inner_auth>` <inner_auth> = *MSCHAPv2*
EAP identity	`network wireless eapIdentity <identity>` <identity> = your user name for EAP authentication
EAP password	`network wireless eapPassword` When prompted to enter the password for EAP authentication, type the password.

To set or enable	Use this command
EAP CA certificate	`network wireless eapCACertificate` When prompted to enter the CA certificate, open the certificate with a text editor, copy and paste the content into the communications program.

The content to be copied from the CA certificate does NOT include the first line containing "BEGIN CERTIFICATE" and the final line containing "END CERTIFICATE." If a certificate is installed, configure the following:

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

- **Wireless IPv4 / IPv6 settings:**

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

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

▶ **To verify network settings:**

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

- `show network`

The IP address configured may take seconds to take effect.

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
- Outlet names and states

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 490).
- For an example of creating and uploading a TLS certificate to Legrand PDU, see *Illustration - GMAIL SMTP Certificate Chain* (on page 492).

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 492).

A certificate or a chain of certificates is used for trusting a TLS server that you want to connect.

The receiver, such as Legrand PDU, 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.

- **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 Legrand PDU:**

Because the TLS server provides only 'Certificate C', you need to upload a file containing the the missing certificates of the chain (that is, 'Certificate A' and 'Certificate B') to the receiver.
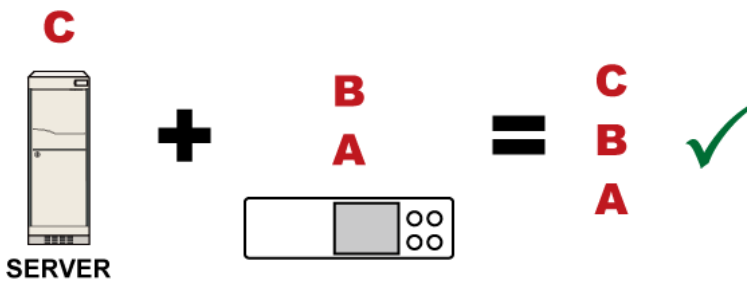
In reality some servers may provide a partial (or even a full) certificate chain instead of a single server certificate. If your server provides a partial certificate chain containing 'Certificate B' and 'Certificate C', then you only need to upload 'Certificate A" to the receiver. If the server has a full certificate chain containing Certificates 'A', 'B', and 'C', then you also need to upload the root certificate 'A".
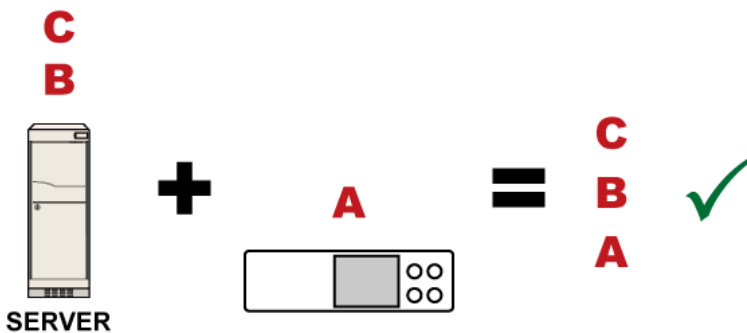
Warning: The certificate (chain) uploaded to the receiver must always contain the ROOT certificate even though the TLS server provides the root certificate. When uploading a (partial) chain onto the Legrand PDU, it means you trust each certificate in the chain to certify the authenticity of certificates a server sends to Legrand PDU. 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.
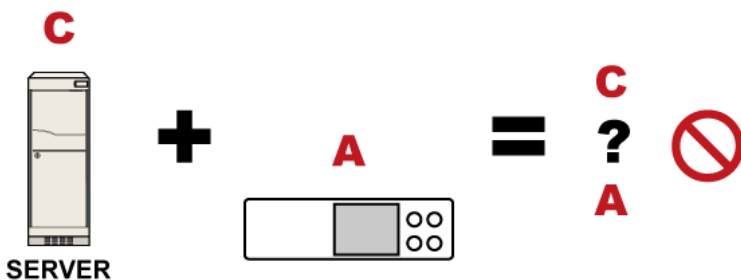
For Legrand PDU, if any required certificate is missing, a certificate error message similar to the following is shown on the Legrand PDU web interface.
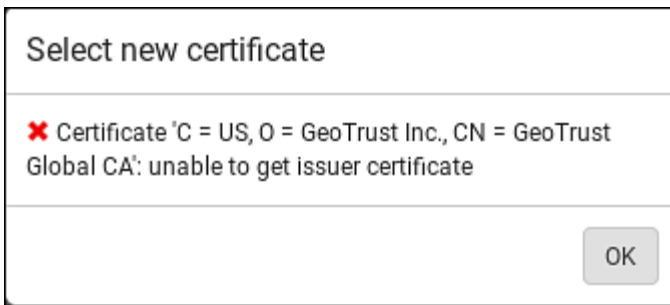
It is NOT recommended to upload the server certificate to the receiver except when it is a self-signed certificate. Using self-signed server certificates is also not recommended and may not even work in all cases.

▶ **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.
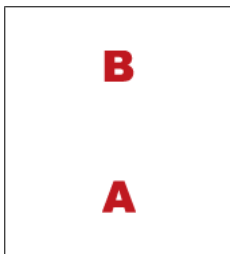
- The top is the final intermediate certificate of the chain "B" if you have to upload a partial chain.
- The bottom is always the root certificate "A".
- When copying multiple certificates to a single file, make sure you also copy the lines of BEGIN CERTIFICATE and END CERTIFICATE from each certificate.

Illustration - GMAIL SMTP Certificate Chain

If you will apply your company's SMTP service to Legrand PDU, ignore this GMAIL illustration topic. Simply contact your IT department to retrieve the appropriate certificate (chain) file and upload it to the Legrand PDU.

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:
        - *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 Legrand PDU.
- If not, you need to find all missing issuer certificates, including the root certificate, and upload them to Legrand PDU.

▶ **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 Legrand PDU:**

1. Paste the root certificate's content into a plain text file that will be uploaded to Legrand PDU.
   - 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 Legrand PDU 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 490).*

▶ **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 Legrand PDU 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 Legrand PDU online help:**

1. Click Online Documentation. See **Web Interface Overview** (on page 82).
2. The online help opens in the default web browser.
3. To view the content of any topic, click the topic in the left pane. Then its content is displayed in the right pane.
4. To select a different topic, do any of the following:
   - To view the next topic, click the Next icon ⊕ in the toolbar.
   - To view the previous topic, click the Previous icon ⊕.
   - To view the first topic, click the Home icon 🏠.
5. To expand or collapse a topic that contains sub-topics, do the following:
   - To expand any topic, click the white arrow ▷ prior to the topic, or double-click that topic. The arrow turns into a black, gradient arrow ◢, and sub-topics appear below the topic.

- To collapse any expanded topic, click the black, gradient arrow ◢ prior to the topic, or double-click the expanded topic. The arrow then turns into a white arrow ▷, and all sub-topics below that topic disappear.

6. To search for specific information, type the key word(s) or string(s) in the Search text box, and press Enter or click the Search icon 🔍 to start the search.

   - If necessary, select the "Match partial words" checkbox to include information matching part of the words entered in the Search text box.

   The search results are displayed in the left pane.

7. To have the left pane show the list of topics, click the Contents tab at the bottom.

8. To show the Index page, click the Index tab.

9. To email any URL link to the currently selected topic to any person, click the "Email this page" icon ✉️ in the toolbar.

10. To email your comments or suggestions regarding the online help to Legrand, click the "Send feedback" icon 💬.

11. To print the currently selected topic, click the "Print this page" icon 🖨️.

Integration

The Legrand PDU can work with certain Raritan or third-party products to provide diverse power solutions.

In This Chapter

Cascading with Raritan PX2-Based Products

You can cascade Legrand PDUs only. See *Cascading Multiple Legrand PDUs for Sharing Ethernet Connectivity* (on page 32).

However, you can also cascade Legrand PDUs with Raritan's PX2-based products via USB or Ethernet ports. These Raritan products include:

- PX2 series power distribution units (PDUs)
- PX3 series PDUs, including PX3-iX7
- EMX asset management devices
- PX3TS transfer switches, including PX3TS-iX7
- Branch Circuit Monitor 1 (BCM1)
- Branch Circuit Monitor 2 (BCM2), PMC and PMMC series, including:
    - BCM2-iX7
    - PMC-iX7

For detailed information on the cascading configuration and restrictions, refer to the *Cascading Guide*, which is available from the Legrand PDU section of Raritan website's *Support page* (*http://www.raritan.com/support/*).

Connection to Raritan Serial Access Products

Legrand PDU supports the integration with Raritan's serial access products - Dominion SX and Dominion SX II.

You can access the CLI of the Legrand PDU via SX / SX II.

To only access the CLI of the Legrand PDU via SX / SX II, treat the Legrand PDU as a serial device by connecting SX /SX II to the PDU's serial port labeled CONSOLE.

For more information on these Dominion serial access products, refer to:

- SX or SX II User Guide on the *Support page* (*http://www.raritan.com/support/*)
- SX or SX II Online Help on the *Product Online Help page* (*http://www.raritan.com/support/online-help/*)

Power IQ Configuration

Sunbird's Power IQ is a software application that collects and manages the data from different PDUs installed in your server room or data center. With this software, you can:

- Do bulk configuration for multiple PDUs
- Name outlets on different PDUs
- Switch on/off outlets on outlet-switching capable PDUs

For more information on Power IQ, refer to the Power IQ online help on the Sunbird website: *http://support.sunbirddcim.com.*

dcTrack

Sunbird's dcTrack® is a product that allows you to manage the data center. The Legrand PDU is categorized as a power item in dcTrack. dcTrack offers an import wizard for conveniently adding the Legrand PDU as well as other IT equipment to dcTrack for management.

You can use dcTrack to:

- Record and manage the data center infrastructure and assets
- Monitor the electrical consumption of the data center
- Track environmental factors in the data center, such as temperature and humidity
- Optimize the data center growth

For more information on dcTrack, refer to the online help accessible from the dcTrack application, or user documentation available on the Sunbird's website: *http://support.sunbirddcim.com.*

dcTrack Overview

dcTrack® is a powerful and intelligent data center management and automation application.

It has been designed by data center and IT professionals to provide broad and deep visibility into the data center. It empowers data center managers to plan for growth and change by optimizing their current operations, assets, and infrastructure.

With dcTrack, you can view everything in the data center from servers, blades, virtual servers and applications to data networks, IP addressing space and cabling. dcTrack also allows you to track real-time power consumption and manage raised floor space and rack elevations.

Use dcTrack to build your floor map data center map directly in the application, or import an existing floor map into the dcTrack. Further, dcTrack allows you to import AutoCAD® 2012 (and earlier) objects to build a data center map.

If you currently maintain data center information in spreadsheet format, that data can be imported into dcTrack using the Import wizard.

Isolate potential problems with end-to-end power and data circuits by visually tracing them. This allows you to identify all intermediate circuit points and locate problems.

By using dcTrack's workflow and change management feature, data center managers are better able to enforce best practices across the enterprise and meet ITIL framework guidelines. You can also opt to skip the Change Control workflow process and work in Request Bypass so requests are processed immediately.

dcTrack® can be used as a standalone product or integrated with Power IQ® for power and environmental monitoring.

June 2018

Index

D

June 2018

June 2018