PXC and PXO

User Guide

Xerus™ Firmware v3.6.10

Copyright © 2020 Raritan, Inc.
PXC_PXO_UserGuide_0C_3.6.10
October 2020
255-80-0066-00

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 Raritan 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 Raritan 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**.

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

© Copyright 2020 Raritan, Inc. All third-party software and hardware mentioned in this document are registered trademarks or trademarks of and are the property of their respective holders.

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

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

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

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.

SecureLock™

Contents

Safety Guidelines ii

Safety Instructions iii

Applicable Models xv

Chapter 1 Introduction 1

Available PDU Models 1
Model List 2
Package Contents 2
PXC 2
PXO 3
APIPA and Link-Local Addressing 3
Before You Begin 4
Unpacking the Product and Components 4
Preparing the Installation Site 4
Checking the Branch Circuit Rating 5
Filling Out the Equipment Setup Worksheet 5

Chapter 2 Rackmount and Locking Outlets 6

Circuit Breaker Orientation Limitation 6
Rack-Mounting the PDU 6
Rackmount Safety Guidelines 6
PXC Rackmount Methods 6
PXO Rackmount Method 10
Locking Outlets 10

Chapter 3 Initial Installation and Configuration 11

Connecting the PDU to a Power Source 11
Connecting the PXC/PXO to Your Network 12
USB Wireless LAN Adapters 13
Supported Wireless LAN Configuration 13
Dual Ethernet Connection 14
Configuring the PXC/PXO 14
Connecting a Mobile Device to PXC/PXO 15
Connecting the PXC/PXO to a Computer 21

Bulk Configuration Methods 23
Cascading Multiple PXC/PXO Devices for Sharing Ethernet Connectivity 24
Cascading All Devices via USB 26
Extended Cascading with PXC/PXO Devices 28
Restrictions of Port-Forwarding Connections 31

Chapter 4 Connecting External Equipment (Optional) 34

Connecting Raritan Environmental Sensor Packages 34
Identifying the Sensor Port 35
DX2 Sensor Packages 35
DX Sensor Packages 38
DPX3 Sensor Packages 39
DPX2 Sensor Packages 40
DPX Sensor Packages 43
Using an Optional DPX3-ENVHUB4 Sensor Hub 48
Mixing Diverse Sensor Types 49
Connecting a Logitech Webcam 54
Connecting a Modbus RTU Device or Bus 54

Chapter 5 Introduction to PDU Components 56

Panel Components 56
Inlet 56
Outlets 56
Connection Port Functions 57
Front Panel Display 59
Reset Button 93
PXC's Energy Pulse LED 93
Circuit Breakers 94
Resetting the Button-Type Circuit Breaker 94
Resetting the Handle-Type Circuit Breaker 95

Chapter 6 Using the Web Interface 96

Supported Web Browsers 96
Login, Logout and Password Change 96
Login 96
Changing Your Password 98
Remembering User Names and Passwords 99
Logout 99
Web Interface Overview 100
Menu 103
Quick Access to a Specific Page 105
Sorting a List 106

Dashboard 107
Dashboard - Inlet I1 109
Dashboard - OCP 111
Dashboard - Alerted Sensors 112
Dashboard - Inlet History 114
Dashboard - Alarms 115
PDU 117
Options for Outlet State on Startup 119
Initialization Delay Use Cases 119
Inrush Current and Inrush Guard Delay 120
Time Units 120
Inlet 121
Outlets 123
Available Data of the Outlets Overview Page 127
Setting Outlet Power-On Sequence and Delay 128
Setting Non-Critical Outlets 129
Load Shedding Mode 130
Individual Outlet Pages 133
Outlet Groups 137
Creating an Outlet Group 138
Outlet Group Power Control 139
Modifying an Outlet Group 142
Deleting an Outlet Group 144
Visiting Other Pages from Current Group 145
OCPs 147
Individual OCP Pages 149
Peripherals 154
Yellow- or Red-Highlighted Sensors 160
Managed vs Unmanaged Sensors/Actuators 162
Sensor/Actuator States 163
Finding the Sensor's Serial Number 164
Identifying the Sensor Position and Channel 165
How the Automatic Management Function Works 167
Managing One Sensor or Actuator 167
Individual Sensor/Actuator Pages 169
Z Coordinate Format 174
User Management 176
Creating Users 177
Editing or Deleting Users 181
Creating Roles 182
Editing or Deleting Roles 184
Setting Your Preferred Measurement Units 185
Setting Default Measurement Units 186
Device Settings 188
Configuring Network Settings 190
Configuring Network Services 216
Configuring Security Settings 227
Setting the Date and Time 251
Door Access Control 255

Event Rules and Actions 259
Setting Data Logging 310
Configuring Data Push Settings 311
Monitoring Server Accessibility 316
Front Panel Settings 323
Configuring the Serial Port 324
Lua Scripts 324
Miscellaneous 329
Maintenance 331
Device Information 333
Viewing Connected Users 338
Viewing or Clearing the Local Event Log 339
Updating the PXC/PXO Firmware 340
Viewing Firmware Update History 342
Bulk Configuration 343
Backup and Restore of Device Settings 349
Network Diagnostics 351
Downloading Diagnostic Information 352
Hardware Issue Detection 352
Rebooting the PXC/PXO 354
Resetting All Settings to Factory Defaults 354
Retrieving Software Packages Information 355
Webcam Management 356
Configuring Webcams and Viewing Live Images 358
Sending Links to Snapshots or Videos 361
Viewing and Managing Locally-Saved Snapshots 363
Changing Storage Settings 365
SmartLock and Card Reader 369
SmartLock 371
Card Readers 376

Chapter 7 Using SNMP 378

Enabling and Configuring SNMP 378
SNMPv2c Notifications 379
SNMPv3 Notifications 380
Downloading SNMP MIB 383
SNMP Gets and Sets 383
The PXC/PXO MIB 384
A Note about Enabling Thresholds 385

Chapter 8 Using the Command Line Interface 386

About the Interface 386
Logging in to CLI 387
With HyperTerminal 387
With SSH or Telnet 388

Different CLI Modes and Prompts 389
Closing a Local Connection 389
The ? Command for Showing Available Commands 389
Querying Available Parameters for a Command 390
Showing Information 391
Network Configuration 391
PDU Configuration 395
Outlet Information 396
Outlet Group Information 397
Inlet Information 398
Overcurrent Protector Information 399
Date and Time Settings 400
Default Measurement Units 400
Environmental Sensor Information 401
Environmental Sensor Package Information 402
Actuator Information 403
Inlet Sensor Threshold Information 404
Inlet Pole Sensor Threshold Information 406
Overcurrent Protector Sensor Threshold Information 408
Environmental Sensor Threshold Information 409
Environmental Sensor Default Thresholds 410
Security Settings 411
Authentication Settings 412
Existing User Profiles 413
Existing Roles 414
Load Shedding Settings 414
Serial Port Settings 414
EnergyWise Settings 415
Event Log 415
Network Connections Diagnostic Log 416
Server Reachability Information 416
Command History 417
Reliability Data 418
Reliability Error Log 418
Reliability Hardware Failures 418
Examples 418
Clearing Information 420
Clearing Event Log 421
Clearing Diagnostic Log for Network Connections 421
Configuring the PXC/PXO Device and Network 421
Entering Configuration Mode 421
Quitting Configuration Mode 422
PDU Configuration Commands 422
Network Configuration Commands 430
Time Configuration Commands 461
Checking the Accessibility of NTP Servers 466
Security Configuration Commands 466
Outlet Configuration Commands 487
Outlet Group Configuration Commands 489

Inlet Configuration Commands 491
Overcurrent Protector Configuration Commands 493
User Configuration Commands 493
Role Configuration Commands 505
Authentication Commands 509
Environmental Sensor Configuration Commands 521
Configuring Environmental Sensors' Default Thresholds 525
Sensor Threshold Configuration Commands 527
Actuator Configuration Commands 537
Server Reachability Configuration Commands 538
EnergyWise Configuration Commands 541
Serial Port Configuration Commands 543
Multi-Command Syntax 544
Load Shedding Configuration Commands 546
Enabling or Disabling Load Shedding 546
Power Control Operations 547
Turning On the Outlet(s) 547
Turning Off the Outlet(s) 548
Power Cycling the Outlet(s) 549
Canceling the Power-On Process 551
Example - Power Cycling Specific Outlets 551
Actuator Control Operations 551
Switching On an Actuator 552
Switching Off an Actuator 552
Example - Turning On a Specific Actuator 553
Unblocking a User 553
Resetting the PXC/PXO 553
Restarting the PDU 553
Resetting to Factory Defaults 554
Network Troubleshooting 554
Entering Diagnostic Mode 554
Quitting Diagnostic Mode 555
Diagnostic Commands 555
Retrieving Previous Commands 557
Automatically Completing a Command 557
Logging out of CLI 558

Chapter 9 Using SCP Commands 559

Firmware Update via SCP 559
Bulk Configuration via SCP 560
Backup and Restore via SCP 561
Downloading Diagnostic Data via SCP 562
Uploading or Downloading Raw Configuration Data 564
Keys that Cannot Be Uploaded 567

Appendix A Specifications 569

Maximum Ambient Operating Temperature 569
Serial RS-232 "RJ-45" Port Pinouts 569
Sensor RJ-45 Port Pinouts 569

Appendix B Equipment Setup Worksheet 571

Appendix C Configuration or Firmware Upgrade with a USB Drive 575

Device Configuration/Upgrade Procedure 575
System and USB Requirements 576
Configuration Files 577
fwupdate.cfg 578
config.txt 582
devices.csv 585
Creating Configuration Files via Mass Deployment Utility 586
Data Encryption in 'config.txt' 587
Firmware Upgrade via USB 588

Appendix D Bulk Configuration or Firmware Upgrade via DHCP/TFTP 590

Bulk Configuration/Upgrade Procedure 591
TFTP Requirements 592
DHCP IPv4 Configuration in Windows 592
DHCP IPv6 Configuration in Windows 602
DHCP IPv4 Configuration in Linux 609
DHCP IPv6 Configuration in Linux 611

Appendix E Raw Configuration Upload and Download 613

Downloading Raw Configuration 613
Download via Web Browsers 613
Download via Curl 614
Uploading Raw Configuration 615
Upload via Curl 616
Curl Upload Return Codes 617

Raritan
A brand of legrand

Appendix F Resetting to Factory Defaults 619

Using the Reset Button ... 619
Using the CLI Command ... 620

Appendix G LDAP Configuration Illustration 621

Step A. Determine User Accounts and Roles ... 621
Step B. Configure User Groups on the AD Server ... 622
Step C. Configure LDAP Authentication on the PXC/PXO ... 623
Step D. Configure Roles on the PXC/PXO ... 626

Appendix H Updating the LDAP Schema 629

Returning User Group Information ... 629
From LDAP/LDAPS ... 629
From Microsoft Active Directory ... 629
Setting the Registry to Permit Write Operations to the Schema ... 630
Creating a New Attribute ... 630
Adding Attributes to the Class ... 631
Updating the Schema Cache ... 633
Editing rciusergroup Attributes for User Members ... 633

Appendix I RADIUS Configuration Illustration 636

Standard Attributes ... 636
NPS Standard Attribute Illustration ... 636
FreeRADIUS Standard Attribute Illustration ... 654
Vendor-Specific Attributes ... 655
NPS VSA Illustration ... 655
FreeRADIUS VSA Illustration ... 667
AD-Related Configuration ... 668

Appendix J Additional PXC/PXO Information 672

Reserving IP Addresses in DHCP Servers ... 672
Reserving IP in Windows ... 673
Reserving IP in Linux ... 674
Sensor Threshold Settings ... 676
Thresholds and Sensor States ... 676
"To Assert" and Assertion Timeout ... 679
"To De-assert" and Deassertion Hysteresis ... 681

Default Voltage and Current Thresholds 684
Altitude Correction Factors 686
Unbalanced Current Calculation 686
Ways to Probe Existing User Profiles 688
Role of a DNS Server 688
Cascading Troubleshooting 688
Possible Root Causes 688
Slave Device Events in the Log 691
The Ping Tool 692
Installing the USB-to-Serial Driver (Optional) 693
Initial Network Configuration via CLI 694
Device-Specific Settings 701
TLS Certificate Chain 702
What is a Certificate Chain 702
Illustration - GMAIL SMTP Certificate Chain 706
Browsing through the Online Help 708

Appendix K Integration 710

Connection to Raritan Serial Access Products 710
Power IQ Configuration 710
dcTrack 711
dcTrack Overview 712

Appendix L Third Party Licenses 713

Licenses - Bind9 713
Licenses - Clish 723
Licenses - Dropbear 731
Licenses - FreeType 734
Licenses - IW 736
Licenses - JSON-C 737
Licenses - LIBTIRPC 738
Licenses - LIBXML2 738
Licenses - Mbus 739
Licenses - Net-SNMP 739
Licenses - Open LDAP 748
Licenses - OpenSSL 750
Licenses - Wireless-RegDB 753
Licenses - WPA Supplicant and Hostapd 753

Index 755

Applicable Models

This User Guide is applicable to all the following PDU Generations.

- PXC Generation (1000/2000 series)
- PXO Generation (1000/2000 series)

Any PDU Generations can be associated with existing metering families called "Series", from 1000 series to 2000 series.

For example, PXC-2000 and PXO-2000 series are all inlet metered and outlet switched PDUs, but have different controller generations.

Note: For information on other Raritan PX PDU models, such as PX2 and PX3 series, refer to respective Online Help or User Guide on Raritan website's **Support page** *(***http://www.raritan.com/support/***).*

PX models comparison in brief:

Features	Inlet power measurement	Outlet power measurement	Outlet switching	Load shedding
1000 Series	✓			
2000 Series	✓		✓	✓
3000 Series (Inline meters)		✓		
4000 Series	✓	✓		
5000 Series	✓	✓	✓	✓

Important: PDUs with similar model names but of different product families may vary in their designs. For example, PX2-5660V and PX3-5660V do NOT share the same outlet sequence and technical designs. For details on a model's technical design, refer to their product specifications on Raritan website's *PDU Product Selector page https://www.raritan.com/product-selector***.**

Comparison between PX2, PX3, PXC and PXO series:

Product models	PX2	PX3	PXC / PXO
Front panel display	LED display	Dot-matrix LCD display	Dot-matrix LCD display
Outlet latching relays		*	
Number of LAN ports	1	2	2
Maximum LAN rate	100 Mbps **	1,000 Mbps	100 Mbps
Replaceable controller		***	
Number of USB-A ports	1	2	1
Maximum USB rate	12 Mbps	480 Mbps	480 Mbps
RS-232 port (CONSOLE/MODEM)	Male DB9 Connector	RJ-45 Connector	RJ-45 Connector
Expansion ports		****	
SENSOR port type	RJ-12	RJ-45	RJ-45

* Only PX3 models with outlet switching have outlet latching relays.

** A few customized PX2 models also support the Ethernet speed up to 1000 Mbps.

*** Only PX3 "Zero U" models have the replaceable controller.

**** PX3 Expansion port is designed for power sharing of controllers.

***Note**: PX3 in this table only refers to PX3 PDUs with "iX7" controller.*

Chapter 1 Introduction

PXC/PXO 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 PXC/PXO is distribution of power to information technology equipment such as computers and communication equipment.

Raritan offers different types of PXC/PXO 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.

Where to use PXC:

- An information technology equipment room where information technology equipment is typically mounted.

Where to use PXO:

- Regular offices where information technology equipment for *average consumers* is mounted.

For the differences between PXO and PXC, refer to the following section.

In This Chapter

Available PDU Models 1
Package Contents 2
APIPA and Link-Local Addressing 3
Before You Begin 4

Available PDU Models

This User Guide introduces two types of Raritan PDU models -- PXO and PXC, both of which are inlet metered PDUs.

Comparison between PXO and PXC:

Item	Difference
Target market	• PXC is designed for an information technology equipment room like data centers or server rooms. • PXO is designed for regular offices.
Mechanical design	• PXO is usually smaller than PXC and has much fewer outlets. • PXC has more rackmount methods than PXO. See ***Rack-Mounting the PDU*** (on page 6).

Item	Difference
Support for DX2-DH2C2 door handle controller	• PXC supports DX2-DH2C2. • PXO does NOT support DX2-DH2C2. See ***SmartLock and Card Reader*** (on page 369).
Energy pulse output	• Some PXC models support this feature. • **NO** PXO models support this feature. See ***PXC's Energy Pulse LED*** (on page 93).

Comparison between metered and switched PDUs:

PXO and PXC models include metered and switched PDUs.

Features	Inlet power measurement	Outlet switching	Load shedding
Metered PDUs	✓		
Switched PDUs	✓	✓	✓

Model List

PXC/PXO comes in several models that are built to stock and can be obtained almost immediately. Raritan also offers custom models that are built to order and can only be obtained on request.

Download the PXC/PXO 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.

PXC

- One PXC
- Buttons (Zero U), or bracket pack and screws (1U/2U)
- Quick Setup Guide

Tip: For PXC rackmount instructions, see **PXC Rackmount Methods** *(on page 6).*

PXO

- One PXO
- Brackets and screws
- Quick Setup Guide

Tip: For PXO rackmount instructions, see **PXO Rackmount Method** *(on page 10).*

APIPA and Link-Local Addressing

PXC/PXO supports Automatic Private Internet Protocol Addressing (APIPA).

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

Exception: PXC/PXO in the Port Forwarding mode does not support APIPA. See **Setting the Cascading Mode** *(on page 207).*

Once the PXC/PXO 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 PXC/PXO, but no IP address is assigned to the PXC/PXO.

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

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

- The PXC/PXO 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 PXC/PXO. See ***Configuring Network Settings*** (on page 190).

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

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

Retrieval of the link-local address:

- See ***Device Info*** (on page 83).

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 PXC/PXO and other equipment from the box in which they were shipped. See ***Package Contents*** (on page 2) 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 Raritan Technical Support Department for assistance.
4. Verify that all circuit breakers on the PXC/PXO 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 Raritan Technical Support for the maximum operating temperature for your model. See **Maximum Ambient Operating Temperature** *(on page 569).*

2. Allow sufficient space around the PXC/PXO for cabling and outlet connections.
3. Review ***Safety Instructions*** (on page iii) listed in this User Guide.

Raritan
A brand of legrand

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 571). 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.

Chapter 2 Rackmount and Locking Outlets

In This Chapter

Circuit Breaker Orientation Limitation 6
Rack-Mounting the PDU 6
Locking Outlets 10

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 PXC/PXO.

Rackmount Safety Guidelines

In Raritan 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 569) 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.

PXC Rackmount Methods

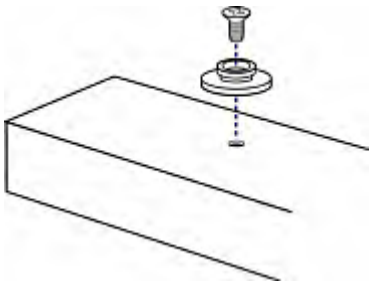
The proper PXC rackmount method is model dependent.

Mounting Zero U Models Using Two Rear Buttons

The following describes how to mount a PXC using two buttons only. If your PDU has circuit breakers implemented, read ***Circuit Breaker Orientation Limitation*** (on page 6) before mounting it.

To mount Zero U models using two buttons:

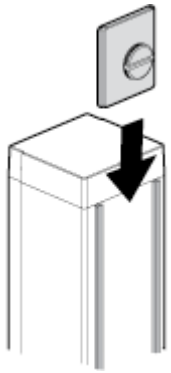
1. Turn to the rear of the PXC.
2. Locate two screw holes on the rear panel: one near the bottom and the other near the top (the side of cable gland).
3. Screw a button in the screw hole near the bottom. The recommended torque for the button is 1.96 N·m (20 kgf·cm).



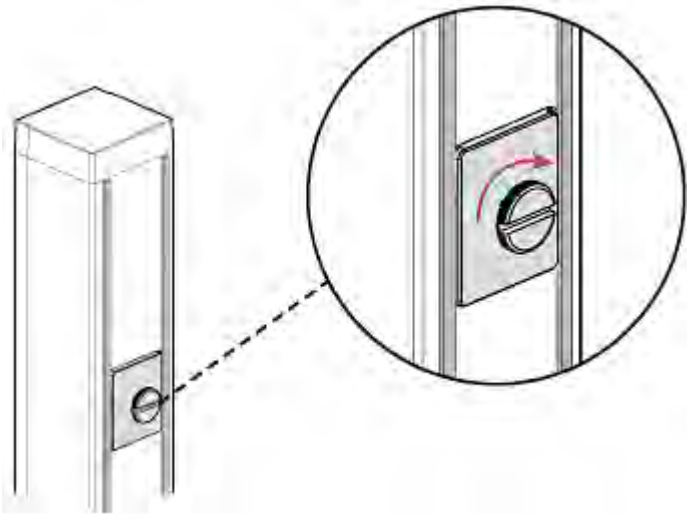
4. Screw a button in the screw hole near the top. The recommended torque for the button is 1.96 N·m (20 kgf·cm).
5. Ensure that the two buttons can engage their mounting holes in the rack or cabinet simultaneously.
6. Press the PXC device forward, pushing the mounting buttons through the mounting holes, then letting the device drop slightly. This secures the PXC device in place and completes the installation.

Mounting Zero U Models with Mount Buttons

1. Turn to the rear of the PXC.
2. Align and slide the Raritan-provided mounting button to the rear rail of the PDU.



3. Turn the button clockwise until it is securely locked in place.



4. Repeat the same steps to install the other button onto the PDU's rear side.

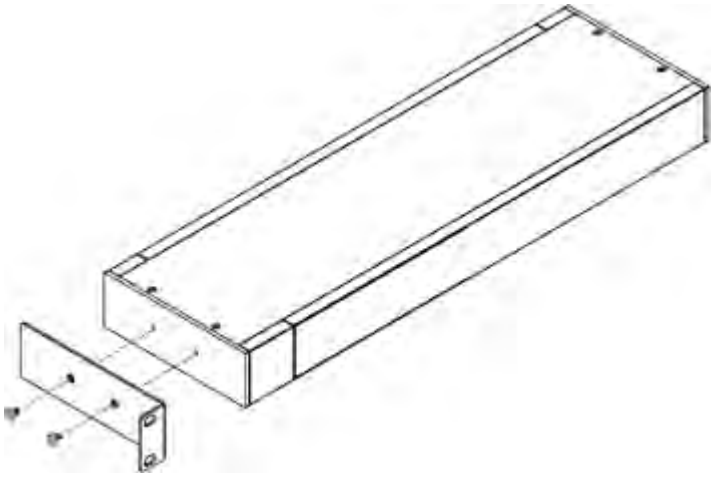
5. Properly install the PDU by fitting the attached rear buttons into position of the rack.
   a. Press the PDU toward the rack.
   b. Push the mounting buttons through the mounting holes.
   c. Let the PDU drop slightly.

Mounting 1U or 2U Models

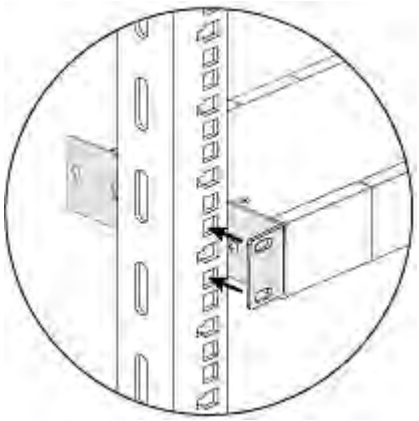
Using the appropriate brackets and tools, fasten the 1U or 2U PXC PDUs to the rack or cabinet.

To mount 1U/2U device:

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

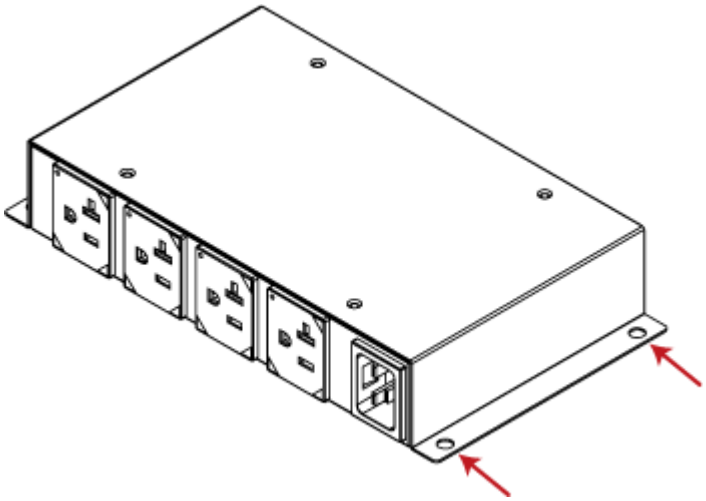


2. Attach PXC to the rack. Fasten the rackmount brackets' ears to the rack using your own fasteners.



PXO Rackmount Method

You can place PXO in any appropriate location with or without fastening it. To fasten it, simply screw up fasteners to screw holes on two sides of PXO.



Locking Outlets

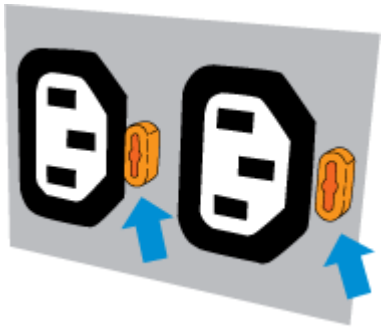
Not every PXC/PXO is implemented with locking outlets.

Locking outlets, if available on your PXC/PXO, help secure the connection of power cords from your IT equipment to PXC/PXO.

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.

Raritan
A brand of legrand

Chapter 3 Initial Installation and Configuration

This chapter explains how to install your PXC/PXO and configure it for network connectivity.

In This Chapter

Connecting the PDU to a Power Source 11
Connecting the PXC/PXO to Your Network.....12
Configuring the PXC/PXO.....14
Bulk Configuration Methods.....23
Cascading Multiple PXC/PXO Devices for Sharing Ethernet Connectivity 24

Connecting the PDU to a Power Source

1. Verify that all circuit breakers on the PXC/PXO 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 PXC/PXO to an appropriately rated branch circuit. Refer to the label or nameplate affixed to your PXC/PXO for appropriate input ratings or range of ratings.

   Note: When a PXC/PXO powers up, it proceeds with the power-on self test and software loading for a few moments.

3. When the software has completed loading, the outlet LEDs show a steady color and the front panel display illuminates. Note that outlet LEDs are only available on some PDU models.

Connecting the PXC/PXO to Your Network

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

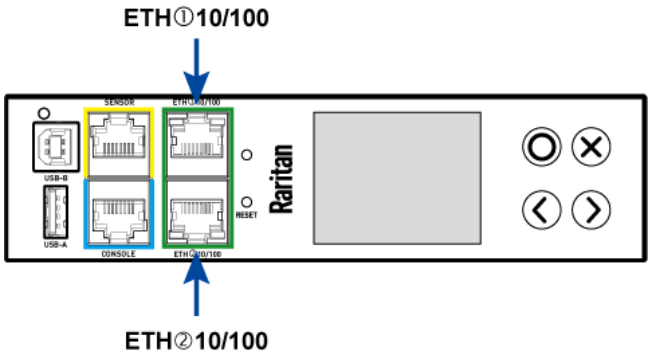
Note: If your PXC/PXO will work as a master device in the bridging mode, you must make a wired connection. See **Cascading Multiple PXC/PXO Devices for Sharing Ethernet Connectivity** *(on page 24).*

Ethernet port of PXC/PXO must be enabled for the described connection to work properly, which has been enabled per default. See ***Wired Network Settings*** (on page 191).

To make a wired connection:

1. Connect a standard network patch cable to either or both Ethernet ports on the PXC/PXO.
   - The two Ethernet ports must be connected to different subnets. See ***Dual Ethernet Connection*** (on page 14).
   - Each Ethernet port supports up to 100 Mbps.
2. Connect the other end of the cable to your LAN.

   Below illustrates the Ethernet ports on PXC 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 PXC/PXO.

- Connect a USB hub to the USB-A port on the PXC/PXO. Then plug the supported USB wireless LAN adapter into the appropriate USB port on the hub.

See ***USB Wireless LAN Adapters*** (on page 13) for a list of supported wireless LAN adapters.

USB Wireless LAN Adapters

The PXC/PXO 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 PXC/PXO matches the access point. The following is the wireless LAN configuration that the PXC/PXO supports.

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

Tip: Supported 802.11 network protocols vary according to the wireless LAN adapter being used with the PXC/PXO. See *USB Wireless LAN Adapters* **(on page 13).**

Note: You must configure PXC/PXO to enable its wireless LAN interface. See the topic titled *Configuring Network Settings* **(on page 190) in the User Guide.**

Dual Ethernet Connection

A PXC/PXO 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 57).

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 PXC/PXO master or slave device to the LAN. See **Cascading Multiple PXC/PXO Devices for Sharing Ethernet Connectivity** *(on page 24).*

Check list when connecting both ports to the networks:

- Both Ethernet interfaces are connecting to different subnets.
- Both Ethernet interfaces have been enabled. By default both are enabled. See ***Device Info*** (on page 83) and ***Ethernet Interface Settings*** (on page 194).
- Both Ethernet interfaces are configured with proper IPv4 and/or IPv6 settings. See ***Wired Network Settings*** (on page 191).
  - 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 207).

Configuring the PXC/PXO

You can initially configure the PXC/PXO via one of the following:

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

Configuration via a DHCP-enabled network:

1. Connect the PXC/PXO to a DHCP IPv4 network. See ***Connecting the PXC/PXO to Your Network*** (on page 12).
2. Retrieve the DHCP-assigned IPv4 address. Use the front panel LCD display to retrieve it. See ***Device Info*** (on page 83).
3. Launch a web browser to configure the PXC/PXO. See ***Login*** (on page 96).

Raritan
A brand of legrand

Configuration via a connected mobile device:

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

Configuration via a connected computer:

1. Connect the PXC/PXO to a computer. See ***Connecting the PXC/PXO to a Computer*** (on page 21).
2. Use the connected computer to configure the PXC/PXO via the command line or web interface.
   - Command line interface: See ***Initial Network Configuration via CLI*** (on page 694).
   - Web interface: Launch the web browser on the computer, and type the link-local IP address or *pdu.local* to access the PXC/PXO. See ***Login*** (on page 96).

     For link-local IP address retrieval, see ***Device Info*** (on page 83).

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

Connecting a Mobile Device to PXC/PXO

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

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

Requirements for using PDView:

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

Step A: Download and install PDView

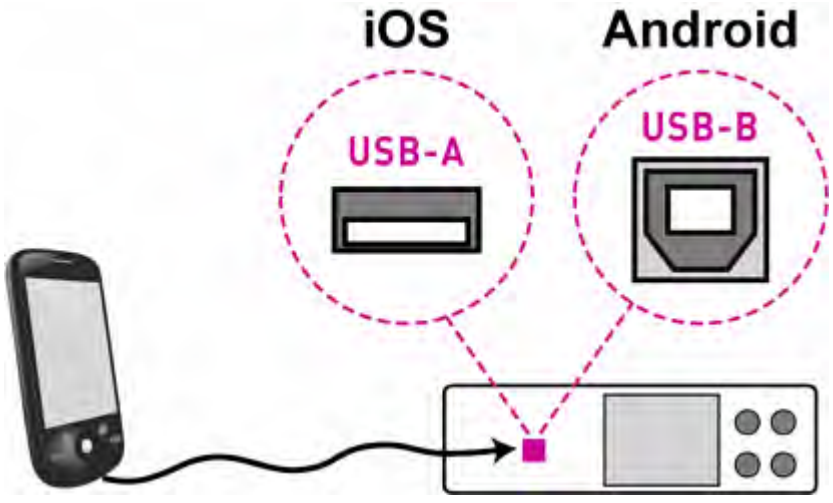
1. Visit either Apple App or Google Play Store.
   - *https://itunes.apple.com/app/raritan-pdview/id780382738*

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

2. Install PDView.

Step B: Connect the mobile device to PXC/PXO

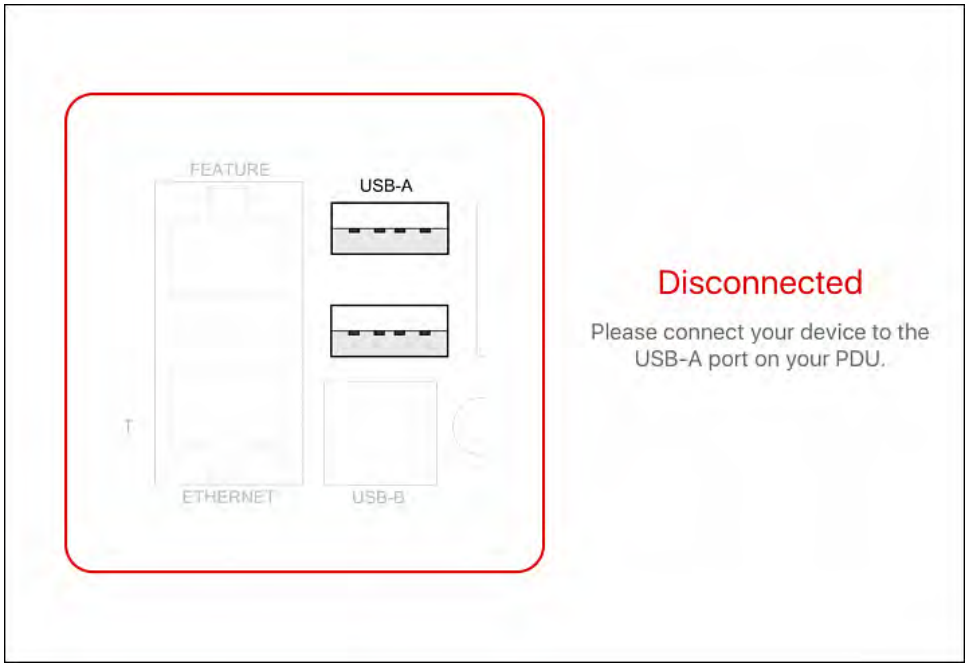
1. Get an appropriate USB cable for your mobile device.
   - *iOS*: Use the regular USB cable shipped with your iOS mobile device.
   - *Android*: Use an **USB OTG** adapter cable.
2. Connect the mobile device to the appropriate USB port on the PXC/PXO.
   - *iOS*: USB-A port.
   - *Android*: USB-B port



Step C: Launch PDView to access the PXC/PXO

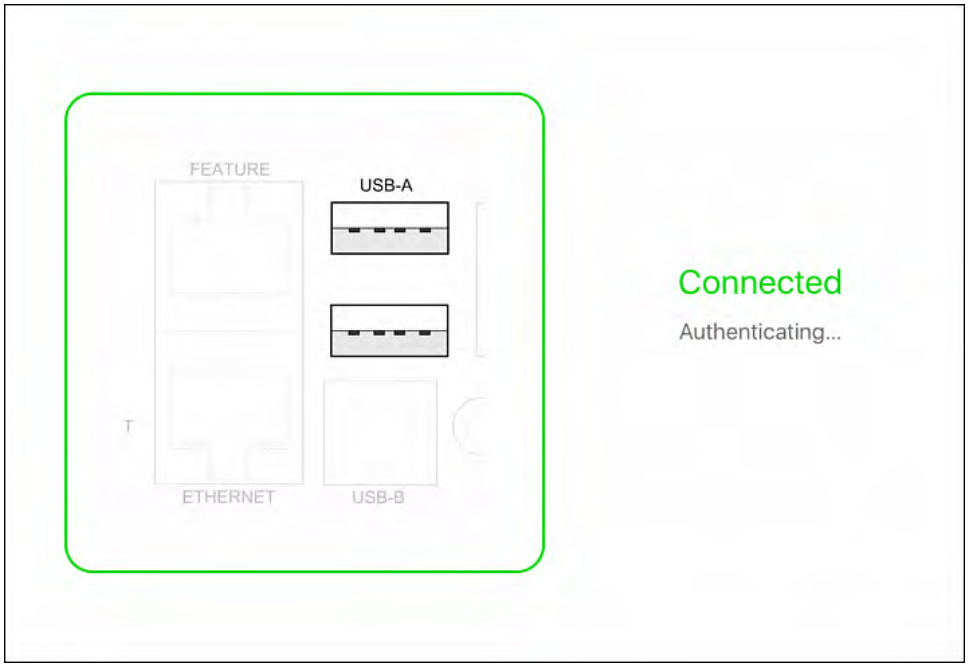
1. Launch the PDView app from your mobile device. Below illustrate iPad's PDView screens.
   a. The "Disconnected" message displays first when PDView has not detected the PXC/PXO yet.

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 PXC/PXO.



2. If the factory-default login credentials remain unchanged, or if PDView has been configured with accurate login credentials, PDView automatically logs in to the web interface of PXC/PXO.

   If PDView can't login automatically, 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 PXC/PXO.
   - 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 PXC/PXO. See **Saving User Credentials for PDView's Automatic Login** *(on page 19).*

Raritan
A brand of legrand

Saving User Credentials for PDView's Automatic Login

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

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

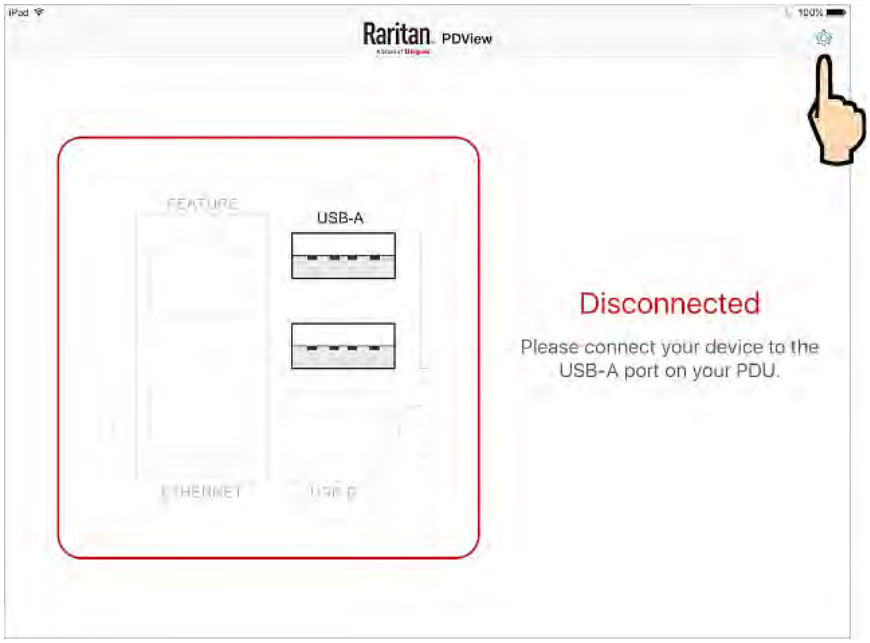
To make automatic login work again, you can save the modified admin credentials or any custom user credentials in PDView. A maximum of 5 user credentials can be saved, and PDView will try these credentials one by one until the login succeeds.

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

To save user credentials in PDView:

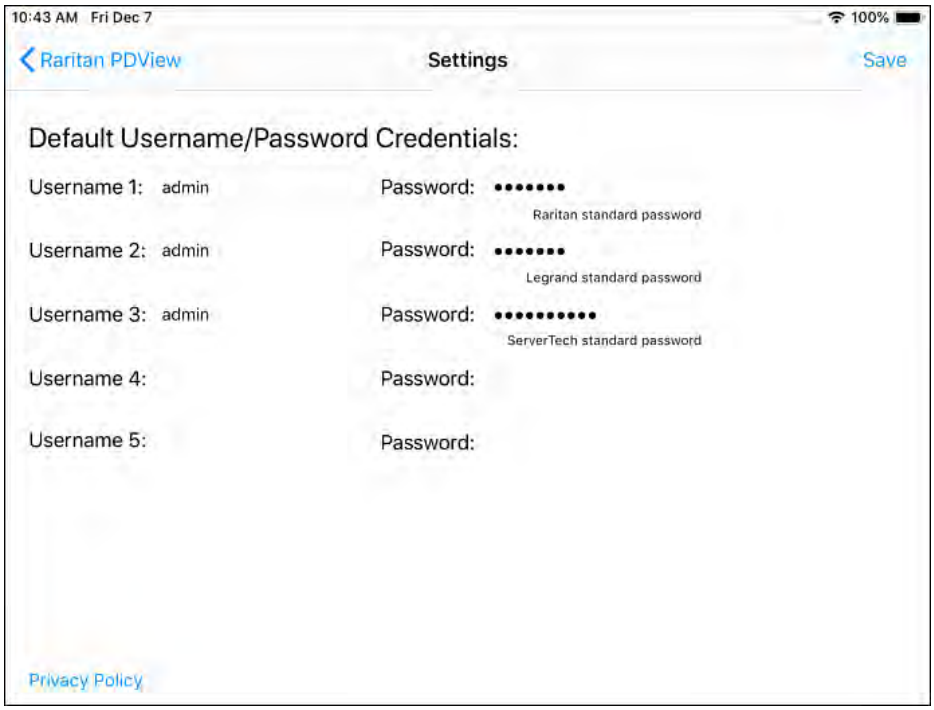
1. Make sure your mobile device is NOT connected to the PXC/PXO so that PDView does NOT perform the automatic login feature after it is launched.
2. Launch PDView on your mobile device.

3. Tap the top-right icon (iOS) or (Android).



4. The user credentials setup page opens.

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



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

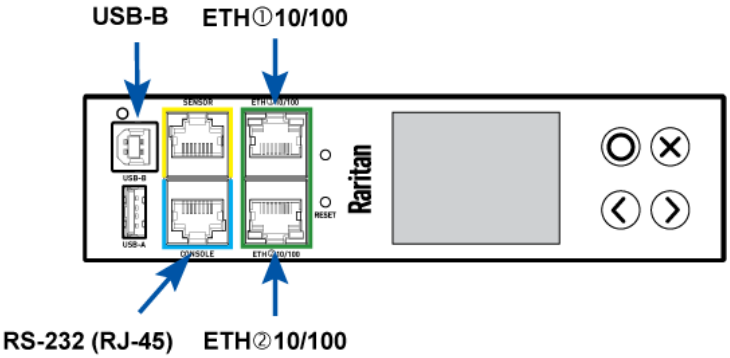
Raritan
A brand of legrand

Connecting the PXC/PXO to a Computer

The PXC/PXO 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 PXC 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 PXC/PXO 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 3).

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

Direct network connection:

1. Connect one end of a standard network patch cable to either Ethernet port of the PXC/PXO.
2. Connect the other end to a computer's Ethernet port.
3. On the connected computer, launch a web browser to access the PXC/PXO, using either link-local addressing: *pdu.local* or *169.254.x.x*. See ***Login*** (on page 96).

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 693).

2. Connect a USB cable between a computer's USB-A port and the USB-B port of PXC/PXO.
3. Perform ***Initial Network Configuration via CLI*** (on page 694).

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

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

1. Connect the RJ-45 end of the RJ45-to-DB9 adapter cable to the RJ-45 port labeled CONSOLE on PXC/PXO.
   - See ***RJ45-to-DB9 Cable Requirements for Computer Connections*** (on page 22).
2. Connect the DB9 end to your computer's RS-232 port (COM).
3. Perform ***Initial Network Configuration via CLI*** (on page 694).

RJ45-to-DB9 Cable Requirements for Computer Connections

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

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

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

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

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

Bulk Configuration Methods

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

A bulk configuration file downloaded from PXC/PXO:

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

  See ***Bulk Configuration*** (on page 343).

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 PXC/PXO devices after connecting them to the network.

  See ***Bulk Configuration or Firmware Upgrade via DHCP/TFTP*** (on page 590).

Curl command:

- *Requirement*: Two files are required -- one is a configuration file in TXT and the other is a devices list file in CSV. See ***config.txt*** (on page 582) and ***devices.csv*** (on page 585).
- *Procedure*: Upload both files to all of PXC/PXO devices one by one, using the appropriate curl command.

  See ***Upload via Curl*** (on page 616).

SCP or PSCP command:

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

  See ***Uploading or Downloading Raw Configuration Data*** (on page 564).

A USB flash drive:

- *Requirement*: A FAT32- or supperfloppy-formatted USB flash drive containing two special configuration files and one devices list file is required.
- *Procedure*: Plug this USB drive into the PXC/PXO. 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 575).

Cascading Multiple PXC/PXO Devices for Sharing Ethernet Connectivity

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

- USB interface
- Ethernet interface

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

Each device in the cascade is accessible over the network, with Bridging or Port-Forwarding cascading mode activated on the master device. See ***Setting the Cascading Mode*** (on page 207).

- **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 PXC/PXO in the chain must run compatible firmware versions, which are Xerus™ Firmware v3.6.10 or later.
- The cascading mode of all devices in the chain must be the same.
- In the Bridging mode, the master device can have "only one" connection to the network. DO NOT connect both Ethernet ports to the network(s) unless your network has the R/STP protocol enabled.

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

Raritan
A brand of legrand

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

Troubleshooting:

When a networking issue occurs, check the cascading connection and/or software settings of all devices in the chain. See ***Cascading Troubleshooting*** (on page 688).

Online Cascading Guide:

For more information on cascading configurations and restrictions, refer to the *Cascading Guide* on the Raritan ***Support page*** (***http://www.raritan.com/support/***).

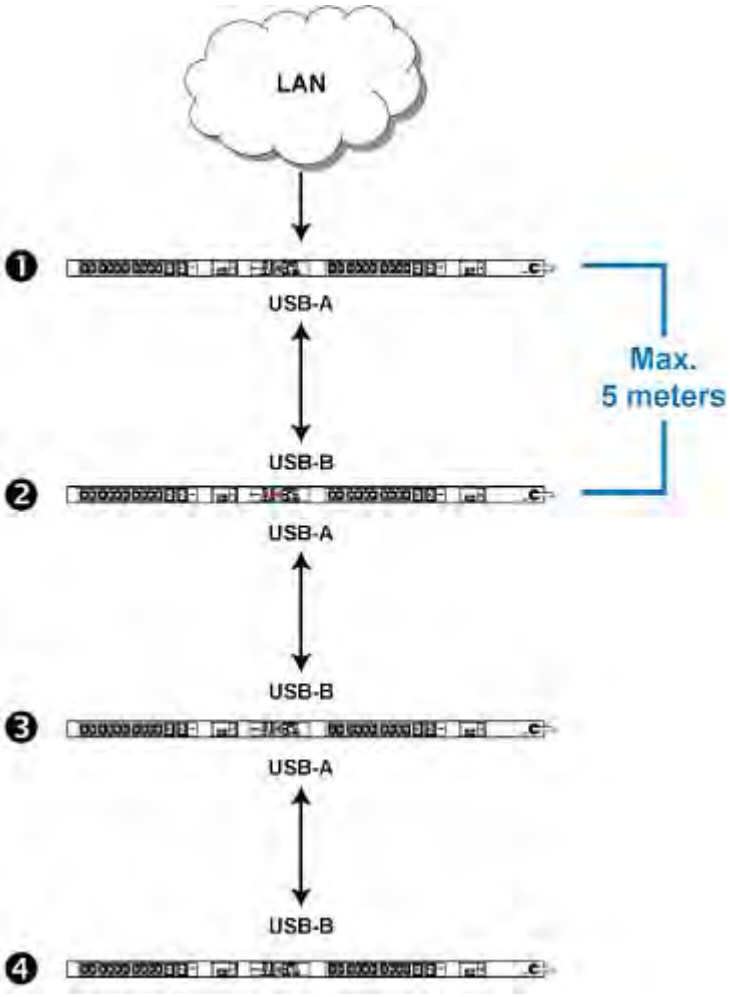
Cascading All Devices via USB

You must set the cascading mode before establishing the chain. See ***Setting the Cascading Mode*** (on page 207).

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 PXC/PXO devices cascaded via USB.



Number	Device role
❶	Master device
❷	Slave 1
❸	Slave 2
❹	Slave 3

To cascade PXC/PXO devices via USB:

- Make sure all devices are running appropriate firmware versions.

1. Choose the appropriate one as the master device.
   - When the Port Forwarding mode over "wireless LAN" is intended, the master device must be a Raritan product with two USB-A ports, such as PX3, Smart Rack Controller, EMX2-888, PX3TS or BCM2.
2. 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 207).
3. 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 13).
4. Connect the USB-A port of the master device to the USB-B port of an additional PXC/PXO via a USB cable. This additional device is Slave 1.
5. Connect Slave 1's USB-A port to the USB-B port of an additional PXC/PXO via another USB cable. The second additional device is Slave 2.
6. Repeat the same step to connect more slave devices. You can cascade up to 15 slave devices.
7. (Optional) Configure or change the network settings of the master and/or slave devices as needed. See ***Configuring Network Settings*** (on page 190).
   - **Bridging mode**: Each cascaded device has its own network settings.

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

A tip for USB cascading:

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

Extended Cascading with PXC/PXO Devices

You can use either Ethernet port on the PXC/PXO PDU for cascading.

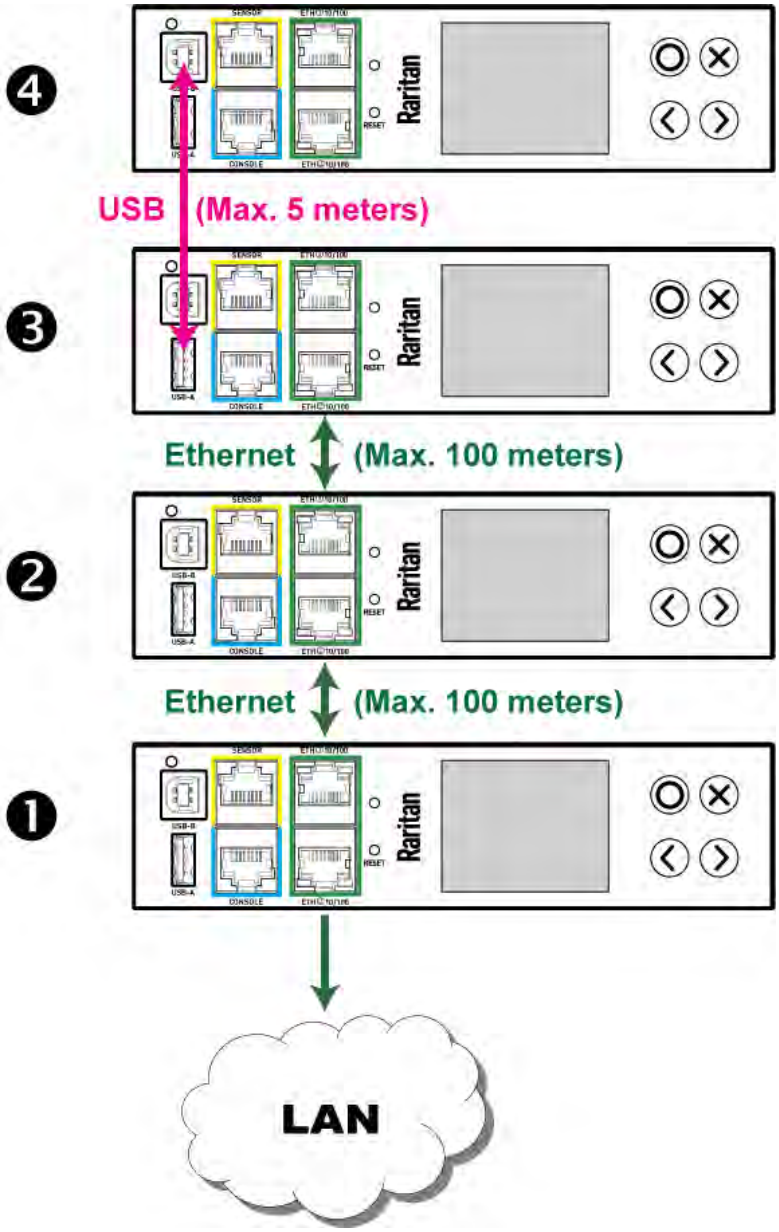
You must set the cascading mode before establishing the chain. See ***Setting the Cascading Mode*** (on page 207).

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 31).

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

The distance between two Ethernet-cascaded devices can be up to 100 meters, while the distance between two USB-cascaded devices supports up to 5 meters only.



Number	Device role
❶	Master device
❷	Slave 1
❸	Slave 2
❹	Slave 3

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 26).*

To cascade PXC/PXO devices via Ethernet ports:

- Make sure all devices are running appropriate firmware versions.

1. Choose one PXC/PXO as the master device.
2. 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 207).
3. 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 13).
4. Connect the available Ethernet port of the master device to either Ethernet port of another PXC/PXO via a standard network patch cable. This additional PXC/PXO device is Slave 1.
5. Connect Slave 1's available Ethernet port to either Ethernet port of another PXC/PXO via a standard network patch cable. The second additional device is Slave 2.
6. Repeat the same step to connect more PXC/PXO PDUs. You can cascade up to 15 slave devices.
7. (Optional) Configure or change the network settings of the master and/or slave devices as needed. See ***Configuring Network Settings*** (on page 190).
   - **Bridging mode**: Each cascaded device has its own network settings.

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

Recommendations for cascade loops:

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

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

   AND

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

A tip for extended cascading:

- The "extended cascading" chain can be a combination of diverse Raritan products that support the extended-cascading feature, including PX3, Smart Rack Controller, transfer switch, PXC and PXO.
- You can also cascade PXC/PXO devices with Legrand PDUs via Ethernet ports.

Restrictions of Port-Forwarding Connections

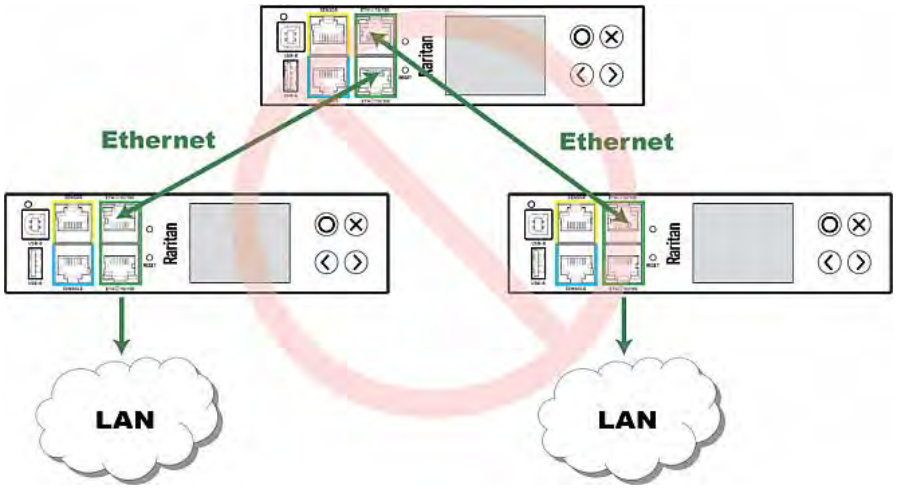
The following guidelines must be obeyed for establishing a cascading chain in the **Port Forwarding** mode.

- 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.

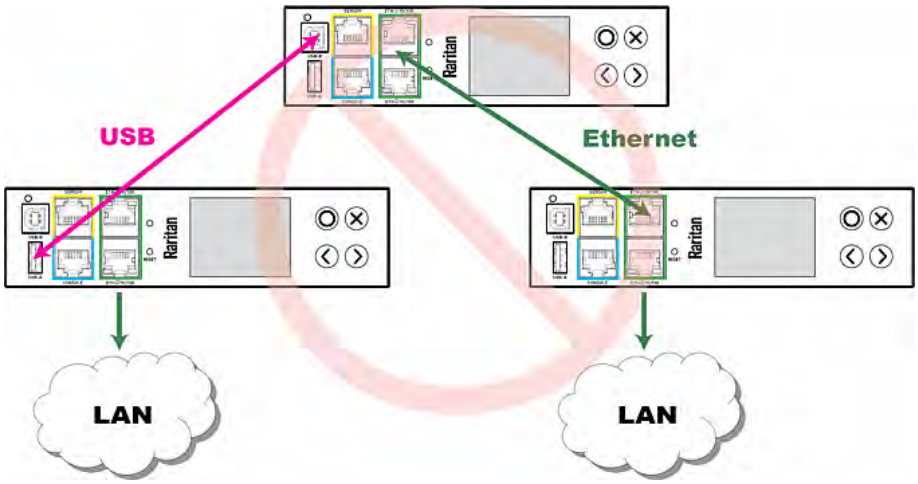
The following diagrams illustrate cascading connections that are NOT supported.

UNSUPPORTED connections:

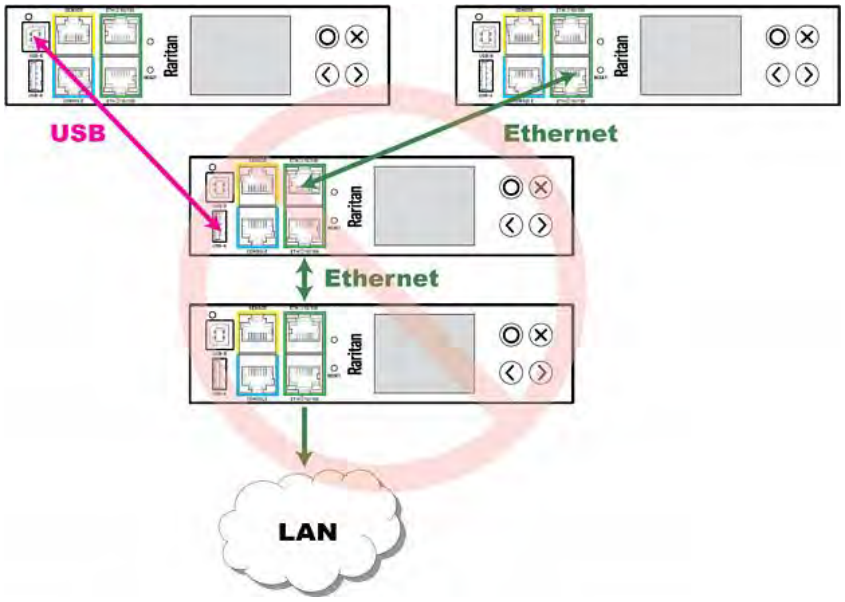
- One cascaded device has two upstream devices via Ethernet cables.



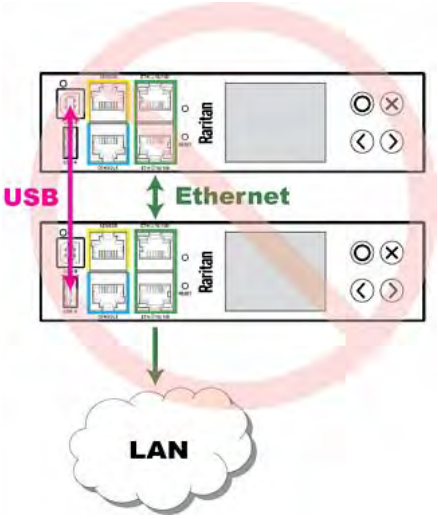
- One cascaded device has two upstream devices via Ethernet and USB cables.



- One cascaded device has two downstream devices.



- One device is connected to another device via two cascading cables - USB and Ethernet cables.



Chapter 4 Connecting External Equipment (Optional)

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

In This Chapter

Connecting Raritan Environmental Sensor Packages 34
Connecting a Logitech Webcam 54
Connecting a Modbus RTU Device or Bus.....54

Connecting Raritan Environmental Sensor Packages

PXC/PXO supports all types of Raritan environmental sensor packages, including DPX, DPX2, DPX3, DX and DX2 sensor packages. DPX series is the first generation while DX2 series is the latest generation.

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.

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

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

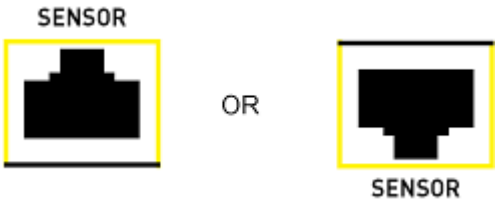
- ***DX2 Sensor Packages*** (on page 35)
- ***DX Sensor Packages*** (on page 38)
- ***DPX3 Sensor Packages*** (on page 39)
- ***DPX2 Sensor Packages*** (on page 40)
- ***DPX Sensor Packages*** (on page 43)

Identifying the Sensor Port

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

How to identify the SENSOR port:

- The correct port is labeled SENSOR.
- The SENSOR port is marked with YELLOW color, as shown below.



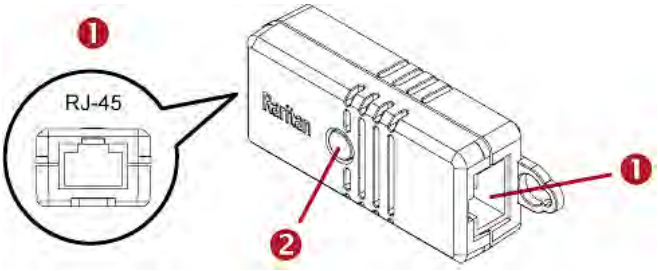
DX2 Sensor Packages

You can cascade up to 12 DX2 sensor packages.

When cascading DX2, remember that the PXC/PXO 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 PXC/PXO.

Tip: To manage the last several sensors/actuators after 32nd function, you can release some "managed" sensors or actuators, and then manually bring the last several sensors/actuators into management. See **Peripherals** *(on page 154).*



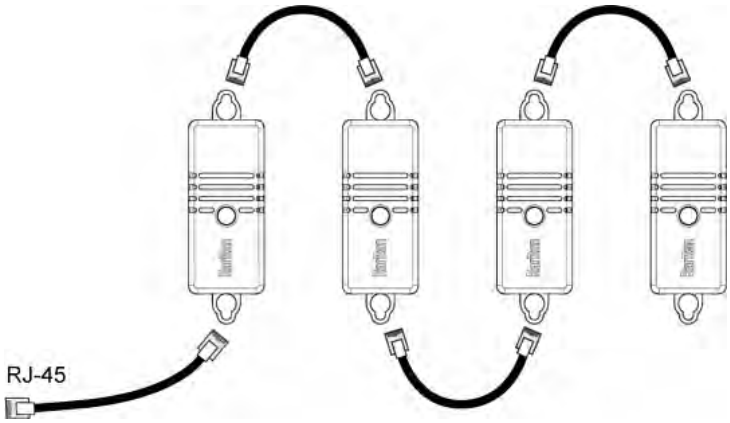
Numbers	Components
1	RJ-45 ports, each of which is located on either end of a DX2 sensor package.
2	LED, which indicates the sensor package's status

Connect DX2 to the PXC/PXO:

1. Connect a standard network patch cable (CAT5e or higher) to either RJ-45 port on a DX2 sensor package.
2. If you want to cascade DX2 packages, get an additional standard network patch cable (CAT5e or higher) and then:
   a. Plug one end of the cable into the remaining RJ-45 port on the prior DX2 package.
   b. Plug the other end into either RJ-45 port on an additional DX2 package.

   Repeat the same steps to cascade more DX2 packages.

Exception: You CANNOT cascade DX2-DH2C2 packages. A PXC/PXO supports only one DX2-DH2C2.



3. Connect the first DX2 sensor package to the PXC/PXO by plugging its cable's connector into the RJ-45 SENSOR port of the PXC/PXO.
4. If needed, connect a DPX2 sensor package to the end of the DX2 chain. See ***Connecting a DPX2 Sensor Package to DX2, DX or DPX3*** (on page 42).

Using an Optional Sensor Hub

A Raritan DX2-ENVHUB4 sensor hub increases the number of sensor ports for the PXC/PXO.

DX2-ENVHUB4:

See ***Connecting a DX2-ENVHUB4 Sensor Hub*** (on page 37) for connections.

- Supports Raritan's DX2 series sensors
- Does not support DX2-DH2C2. No door handle support.
- Max cable: 2 meter Cat5 STP
- Powered by the Sensor port of the connected device.
- Supported by the following Raritan, Legrand, and ServerTech products:
  - PX3 PDUs with iX7 controller (or newer)

  - PXC
  - PXO
  - BCM2
  - SRC
  - PRO3X PDUs
  - Legrand PDU (limited models)
- Connects to SENSOR port only.
- Sensors may cascade from hubs, but hubs themselves cannot be cascaded.

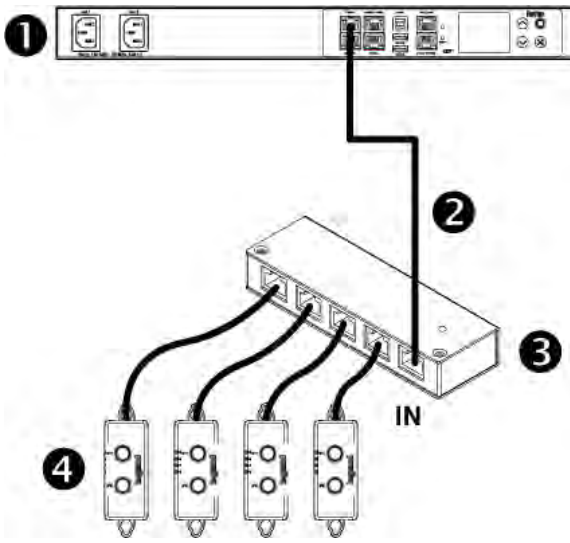
Connecting a DX2-ENVHUB4 Sensor Hub

To connect Raritan sensor packages via the DX2-ENVHUB4 hub:

1. Connect the sensor hub to the PXC/PXO using a standard network patch cable (CAT5e or higher), on the following ports:
   - IN port (Port 1) of the hub
   - RJ-45 SENSOR port of the PXC/PXO
2. Connect the Raritan sensor packages to any of the four OUT ports on the hub.

   This diagram illustrates a configuration with a sensor hub connected.

1	A supported Raritan or Legrand device, see ***Using an Optional Sensor Hub*** (on page 36)
2	A standard network cable
3	DX2-ENVHUB4 sensor hub
4	DX2 series Raritan sensor packages



DX Sensor Packages

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

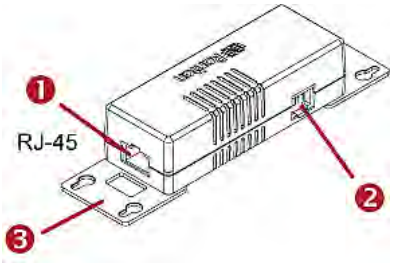
You can cascade up to 12 DX sensor packages.

When cascading DX, remember that the PXC/PXO 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 PXC/PXO.

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

Tip: To manage the last several sensors/actuators after 32nd function, you can release some "managed" sensors or actuators, and then manually bring the last several sensors/actuators into management. See **Peripherals** *(on page 154).*



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

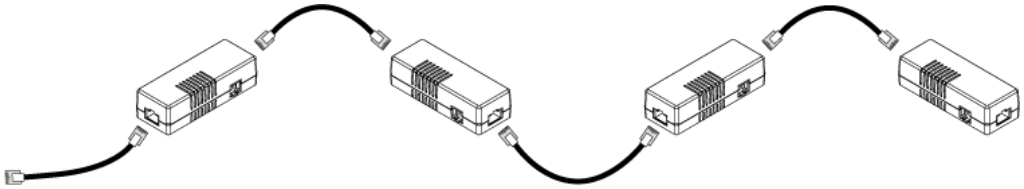
Connect DX to the PXC/PXO:

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.

Raritan
A brand of legrand

Exception: You CANNOT cascade DX-PD2C5 sensor packages. One PXC/PXO supports only one DX-PD2C5.

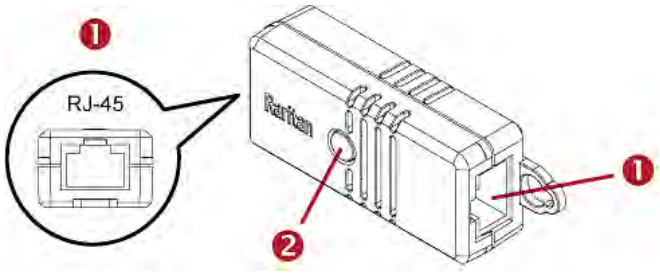


3. Connect the first DX sensor package to the PXC/PXO by plugging its cable's connector into the RJ-45 SENSOR port of the PXC/PXO.
4. If needed, connect a DPX2 sensor package to the end of the DX chain. See ***Connecting a DPX2 Sensor Package to DX2, DX or DPX3*** (on page 42).

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.

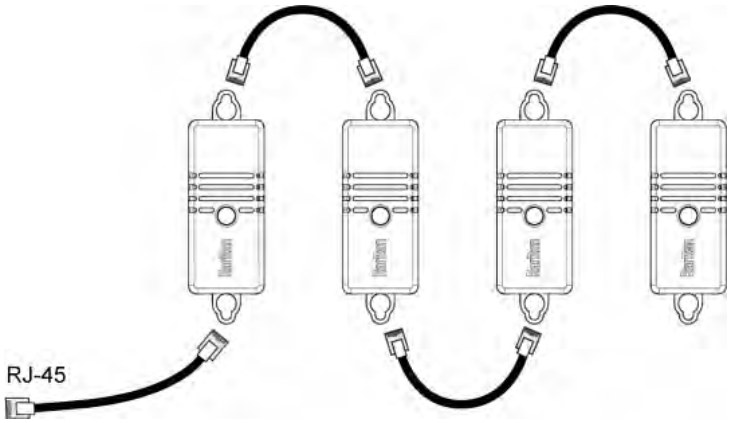


Numbers	Components
1	RJ-45 ports, each of which is located on either end of a DPX3 sensor package.
2	LED for indicating the sensor status.

To connect DPX3 to the PXC/PXO:

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.

Repeat the same steps to cascade more DPX3 sensor packages.

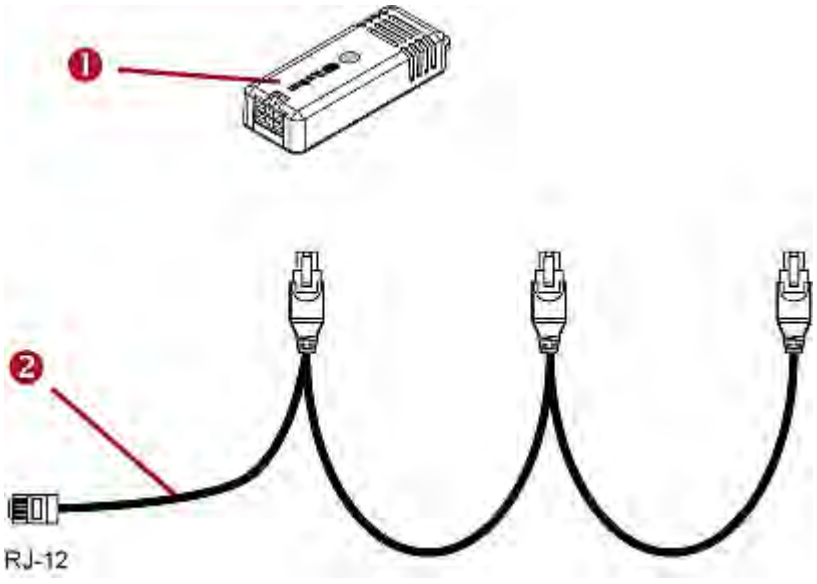


3. Connect the first DPX3 sensor package to the PXC/PXO by plugging its cable's connector into the RJ-45 SENSOR port of the PXC/PXO.
4. If needed, connect a DPX2 sensor package to the end of the DPX3 chain. See ***Connecting a DPX2 Sensor Package to DX2, DX or DPX3*** (on page 42).

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/***).



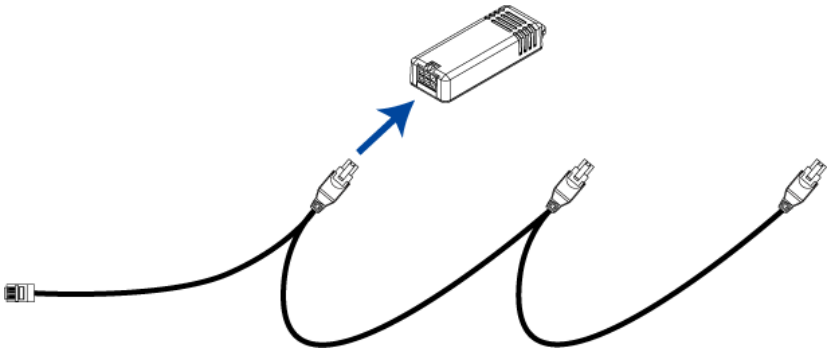
Item	
❶	DPX2 sensor package
❷	DPX2 sensor cable with one RJ-12 connector and three head connectors

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

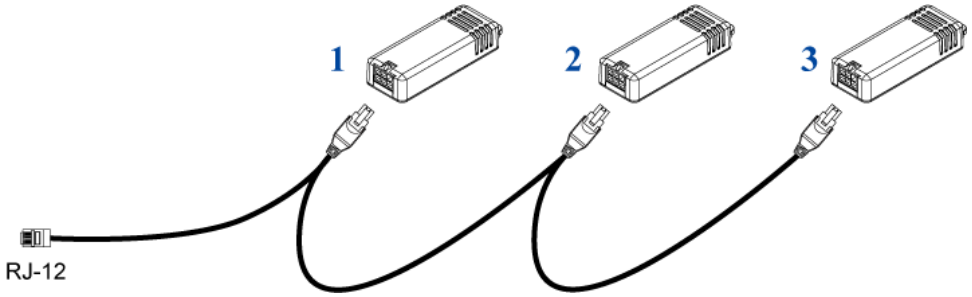
Warning: If there are free head connectors between a DPX2 sensor cable's RJ-12 connector and the final attached DPX2 sensor package, the sensor packages following the free head connector(s) on the same cable do NOT work properly. Therefore, always occupy all head connectors prior to the final sensor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

To connect DPX2 to the PXC/PXO:

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 PXC/PXO.
   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 PXC/PXO.

   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 DX2, DX or DPX3*** (on page 42).

Connecting a DPX2 Sensor Package to DX2, DX or DPX3

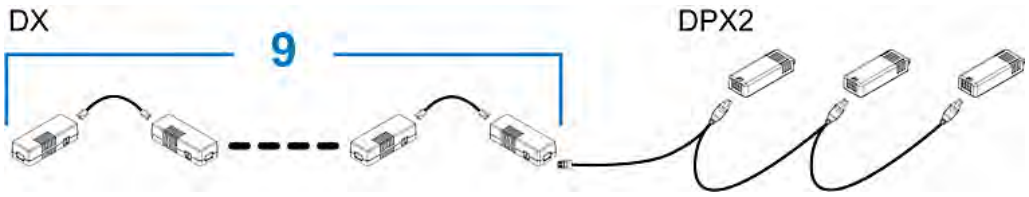
You can connect one DPX2 sensor package to the "end" of a DX2, DX or DPX3 sensor chain. It is strongly recommended to use an RJ-12 to RJ-45 adapter for connecting DPX2 to the final DX2, DX or DPX3 in the chain.

The maximum number of DX2, DX or DPX3 sensor packages in the chain must be less than 12 when a DPX2 sensor package is involved.

The following diagrams illustrate DX sensor chain only, but the same principles also apply to DX2 and DPX3 sensor chains if connecting DPX2 to the end of DX2 or DPX3 sensor chains.

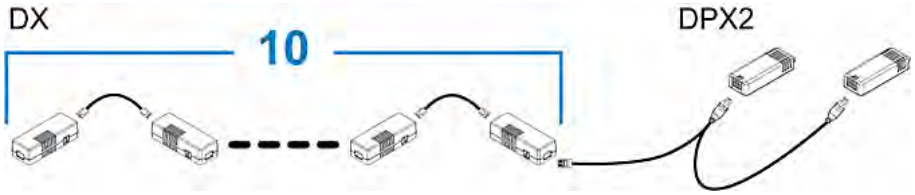
- **When connecting a DPX2 sensor package containing "three" DPX2 sensors:**

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



- **When connecting a DPX2 sensor package containing "two" DPX2 sensors:**

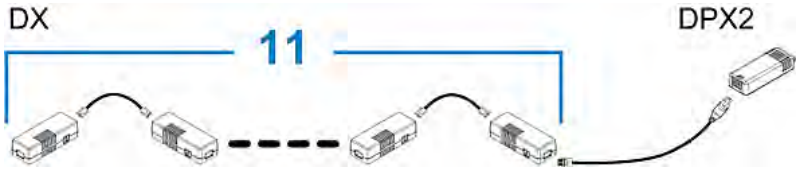
  A maximum of ten DX sensor packages can be cascaded because 12-2=10.



Raritan
A brand of legrand

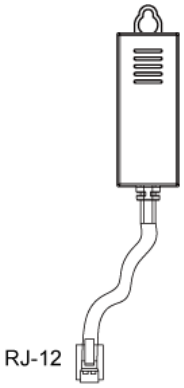
When connecting a DPX2 sensor package containing "one" DPX2 sensor:

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



DPX Sensor Packages

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



For the cabling length restrictions, see ***Supported Maximum DPX Sensor Distances*** (on page 47).

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:

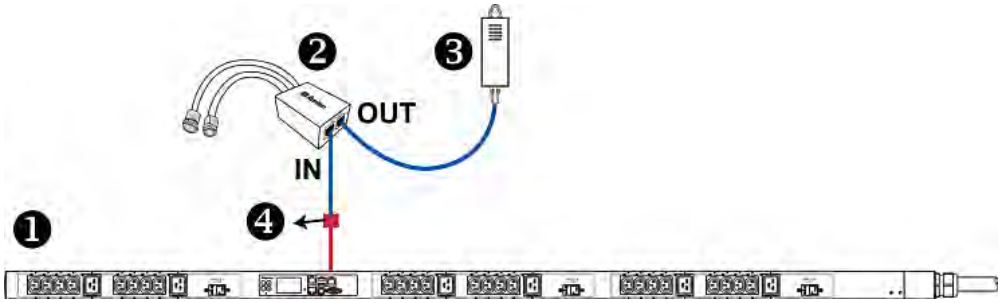
An RJ-12 to RJ-45 adapter is required to connect a DPX sensor package to PXC/PXO.

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 PXC/PXO.

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 PXC/PXO.
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.



1	The PXC/PXO
2	Raritan differential air pressure sensors
3	One DPX sensor package (optional)
4	RJ-12 to RJ-45 adapter

Using an Optional DPX-ENVHUB4 Sensor Hub

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

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

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

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 48).*

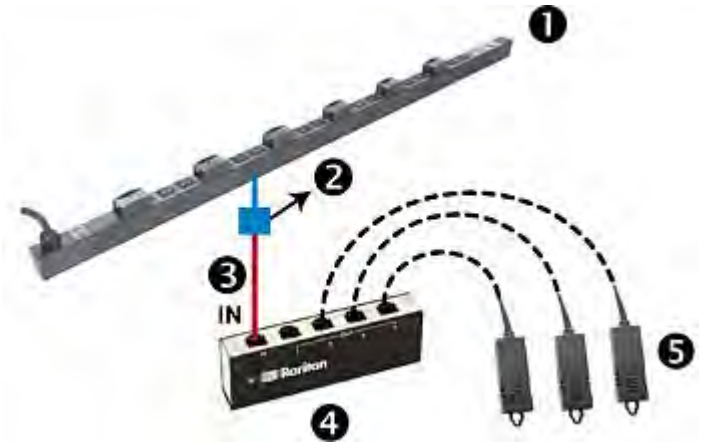
To connect DPX sensor packages via the DPX-ENVHUB4 hub:

1. Connect the DPX-ENVHUB4 sensor hub to the PXC/PXO.
   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.



1	PXC/PXO
2	RJ-12 to RJ-45 adapter
3	Raritan-provided phone cable
4	DPX-ENVHUB4 sensor hub
5	DPX sensor packages

Using an Optional DPX-ENVHUB2 cable

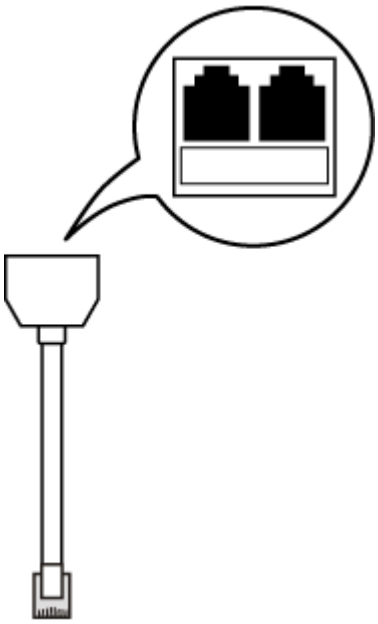
A Raritan *DPX-ENVHUB2* cable doubles the number of connected environmental sensors per SENSOR port.

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 PXC/PXO.
   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 PXC/PXO.

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 PXC/PXO.

Raritan
A brand of legrand

Supported Maximum DPX Sensor Distances

When connecting the following DPX sensor packages to the PXC/PXO, you must follow two restrictions.

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

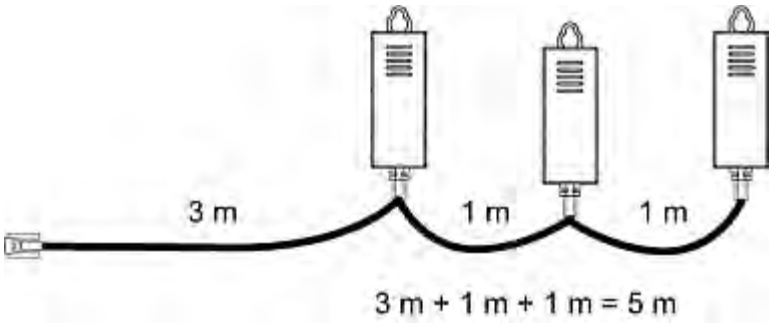
Sensor connection restrictions:

- Connect a DPX sensor package to the PXC/PXO 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 PXC/PXO 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 PXC/PXO via a sensor hub.

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



- The total cabling length between the PXC/PXO and one DPX-T3H1 is 49' (15 m) as illustrated below.

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

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

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 PXC/PXO, except for the following differences:

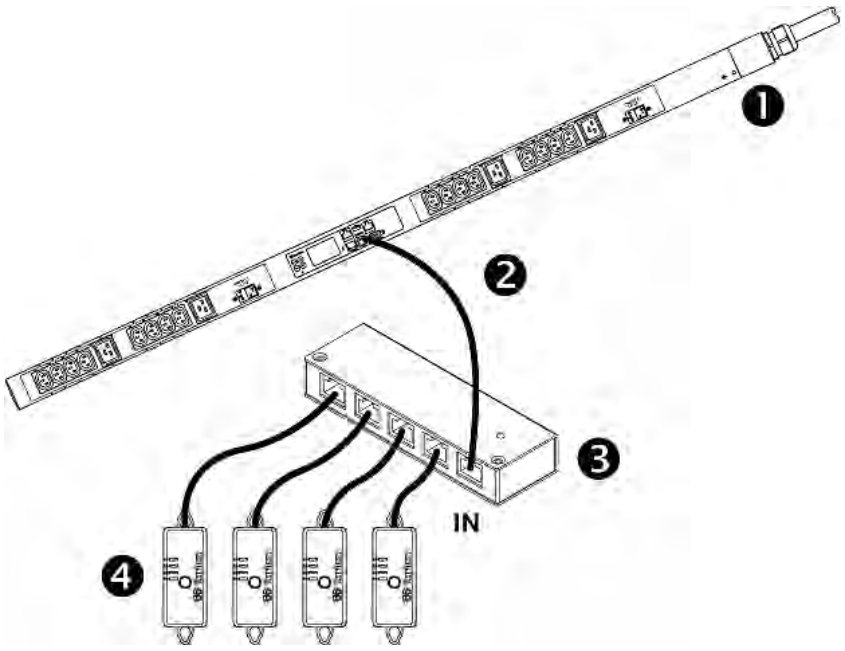
- All ports on the DPX3-ENVHUB4 sensor hub are RJ-45 instead of RJ-12 as the DPX-ENVHUB4 sensor hub.
- The DPX3-ENVHUB4 sensor hub supports all Raritan environmental sensor packages, including DPX, DPX2, DPX3, DX and DX2 sensor packages.

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 49).

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

1. Connect the DPX3-ENVHUB4 sensor hub to the PXC/PXO 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 PXC/PXO.
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	PXC/PXO
❷	A standard network cable
❸	DPX3-ENVHUB4 sensor hub
❹	Any Raritan sensor packages

Mixing Diverse Sensor Types

You can mix diverse sensor packages on one PXC/PXO according to the following sensor combination principles. In some scenarios, the DPX3-ENVHUB4 sensor hub is required.

When mixing different sensor types, remember that the PXC/PXO only supports a maximum of 32 sensors/actuators.

PXC/PXO does NOT support any other sensor-mixing combinations than those described in this section.

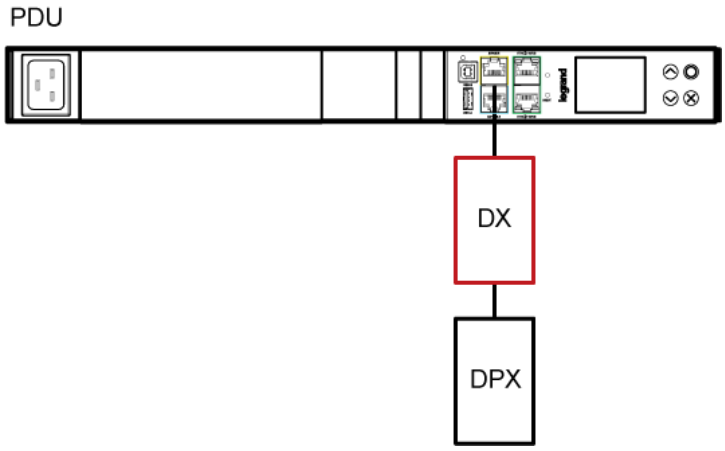
In most illustrations below, any DX or DPX3 sensor package can be replaced with a DX2 sensor package.

For those illustrations where DX, DPX3 and DX2 are interchangeable, they are all marked with the following oval image.

Important: Unlike DX or DPX3 series, DX2 CANNOT be connected with DPX sensor package(s).

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.



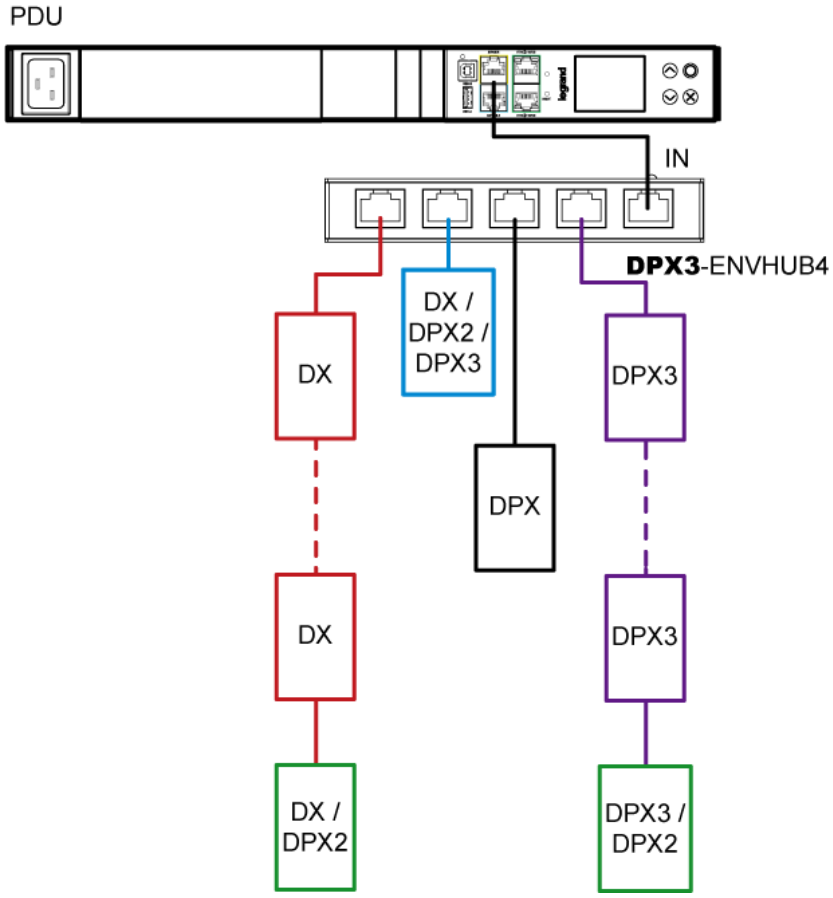
Diverse combinations via the DPX3-ENVHUB4 sensor hub:

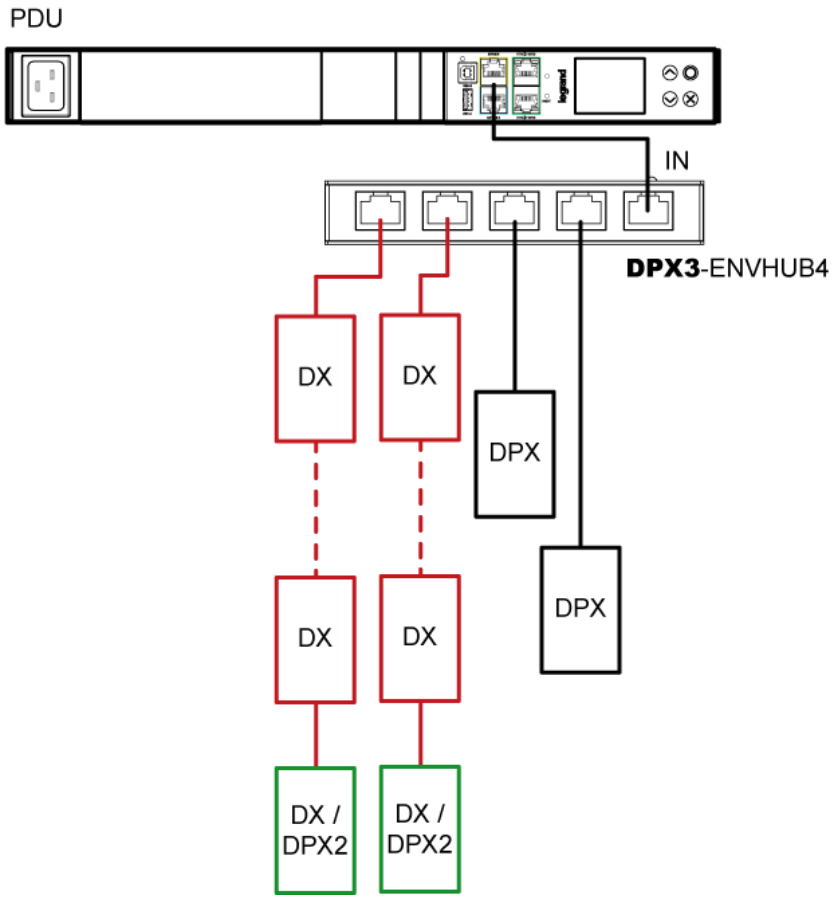
- You must use the **DPX3**-ENVHUB4 sensor hub instead of the old DPX-ENVHUB4 sensor hub. Each port on the hub supports any of the following:
  - One individual DX2 sensor package
  - A chain of DX2 sensor packages
  - One individual DX sensor package
  - A chain of DX sensor packages
  - One individual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

Raritan
A brand of legrand

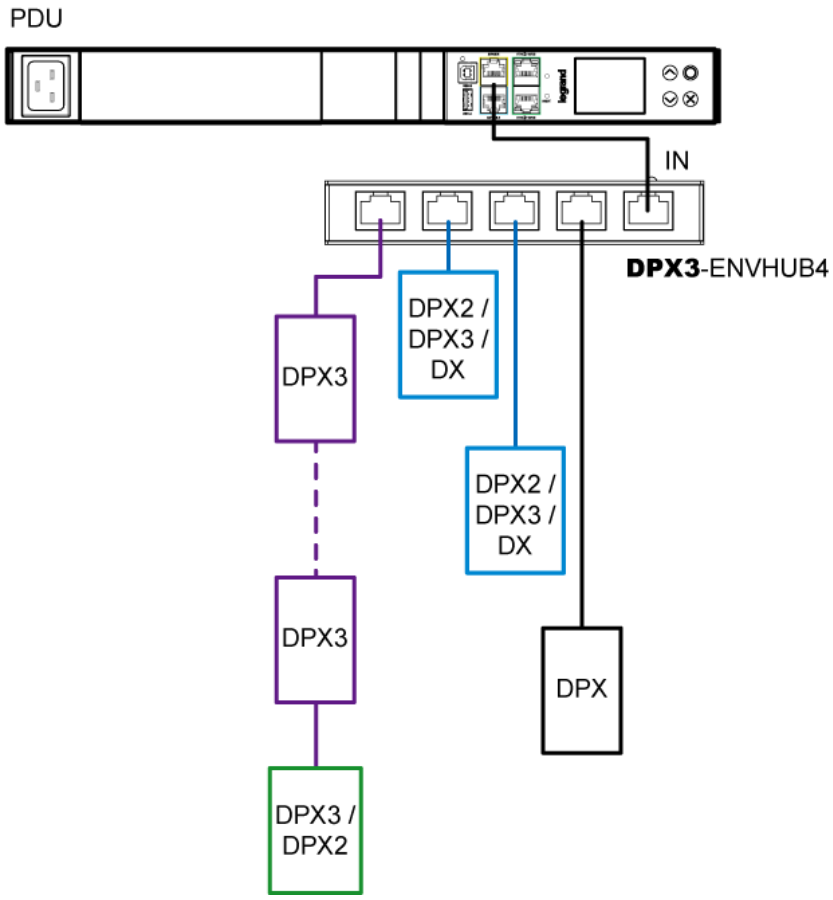
- An RJ-12 to RJ-45 adapter is recommended to connect a DPX or DPX2 sensor package to DPX3-ENVHUB4.
- In the following diagrams, the sensor package in "green" can be replaced by a DPX2 sensor package. The sensor package in "blue" can be one DPX2, DPX3, DX or DX2 sensor package.

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





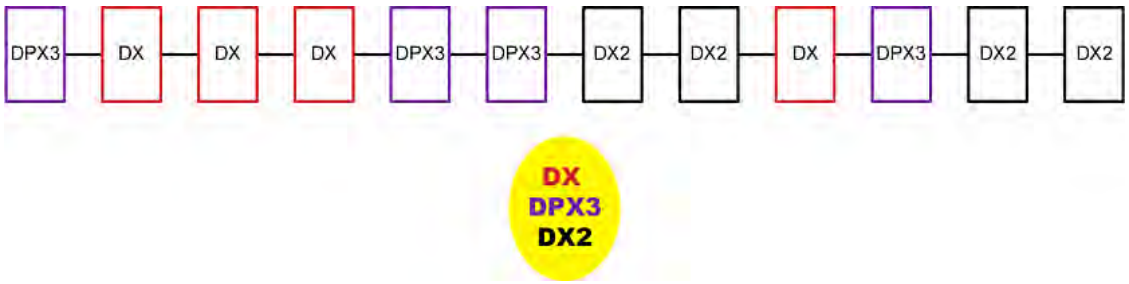
Raritan
A brand of legrand



Mix DX2, DX and DPX3 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 DX2, DX and DPX3 sensor packages.



You can add a DPX2 sensor package to the end of such a sensor-mixing chain if needed. See ***Connecting a DPX2 Sensor Package to DX2, DX or DPX3*** (on page 42).

Connecting a Logitech Webcam

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

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

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

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

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

The PXC/PXO 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 PXC/PXO 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 PXC/PXO. The PXC/PXO 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 PXC/PXO web interface after the connection is complete. See ***Configuring Webcams and Viewing Live Images*** (on page 358).

Connecting a Modbus RTU Device or Bus

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

To use the Modbus Gateway feature:

1. Connect a Modbus RTU device, or a Modbus bus with multiple RTU devices, to the PXC/PXO via two adapters described below.
   a. Connect an isolated RS485-to-RS232 adapter to the Modbus RTU device or Modbus bus.

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

c. Connect the RS232-to-USB adapter to the USB-A port on the PXC/PXO.

2. On the PXC/PXO, enable and properly configure the Modbus Gateway feature. See ***Changing Modbus Settings*** (on page 223).

Communications between Modbus TCP and RTU devices:

- The PXC/PXO acts only as a message gateway for the Modbus TCP client.

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

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

  If the Modbus TCP client does not support unit identifier addressing, refer to ***Changing Modbus Settings*** (on page 223).

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

Chapter 5 Introduction to PDU Components

This chapter explains how to use the PXC/PXO, 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 56
Circuit Breakers 94

Panel Components

PXC/PXO 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 PXC/PXO to an appropriately rated branch circuit. Refer to the label or nameplate affixed to your PXC/PXO for appropriate input ratings or range of ratings.

There is no power switch on the PXC/PXO. 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.

Raritan 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.

LED state	Outlet status	What it means
		OR the outlet's associated circuit breaker has tripped.
Red	ON and LIVE	LIVE power. The outlet is on and power is available.
	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 Raritan Technical Service for RMA service.

Raritan Metered PDU

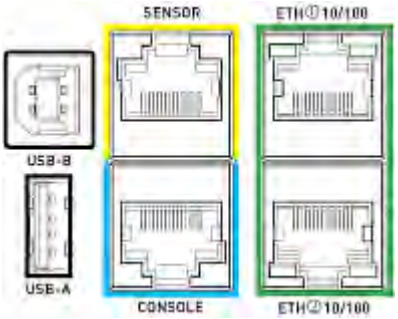
These models are NOT outlet-switching capable so all outlets are always in the ON state.

Outlet LEDs are not available.

Connection Port Functions

A PXC/PXO has 6 ports.

6 front panel ports:



- 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)

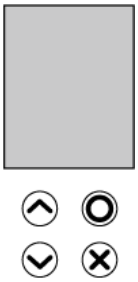
Port functions:

The table below explains the function of each port.

Port	Used for...
USB-B	• Cascading PXC/PXO devices for sharing a network connection. See ***Cascading All Devices via USB*** (on page 26). • Establishing a USB connection between a computer and the PXC/PXO for: ▪ Using the command line interface. ▪ Performing the disaster recovery. Contact Raritan Technical Support for instructions. • Connecting to an Android mobile device for viewing or configuring the PXC/PXO. See ***Connecting a Mobile Device to PXC/PXO*** (on page 15).
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 PXC/PXO. See ***Connecting a Mobile Device to PXC/PXO*** (on page 15). • Connecting a USB device, such as a Logitech® webcam or wireless LAN adapter. • Cascading PXC/PXO devices for sharing a network connection.
CONSOLE **(RJ-45)**	Establishing a serial connection between the PXC/PXO 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 22).
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	PXC/PXO has two Ethernet ports, supporting up to 100 Mbps. Connecting the PXC/PXO to your company's network via a standard network patch cable (Cat5e/6). This connection is necessary to administer or access the PXC/PXO 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 PXC/PXO Devices*** (on page 28). *Note: Network connection to this port is not required if wireless connection is preferred, or if the PXC/PXO is a slave device in the cascading configuration.*

Front Panel Display

The following diagram shows the dot-matrix LCD display panel on PXC Zero U models.



You can use the LCD display to view the 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.

If the orientation of your Zero U model's LCD content does not meet your need, you can manually change it and stick to the orientation. See ***Manually Changing PXC's Zero U LCD Orientation*** (on page 88).

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 PXC/PXO, the front panel LCD display first shows some dots, then Raritan logo and finally enters the automatic mode.

Automatic mode without alerts available:

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

If overcurrent protectors are available on your PXC/PXO, the display cycles between both the inlet and overcurrent protector information.

Note: You can make a PXC/PXO with overcurrent protectors show the inlet information only in the automatic mode. See **Front Panel Settings** *(on page 323).*

Manual mode:

To view more information or control outlets if your PXC/PXO 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 63).

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

When an alert exists:

- In the automatic mode, when an alert occurs, the LCD display stops cycling through information, and warns you by showing the alerts notice in a yellow or red background. See ***Alerts Notice in a Yellow or Red Screen*** (on page 89).

  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 62).

Raritan
A brand of legrand

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 PXC/PXO, built-in components, or connected peripheral devices
- Control actuators if any
- Control outlets if your model supports outlet-switching

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 160).

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

Raritan
A brand of legrand

Main Menu

The Main Menu contains 5 to 8 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.

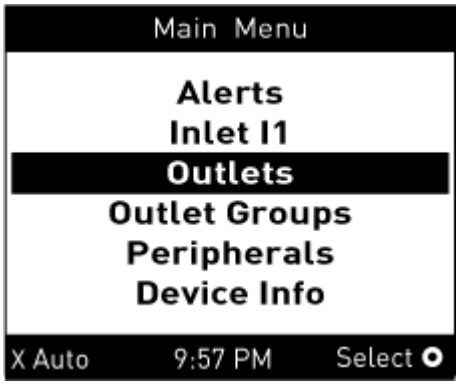
PXC LCD Main Menu (Zero U):

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 62).

Menu command	Function
Alerts	Indicates all alerted sensors, if any. See ***Alerts*** (on page 65).
PDU	Shows the PXC energy pulse output settings. If your PDU has multiple inlets, this menu item also shows the total active power and total active energy. See ***PDU*** (on page 67).
Inlet I1	Shows the inlet I1's information. See ***Inlet*** (on page 68).
OCPs	Shows a list of overcurrent protector information. See ***OCPs*** (on page 70). Only the models with overcurrent protectors have this menu item.
Outlets	This menu command is available on Switched PDUs only. Shows each outlet's information. If your PDU supports outlet-switching, you can turn on, off or power cycle an outlet. See ***Outlets*** (on page 71).
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 79).
Device Info	Shows the device information, such as IP and MAC address. See ***Device Info*** (on page 83).

Note: To return to the automatic mode, press ⊗*. See* **Automatic and Manual Modes** *(on page 60).*

PXO LCD Main Menu:



Raritan
A brand of legrand

Alerts

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

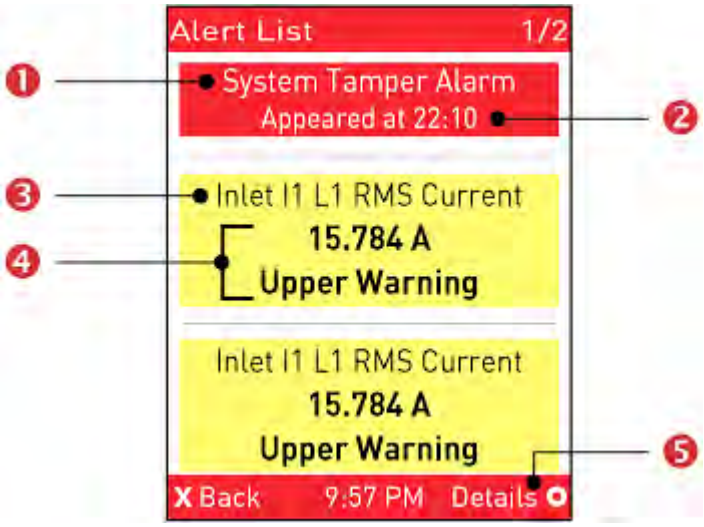
- Any numeric sensor that enters the warning or critical range if the thresholds have been enabled
- State sensors that enter the alarmed state
- Any tripped circuit breakers or blown fuses

Tip: The same information is available in the web interface's Dashboard. See **Dashboard - Alerted Sensors** *(on page 112).*

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 160).
   - 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 62).



Number	Description
❶	Alarm names.

Number	Description
❷	The time the alarm occurred. If the alarm occurred at least two times, then more information is shown. ▪ Number of alarms ▪ The first occurrence time ▪ The last occurrence time
❸	Alerted sensor names.
❹	Sensor readings and/or states. A numeric sensor shows both the reading and state. A state sensor or actuator shows the state only. Available states are listed below. For further information, see ***Sensor/Actuator States*** (on page 163). ▪ Alarmed ▪ Lower Critical = below lower critical ▪ Lower Warning = below lower warning ▪ Upper Warning = above upper warning ▪ Upper Critical = above upper critical ▪ Open (only available for Raritan PDUs with overcurrent protectors)
❺	The 'Details' command appears for alarms only. ▪ If your Alert List comprises alerted sensors only, then 'Details' is not shown.

3. Press or to view additional pages. When there are multiple pages, page numbers appear in the top-right corner of the display.
4. (Optional) If there are alarms in the Alert List, you can perform the following operations.

Raritan
A brand of legrand

a. Press to view detailed information of the alarm.

b. (Optional) If the alarm occurred more than one time, the numbers of current page and total pages are shown in the top-right corner, similar to the above diagram. Press or to view the information of other occurrences.

c. To acknowledge all alarms now, press .

PDU

The following front panel 'PDU' operation applies to PXC models only. Note that only specific PXC models support this feature.

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

- Energy pulse output settings

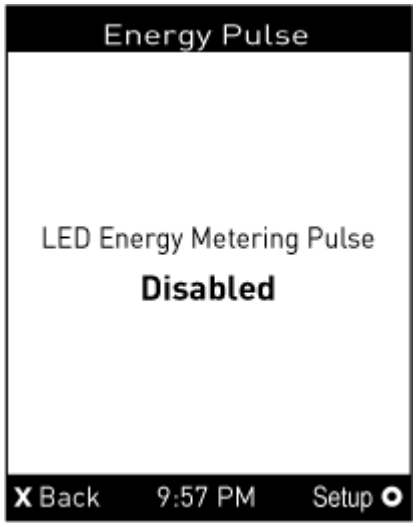
This feature, once enabled, blinks the energy pulse LED proportional to the energy consumption. For this LED's location, see ***PXC's Energy Pulse LED*** (on page 93).

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.



   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

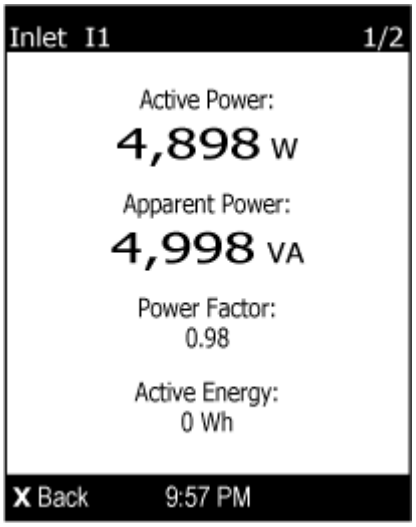
An inlet's information is divided into two pages. Page numbers are indicated in the top-right corner of the LCD display.

To show the inlet information:

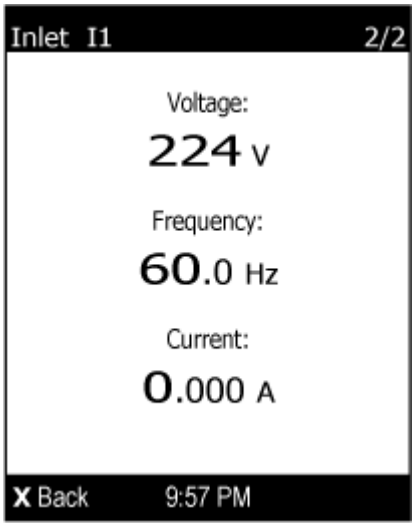
1. Press or to select "Inlet I1" in the Main Menu, and press .

Raritan
A brand of legrand

2. The first page shows the inlet's active power (W), apparent power (VA), power factor (PF), and active energy (Wh).



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).



   - 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.

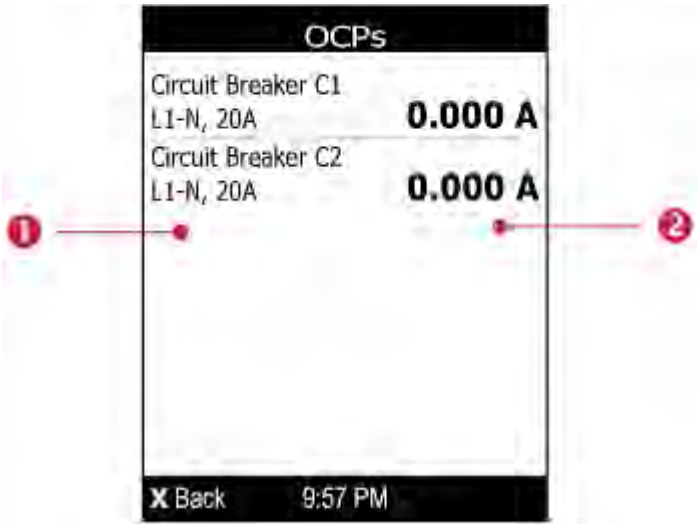
4. To return to the Main Menu, press .

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.



Number	Description
1	Overcurrent protector names. Associated lines and rated current are displayed below each overcurrent protector's name.
2	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.

Raritan
A brand of legrand

Outlets

This outlet-related section applies to 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 PXC/PXO is outlet-switching capable. To do this, you must first enable the front panel outlet control function. See ***Front Panel Settings*** (on page 323).

Showing Outlets Information

Multiple outlet information can be displayed on the LCD display.

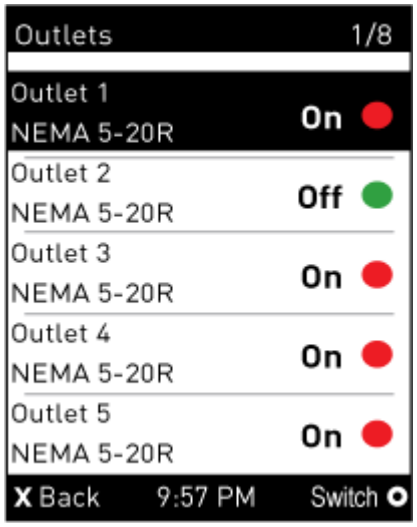
Control buttons that can be used and the system time are shown at the bottom of the LCD display.

To show outlets information:

1. Press ^ or v 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 v to select an outlet, and press ◎.
   - If the desired outlet is not visible, press ^ or v 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 323).

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.

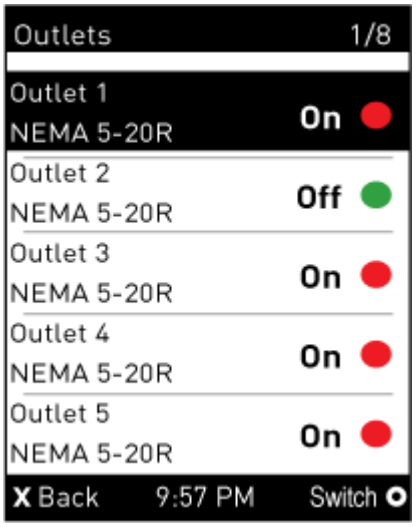
Control buttons that can be used and the system time are shown at the bottom of the LCD display.

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.



3. Press ∧ or ∨ to select an outlet, and press ○.

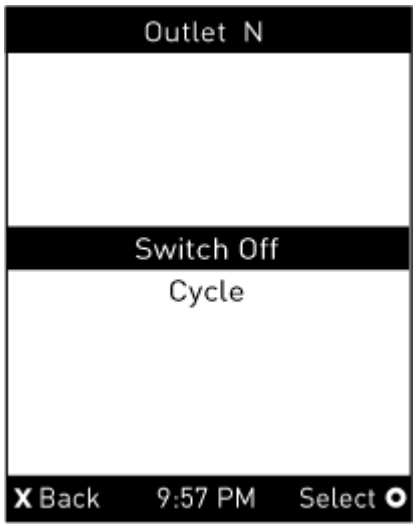
Raritan
A brand of legrand

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'.



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.

Outlet Groups

This outlet-related section applies to Switched PDUs only.

You can do the following on the front panel display:

- Show each outlet group's information, including each member outlet of a group.
- Turn on, off or power cycle an individual outlet group if your PXC/PXO is outlet-switching capable. To do this, you must first enable the front panel outlet control function. See ***Front Panel Settings*** (on page 323).

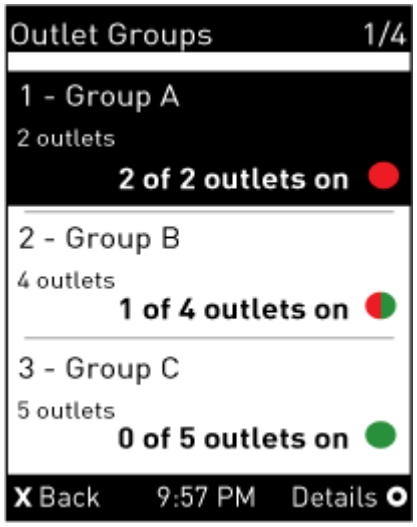
Showing an Outlet Group's Information

If any outlet group has been created, the front panel then shows a list of these groups and their status. See ***Creating an Outlet Group*** (on page 138).

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

To show an outlet group's information:

1. Press or to select "Outlet Groups" in the Main Menu, and press .
2. The LCD display shows a list of outlet groups with the information below:
   - The total number of outlets in the group
   - Power states which are indicated by the colors of circles
   - The total number of outlets that are turned ON in the group

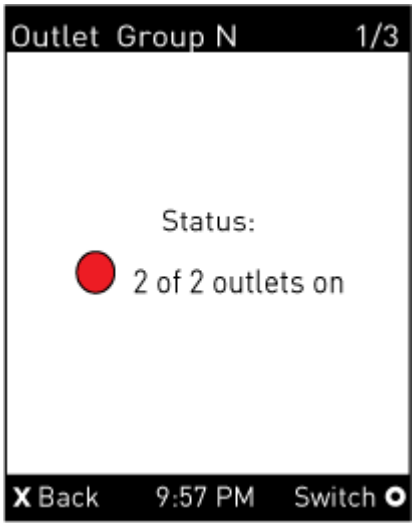


The currently-selected outlet group's number and total of outlet groups are indicated in the top-right corner of the display, such as "1/4" in the above diagram.

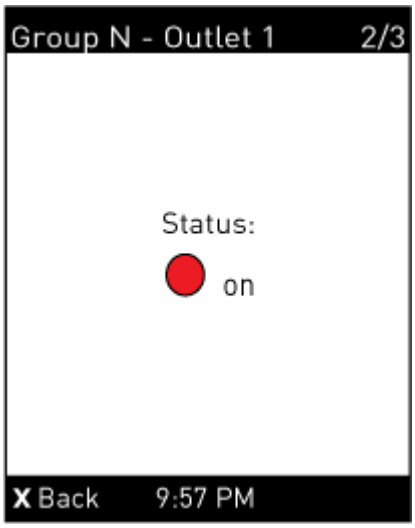
- A red circle indicates that all outlets of the group are powered on.
- A green circle indicates that all outlets of the group are powered off.
- A half-red half-green circle indicates some outlets are powered on while the others of the group are powered off.

3. Press or to select an outlet group, and press .
   - If the desired outlet group is not visible, press or to scroll up or down.
4. The LCD display shows the selected outlet group's power state.

Note: In the following diagrams, N represents the selected outlet group's index number. The rightmost number in the title bar represents this group's total pages.



5. To check the status of each member outlet of the group, press or .



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

Group's Power Control

This section applies to outlet-switching capable models only.

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 323).

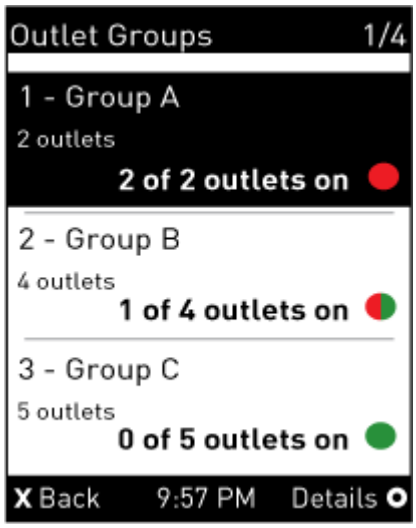
Control buttons that can be used and the system time are shown at the bottom of the LCD display.

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

1. Press or to select "Outlet Groups" in the Main Menu, and press .

Raritan
A brand of legrand

- The LCD display shows a list of outlet groups.



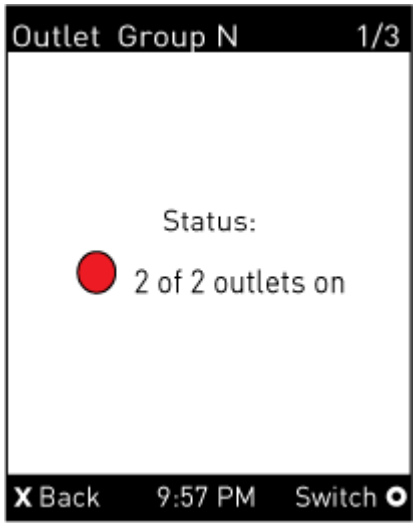
The currently-selected outlet group's number and total of outlet groups are indicated in the top-right corner of the display, such as "1/4" in the above diagram.

- A red circle indicates that all outlets of the group are powered on.
- A green circle indicates that all outlets of the group are powered off.
- A half-red half-green circle indicates some outlets are powered on while the others of the group are powered off.

2. Press ^ or v to select an outlet group, and press O.

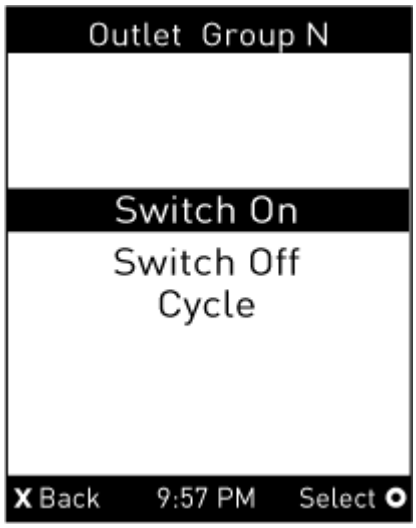
   If the desired outlet group is not visible, press ^ or v to scroll up or down.

Note: In the following diagrams, N represents the selected outlet group's index number. The rightmost number in the title bar represents this group's total pages.



3. Press to go to the power control page. 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.



4. Press or to select the desired option, and press .
   - Switch On: Turn on the outlet group.
   - Switch Off: Turn off the outlet group.

- Cycle: Power cycle the outlet group.

5. A confirmation message appears. Press or to select Yes or No, and then press .
   - Yes: Confirm the operation.
   - No: Abort the operation.
6. Verify that the selected outlet group is switched on or off, depending on the option you selected in the above step.
   - Check the outlet group state shown on the LCD display -- red or green circles.
   - Check each member outlet's LED of the group. A green LED indicates that the outlet is turned off, and a red LED indicates that the outlet is turned on.
7. To return to the Main Menu, press several times until the Main Menu is shown.

Peripherals

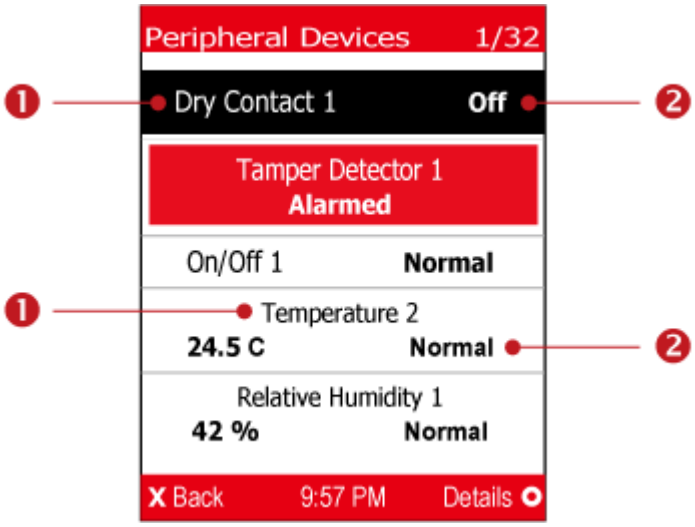
If there are no Raritan environmental sensor packages connected to your PXC/PXO, the LCD display shows the message "*No managed devices*" for the "Peripherals" menu command.

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 329).

To show environmental sensor or actuator information:

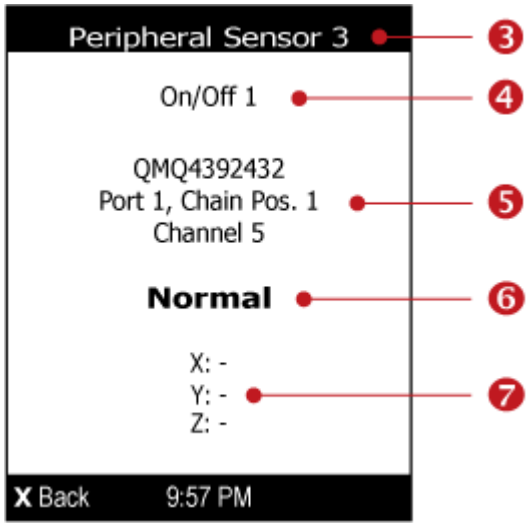
1. Press or to select "Peripherals" in the Main Menu, and press .
2. The display shows a list of environmental sensors/actuators.
   - If the desired sensor or actuator is not visible, press or to scroll up or down.
   - When the list exceeds one page, the currently-selected sensor/actuator's ID number 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 160).

The top and bottom bars also turn yellow or red. See ***Operating the Dot-Matrix LCD Display*** (on page 62).



Number	Description
1	Sensor or actuator names.
2	Sensor or actuator states as listed below. For further information, see ***Sensor/Actuator States*** (on page 163). ▪ *n/a* = unavailable ▪ *Normal* ▪ *Alarmed* ▪ *Lower Critical* = below lower critical ▪ *Lower Warning* = below lower warning ▪ *Upper Warning* = above upper warning ▪ *Upper Critical* = above upper critical ▪ *On* ▪ *Off* ▪ *Open* ▪ *Closed* A numeric sensor shows both the reading and state. A state sensor or actuator shows the state only.

3. To view an environmental sensor or actuator's detailed information, press or to select that sensor or actuator, and press . A screen similar to the following is shown.



Number	Description
3	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"
4	Sensor or actuator name.

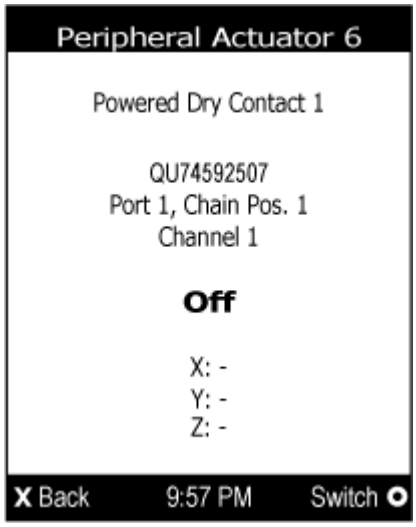
5	The following information is listed.
	▪ Serial number
	▪ Chain position, which involves the following information:
	  ▪ *Port <N>*: <N> is the number of the sensor port where this sensor or actuator is connected. This number is always 1 for PXC/PXO.
	  ▪ *Chain Pos. <n>*: <n> is the sensor or actuator's position in a sensor daisy chain.
	Note: Only Raritan's DX, DX2, DPX2 and DPX3 series provide the chain position information.
	▪ If this sensor or actuator is on a sensor package with multiple channels, such as DX2-DH2C2, its channel number is indicated as "Channel x", where x is a number.

6	Depending on the sensor type, any of the following information is displayed: ▪ State of a state sensor: *Normal*, *Alarmed*, *Open* or *Closed*. ▪ State of an actuator: *On* or *Off*. ▪ Reading of a numeric sensor.

Number	Description
7	X, Y, and Z coordinates which you specify for this sensor or actuator. See ***Individual Sensor/Actuator Pages*** (on page 169).

To switch on or off an actuator:

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



2. Press ⭘ to turn on or off the actuator. A confirmation message similar to the following is shown.

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.

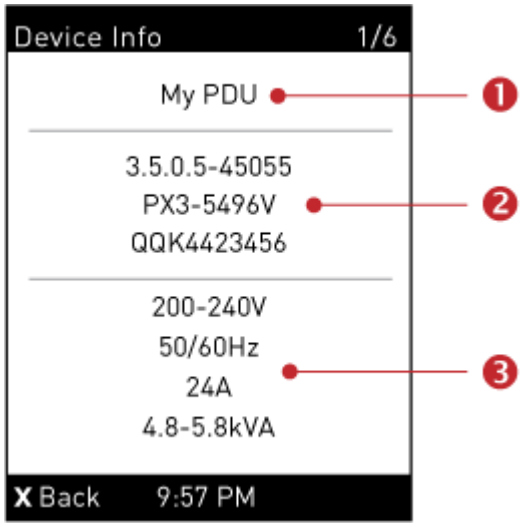
Raritan
A brand of legrand

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.

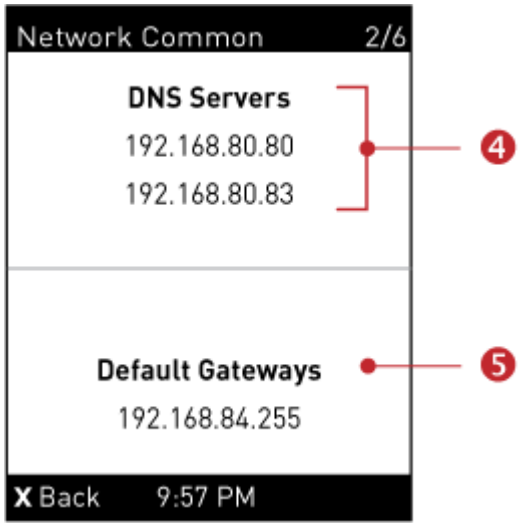
To show the device information:

1. Press ^ or v to select "Device Info" in the Main Menu, and press ○.
2. Device information similar to the following diagram displays.



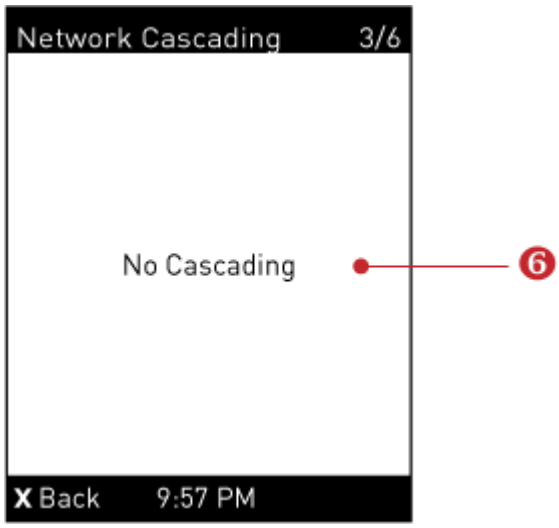
Number	Description
❶	Device name.
❷	Firmware version, model name and serial number.
❸	Device ratings, including rated voltage, frequency, current and power.

3. Press to show the Network Common page.

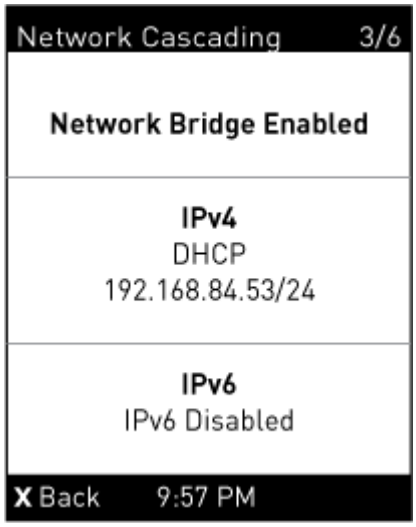


Number	Description
4	DNS servers.
5	Default gateways.

4. Press to show the Network Cascading page.



Raritan
A brand of legrand

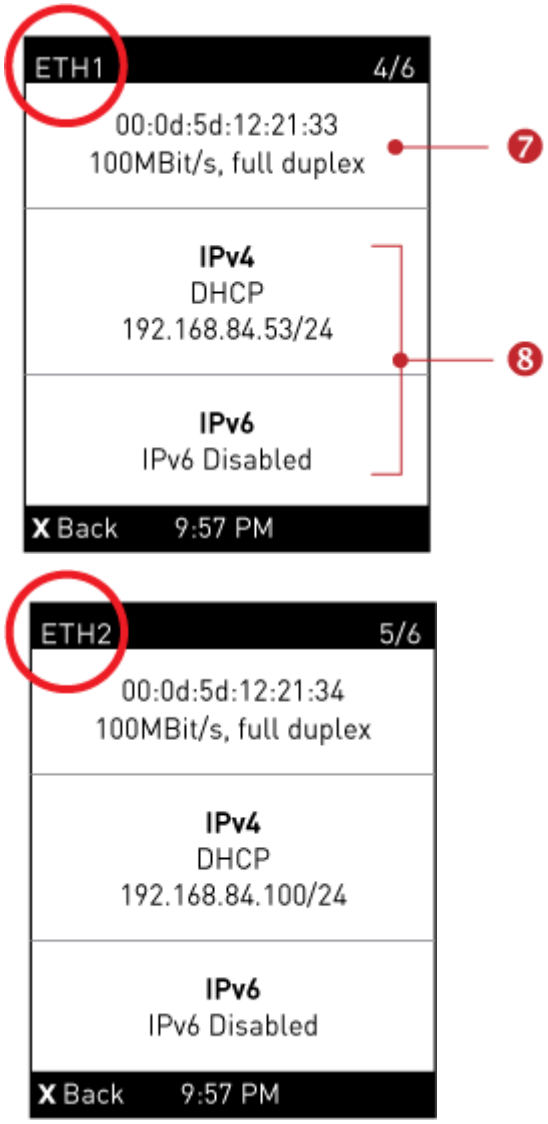


Number	Description

❻	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 207).
	▪ 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 PXC/PXO has two Ethernet pages -- ETH1 and ETH2.



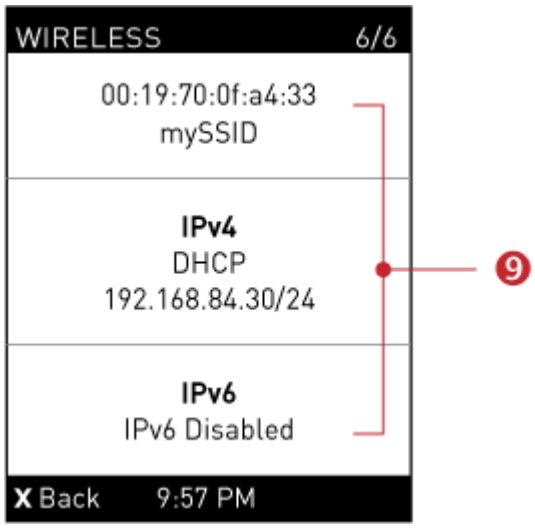
Number	Description
7	Ethernet interface information, including: ▪ MAC address. ▪ Speed. ▪ Full or half duplex.

Number	Description
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 194).*

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

6. Press to show the WIRELESS page.

-- 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 ⊗.

Manually Changing PXC's Zero U LCD Orientation

A Zero U model has a tilt sensor that can detect the orientation of its physical device to automatically adjust ts LCD content's orientation.

If the LCD's orientation does not meet your need, you can manually configure it.

The factory default is automatic orientation.

To set up the LCD orientation:

1. Press ⌃ or ⌄ simultaneously until you see the LCD shows "Fixed Orientation".
2. If the current LCD orientation does not meet your need, repeat the above step until the orientation you preferred is displayed.
   - If you want to return to the factory default, also repeat step 1 until the LCD shows "Automatic Orientation".

Raritan
A brand of legrand

Alerts Notice in a Yellow or Red Screen

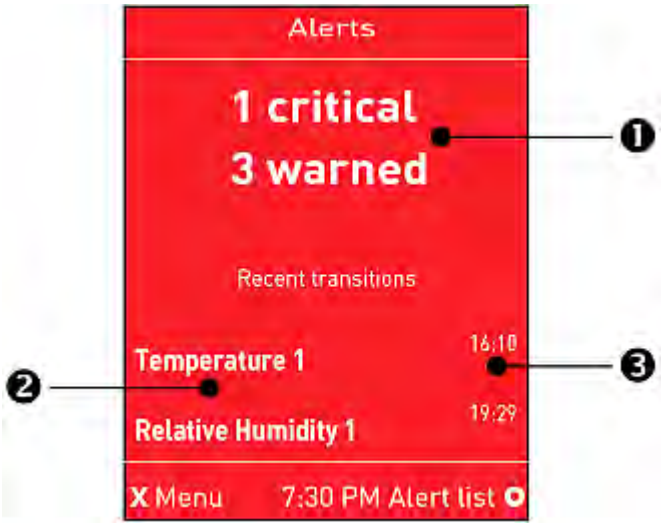
In the automatic mode, if an alert occurs, the LCD display automatically shows a yellow or red screen which indicates the total number of alerted sensors and information of the latest transitions.

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

For color definitions, see ***Yellow- or Red-Highlighted Sensors*** (on page 160).

The following illustrates the alerts notices in red.

▶ **When there are only alerted sensors -- NO ALARMS are present:**



Number	Description
1	The total of alerted sensors in critical and warning levels.
2	A list of final alerted sensors that changed their readings or states.
3	The final time that each alerted sensor changed its readings or states.

When there is any alarm present:

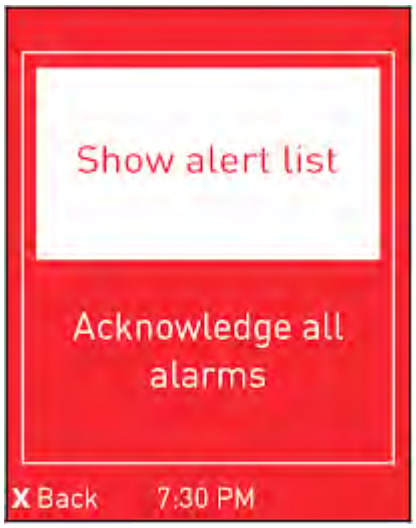
The LCD display looks similar to the above diagram except that it shows the alarm(s) and the available command in the bottom-right corner is 'Actions' instead of 'Alert list'.

Raritan
A brand of legrand

Available operations:

- For the notice listing alerted sensors only, press to view a list of all alerted sensors. See ***Alerts*** (on page 65).
- For the notice where at least an alarm is present, press . Then do the following:

  a. Two options display. Press or to select either option, and press .



- *Show alert list*: This option lists all of alerted sensors and alarms. You still can choose to acknowledge alarms after viewing the list. See ***Alerts*** (on page 65).
- *Acknowledge all alarms*: This option immediately acknowledges all existing alarms, without showing the list of alarms.

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

Showing the Firmware Upgrade Progress

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

Raritan
A brand of legrand

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

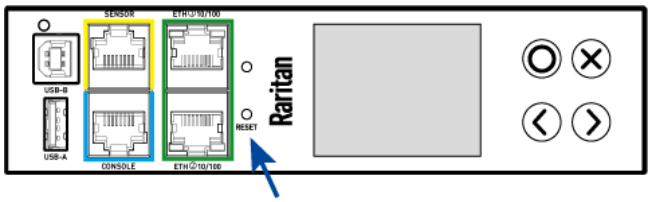
Reset Button

The reset button is located inside the small hole labeled RESET near the display panel.

Pressing this reset button restarts the PXC/PXO software without any loss of power to outlets.

The PXC/PXO can be reset to its factory default values using this button when a serial connection is available. See ***Resetting to Factory Defaults*** (on page 619).

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

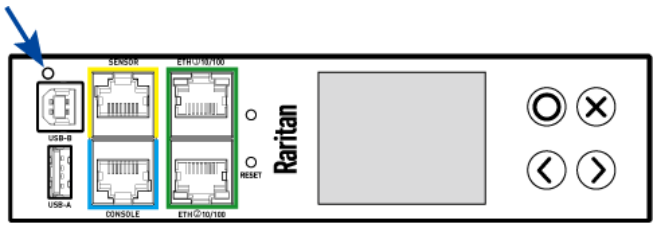


PXC's Energy Pulse LED

The following feature applies to PXC only, but only specific PXC models support this feature and have this LED. As for PXO series, they do NOT have this 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 67).

Circuit Breakers

PXC/PXO 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 62).

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.

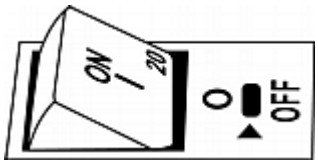
Depending on the model you purchased, the circuit breaker may use a button- or handle-reset mechanism.

Resetting the Button-Type Circuit Breaker

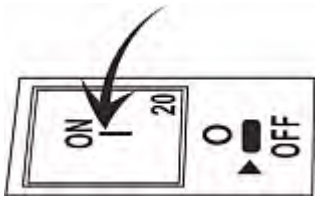
Your button-type circuit breakers may look slightly different from the images shown in this section, but the reset procedure remains the same.

To reset the button-type breakers:

1. Locate the breaker whose ON button is up, indicating that the breaker has tripped.



2. Examine your PXC/PXO 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.



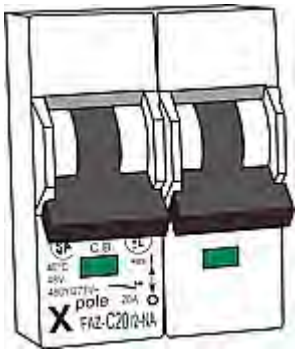
Raritan
A brand of legrand

Resetting the Handle-Type Circuit Breaker

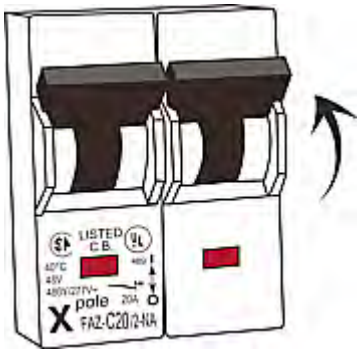
Your handle-type circuit breakers may look slightly different from the images shown in this section, but the reset procedure remains the same.

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 PXC/PXO 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.



Chapter 6 Using the Web Interface

This chapter explains how to use the web interface to administer the PXC/PXO.

In This Chapter

Supported Web Browsers 96
Login, Logout and Password Change 96
Web Interface Overview 100
Dashboard 107
PDU 117
Inlet 121
Outlets 123
Outlet Groups 137
OCPs 147
Peripherals 154
User Management 176
Device Settings 188
Maintenance 331
Webcam Management 356
SmartLock and Card Reader 369

Supported Web Browsers

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

Login, Logout and Password Change

The first time you log in to the PXC/PXO, 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 177).

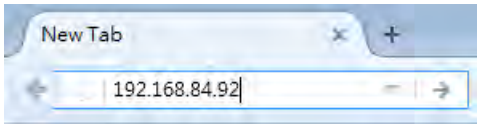
Login

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

To log in to the web interface:

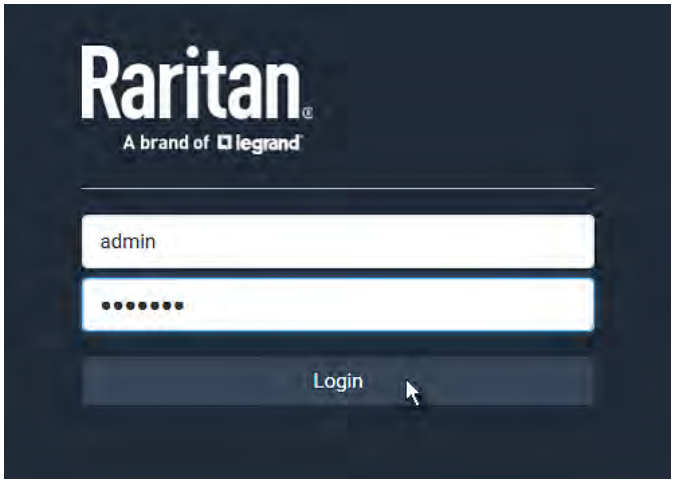
1. Open a browser and type the IP address of your PXC/PXO.

- 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 3).



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 105).*

2. If any security alert message appears, accept it.
3. The login screen displays. Type your user name and password. User credentials are case sensitive.

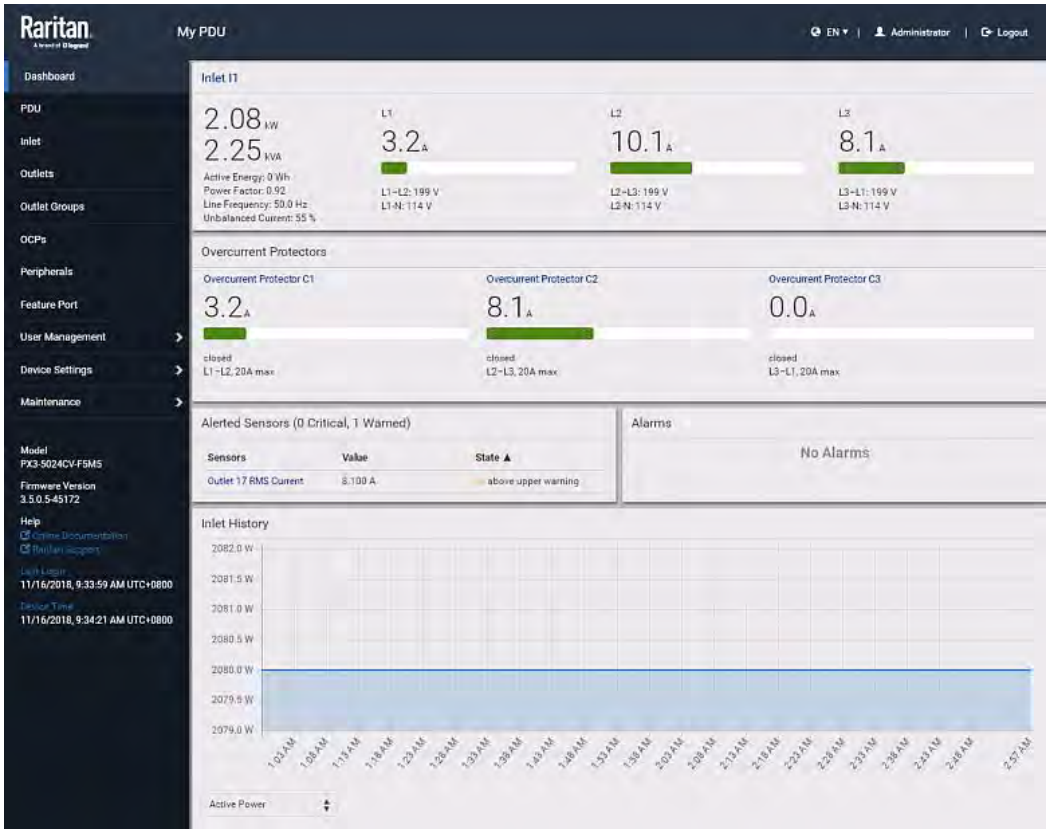


4. (Optional) If a security agreement is displayed, accept it. Otherwise, you cannot log in.

Note: To configure the security agreement, see **Enabling the Restricted Service Agreement** *(on page 249).*

5. Click Login or press Enter. The web interface of PXC/PXO 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 213).*

Changing Your Password

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

To change other users' passwords, Change Local User Management privilege is required. See ***Editing or Deleting Users*** (on page 181).

Password requirements:

- Case sensitive.
- 4 to 64 characters.

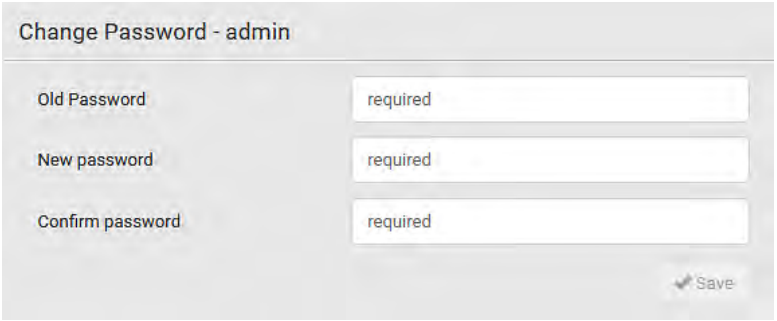
Password change required on first login:

- On *first login*, password change is forced and strong passwords are enabled by default. The new password must be at least 8 characters and contain at least one upper case letter, one lower case letter, and one digit.
- Change the default password and click OK.

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 182).

- Choose User Management > Change Password. Change the password and click Save.



Remembering User Names and Passwords

PXC/PXO 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.

PXC/PXO does NOT support other browser password managers.

Logout

After finishing your tasks, you should log out to prevent others from accessing the PXC/PXO web interface. You can click Logout in the top right corner, or close the tab or browser.

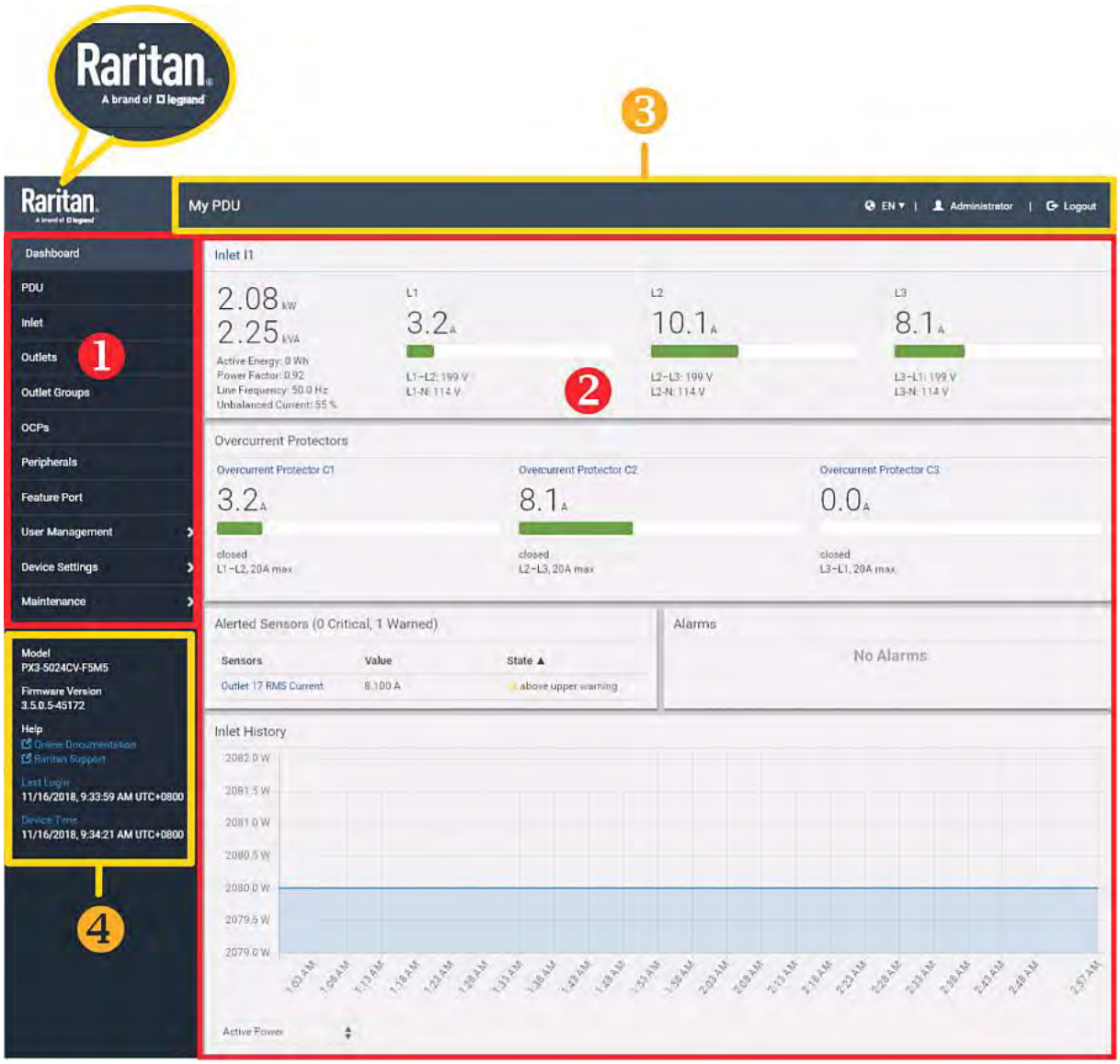
Web Interface Overview

The web interface consists of four areas as shown below.

Operation:

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

4. To return to the main menu and the Dashboard page, click on the top-left corner.

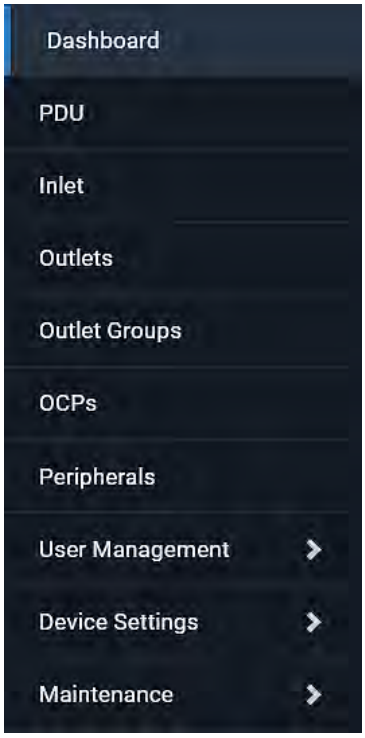


Number	Web interface element
1	***Menu*** (on page 103)
2	Data/setup page of the selected menu item.
3	▪ Left side: - PXC/PXO device name.

Number	Web interface element
	Note: To customize the device name, see **PDU** *(on page 117).* ▪ Right side: - Displayed language, which is English (EN) by default. You can change it. - Your login name, which you can click to view your user account settings. - Logout button.
4	From top to bottom -- ▪ Your PXC/PXO model. ▪ Current firmware version. ▪ **Online Documentation**: link to the online help of PXC/PXO. - See ***Browsing through the Online Help*** (on page 708). ▪ **Raritan Support**: link to Raritan Technical Support webpage. ▪ Date and time of your user account's last login. - Click **Last Login** to view your login history. ▪ PXC/PXO 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 PXC/PXO may show all or some menu items shown below.



In the following table, the menu item marked with * is NOT supported by PXO.

Menu	Information shown
Dashboard	Summary of the PXC/PXO status, including a list of alerted sensors and alarms, if any. See ***Dashboard*** (on page 107).
PDU	Device data and settings, such as the device name and MAC address. See ***PDU*** (on page 117).
Inlet	Inlet status and settings, such as inlet thresholds. See ***Inlet*** (on page 121).
Outlets	Outlet status, settings and outlet control if your model is outlet-switching capable. See ***Outlets*** (on page 123).

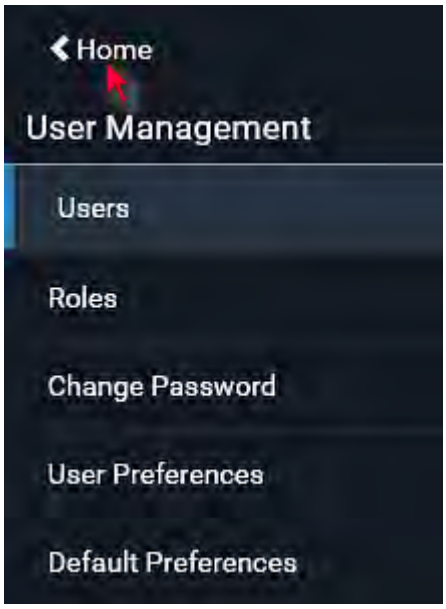
Menu	Information shown
Outlet Groups	Only PDUs with outlet-switching and/or outlet-metering feature show this menu item. You can create one or multiple groups comprising one or multiple outlets of the same PXC/PXO. Functions which you can perform on an outlet group vary depending on the model you purchased. See ***Outlet Groups*** (on page 137).
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 147).
Peripherals	Status and settings of Raritan environmental sensor packages, if connected. See ***Peripherals*** (on page 154).
Webcams	The 'Webcams' menu item appears when there is any webcam(s) connected to the PXC/PXO, or when there are snapshots saved onto the PXC/PXO already. Webcam live snapshots/video and webcam settings. See ***Webcam Management*** (on page 356).
* SmartLock *-- and/or --* Card Readers	Either or both menu items appear only when you connect Raritan's SmartLock kit to this product. For details, refer to the user documentation accompanying the SmartLock kit or download it from Raritan's ***Support page*** (***http://www.raritan.com/support/***). ▪ **SmartLock**: Configures and controls the door handles connected to this product via DX2-DH2C2. Note that this page is not available if connecting the door handles to other Raritan sensors than DX2-DH2C2. ▪ **Card Readers**: Lists the card readers connected to PXC/PXO directly or indirectly. See ***SmartLock and Card Reader*** (on page 369). **Note that PXO does NOT support Raritan's SmartLock kit. Only PXC supports it.**
User Management	Data and settings of user accounts and groups, such as password change. See ***User Management*** (on page 176).
Device Settings	Device-related settings, including network, security, system time, event rules and more. See ***Device Settings*** (on page 188).

Menu	Information shown
Maintenance	Device information and maintenance commands, such as firmware upgrade, device backup and reset. See ***Maintenance*** (on page 331).

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

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

- Click the topmost link with the symbol <. For example, click Home.



- Click Raritan 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 PXC/PXO 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 PXC/PXO 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 PXC/PXO is 192.168.84.118.

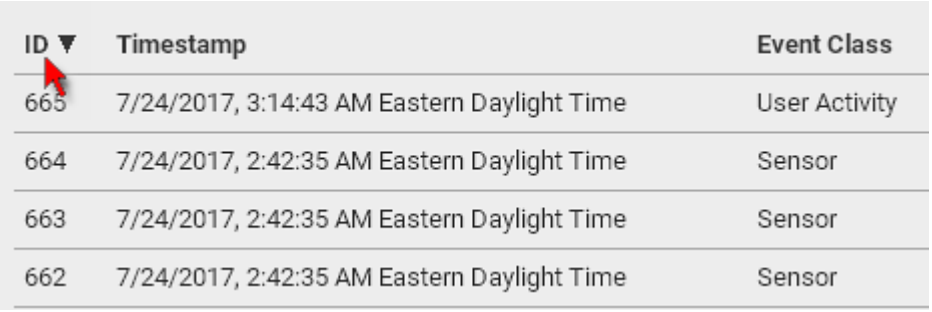
Page	URL
Peripherals	https://192.168.84.118/#/peripherals
Event Log	https://192.168.84.118/#/maintenance/eventLog/0

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:

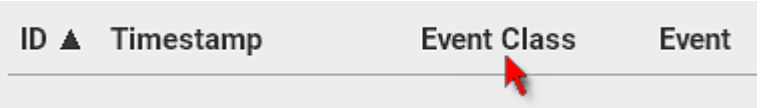
1. By default, the Event Log is sorted in the descending order based on the ID column. Therefore, the arrow ▼ is displayed adjacent to the ID header.
2. To have it resorted in the ascending order based on the same column, click the ID header.



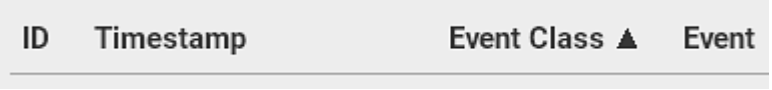
ID ▼	Timestamp	Event Class
665	7/24/2017, 3:14:43 AM Eastern Daylight Time	User Activity
664	7/24/2017, 2:42:35 AM Eastern Daylight Time	Sensor
663	7/24/2017, 2:42:35 AM Eastern Daylight Time	Sensor
662	7/24/2017, 2:42:35 AM Eastern Daylight Time	Sensor

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

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



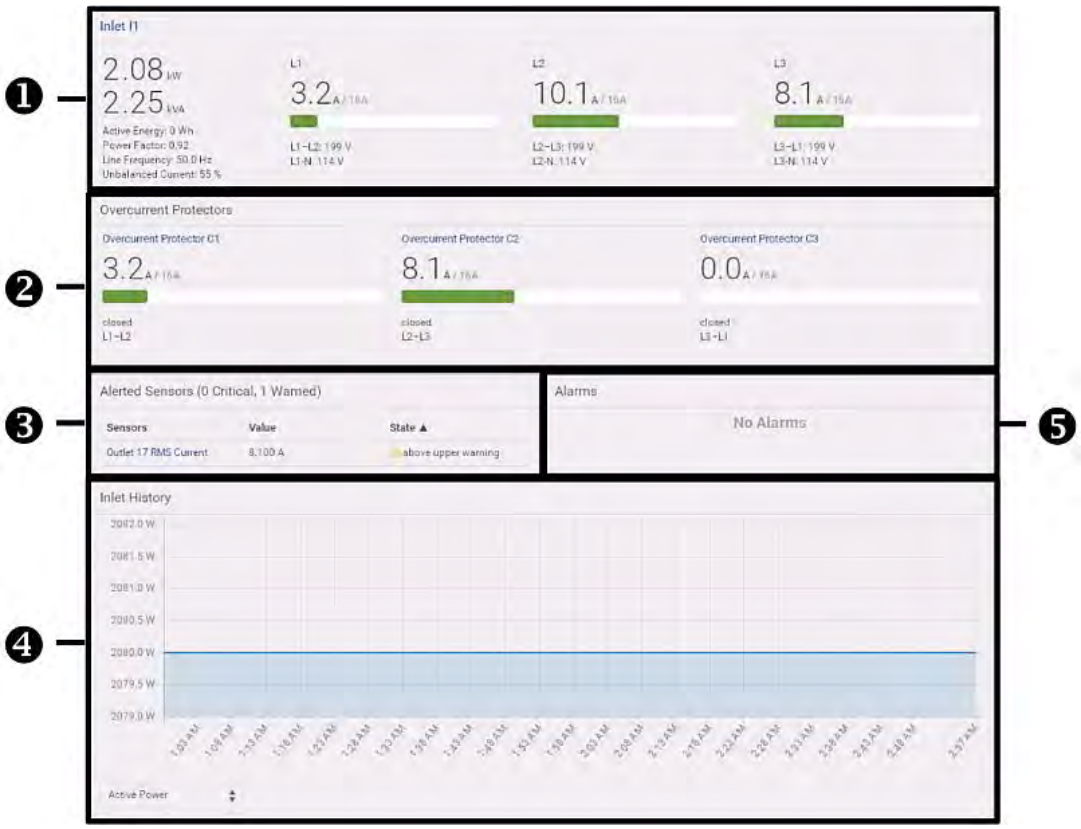
5. The arrow ▲ now appears adjacent to the selected column 'Event Class,' indicating the list is sorted in the ascending order based on that column.



Raritan
A brand of legrand

Dashboard

The Dashboard page contains four to five sections, depending on your model.

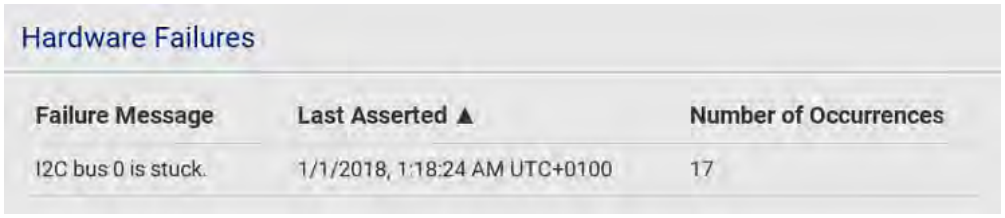


Number	Section	Information shown
❶	**Inlet I1**	▪ Overview of inlet power data ▪ A current bar per phase, which changes colors to indicate the RMS current state - green: normal - yellow: warning - red: critical See ***Dashboard - Inlet I1*** (on page 109).
❷	**Overcurrent Protectors**	This section is available only when your PXC/PXO 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 111).
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 112).
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 114).
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 115).

The Hardware Failures section:

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

Raritan
A brand of legrand



This section does NOT display as long as there are no hardware failures present. See ***Hardware Issue Detection*** (on page 352).

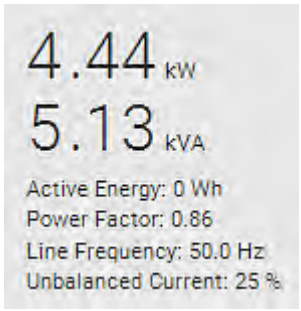
Dashboard - Inlet I1

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 121).

Left side - generic inlet power data:



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:

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 121).

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 147).

Status	Bar colors
normal	
above upper warning	
above upper critical	

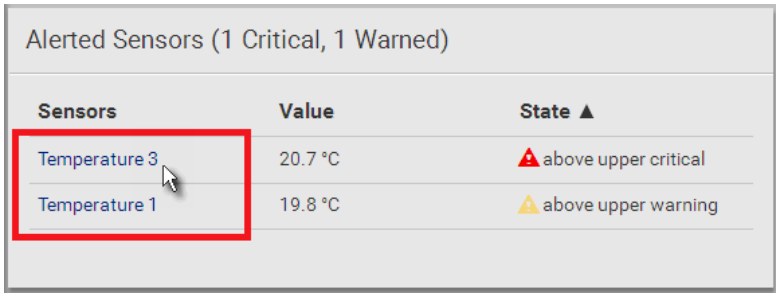
Note: The "below lower warning" and "below lower critical" states also show yellow and red colors respectively. However, it is not meaningful to enable the two thresholds for current levels.

Dashboard - Alerted Sensors

When any internal sensors or environmental sensor packages connected to the PXC/PXO 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 169).

If wanted, you can resort the list by clicking the desired column header. See ***Sorting a List*** (on page 106).



Raritan
A brand of legrand

Summary in the section title:

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

For example:

- **1 Critical**: 1 sensor enters the critical or alarmed state.
  - Numeric sensors enter the critical state.
  - State sensors enter the alarmed state.
- **1 Warned**: 1 'numeric' sensor enters the warning state.

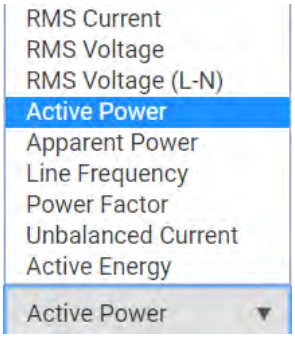
List of alerted sensors:

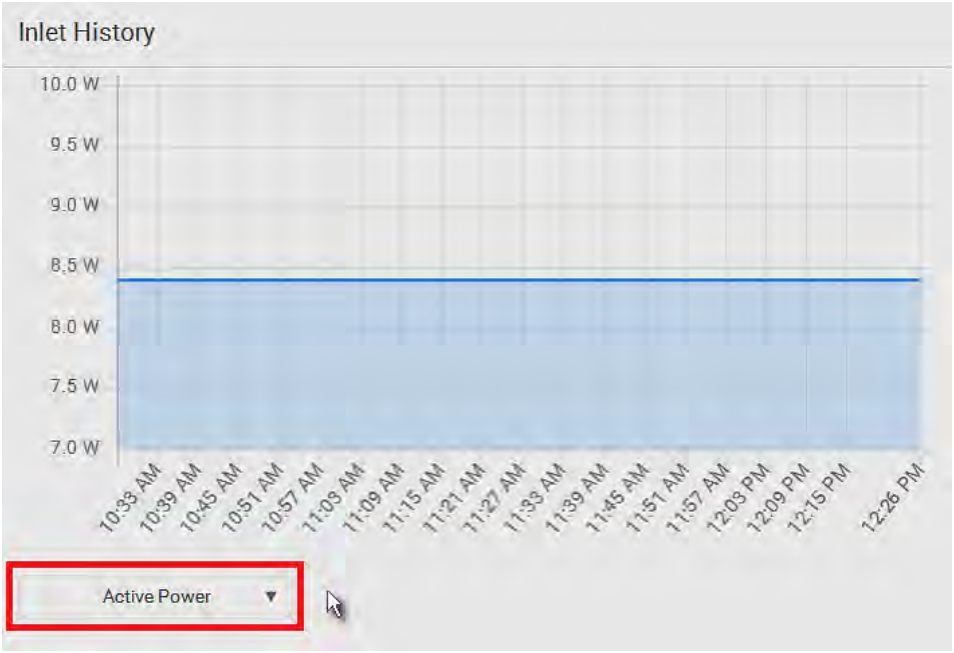
Two icons are used to indicate various sensor states.

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

For details, see ***Sensor/Actuator States*** (on page 163).

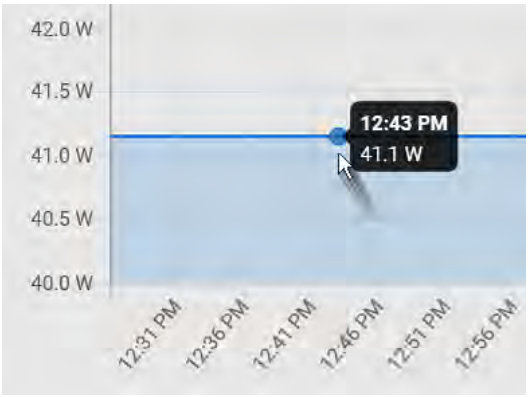
Dashboard - Inlet History

- The Inlet History graph displays the history of the sensor values. Select a different data type by clicking the selector ▼ below the diagram.
- 



Raritan
A brand of legrand

- 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

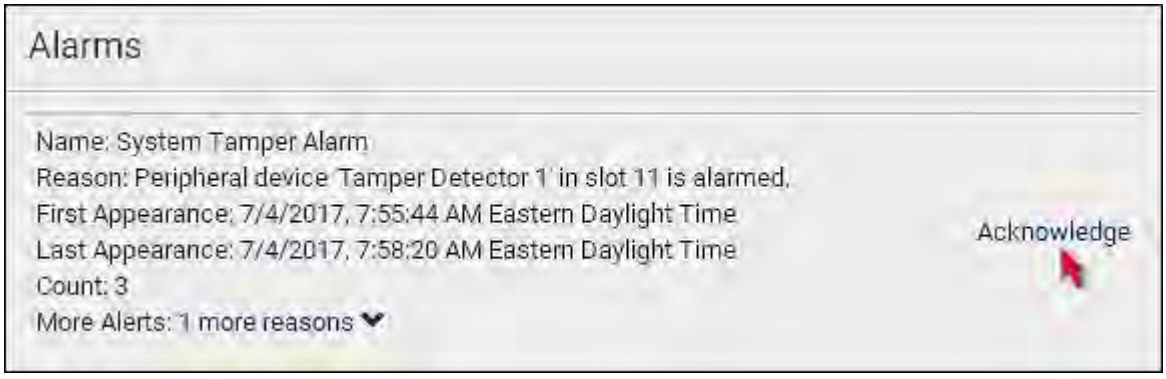
If configuring any event rules which require users to take the acknowledgment action, the Alarms section will list any event which no one acknowledges yet since event occurrence.

Note: For information on event rules, see **Event Rules and Actions** *(on page 259).*

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.

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

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

Tip: You can also acknowledge all alarms by operating the LCD display. Refer to **Alerts Notice in a Yellow or Red Screen** *(on page 89).*

Raritan
A brand of legrand

PDU

The PXC/PXO device's generic information and PDU settings are available on the PDU page.

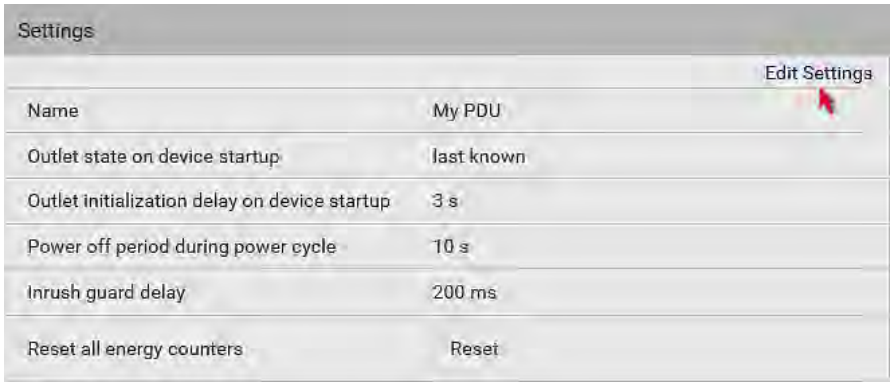
To open the PDU page, click 'PDU' in the ***Menu*** (on page 103).

Device information shown:

- Firmware version
- Serial number
- MAC address
- Rating

To configure global settings:

1. Click Edit Settings.



2. Now you can configure the fields.
   - Click to select an option.
   - Adjust the numeric values.
   - Select or deselect the checkbox.
   - 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 120).

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

Field	Function	Note
Name	Customizes the device name.	

Field	Function	Note
*Outlet state on device startup	Determines the initial power state of ALL outlets after the PXC/PXO powers up. ▪ *Options: on, off, and last known* See ***Options for Outlet State on Startup*** (on page 119).	▪ 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 133).
*Outlet initialization delay on device startup	Determines how long the PXC/PXO 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 119).
*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 133).
*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 120).

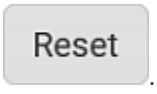
3. Click Save.

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 PXC/PXO 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.

Note: This reset button does not reset the active energy values of outlet groups. See **Outlet Groups** *(on page 137).*

1. Click 

.
2. Click Reset on the confirmation message.
   - All active energy readings on this PXC/PXO 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 PXC/PXO 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 PXC/PXO was powered off.

If you are configuring an individual outlet on ***Individual Outlet Pages*** (on page 133), 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 117). 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.

Time Units

If you choose to type a new value in the time-related fields, such as the "Idle timeout period" field, you must add a time unit after the numeric value. For example, you can type '15 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)

Raritan
A brand of legrand

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 103).

Inlet thresholds, once enabled, help you identify whether the inlet enters the warning or critical level. In addition, you can have PXC/PXO automatically generate alert notifications for any warning or critical status. See ***Event Rules and Actions*** (on page 259).

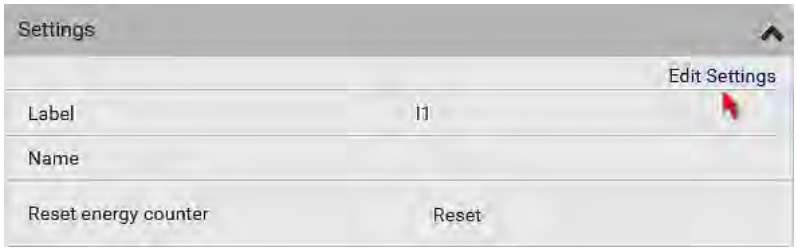
Generic inlet information shown:

- Inlet power overview, which is the same as ***Dashboard - Inlet I1*** (on page 109).
- 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 160).
- Inlet's power chart, which is the same as ***Dashboard - Inlet History*** (on page 114)

To customize the inlet's name:

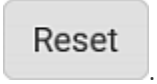
1. Click Edit Settings.



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 

.
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 684). You can modify them to meet your needs.

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

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

Thresholds

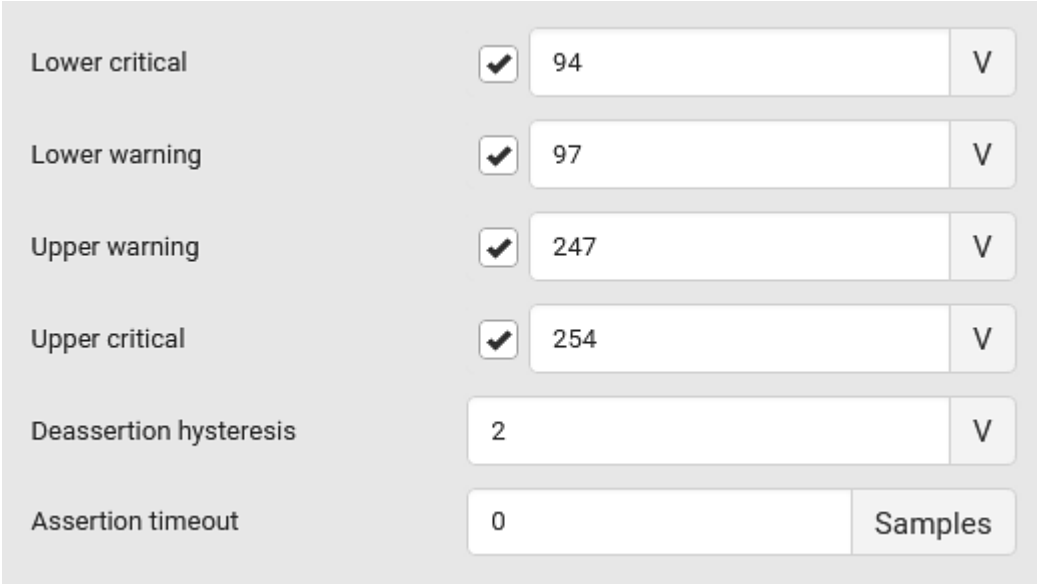
Edit Thresholds

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.

Raritan
A brand of legrand

- Type a new value in the accompanying text box.



For concepts of thresholds, deassertion hysteresis and assertion timeout, see ***Sensor Threshold Settings*** (on page 676).

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 103).

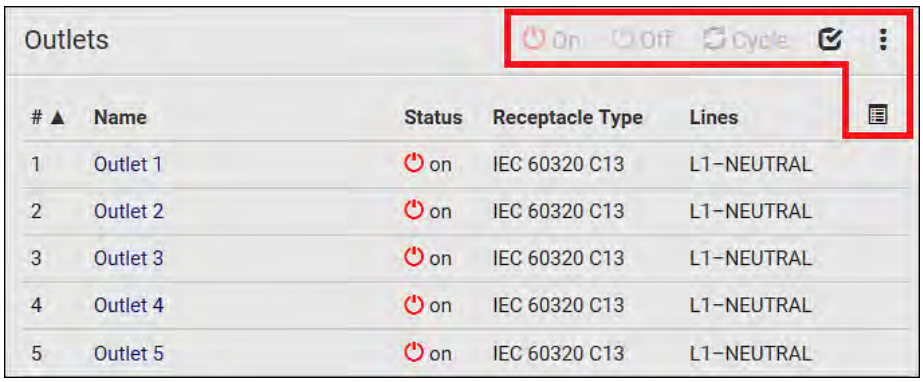
On this page, you can:

- **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 133).

If wanted, you can resort the list by clicking the desired column header. See ***Sorting a List*** (on page 106).

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 127).

Raritan
A brand of legrand

Only Switched PDUs support all of the following features while 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 128)
Load Shedding Setup	***Setting Non-Critical Outlets*** (on page 129)
Activate Load Shedding -- OR-- Deactivate Load Shedding	***Load Shedding Mode*** (on page 130)

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.

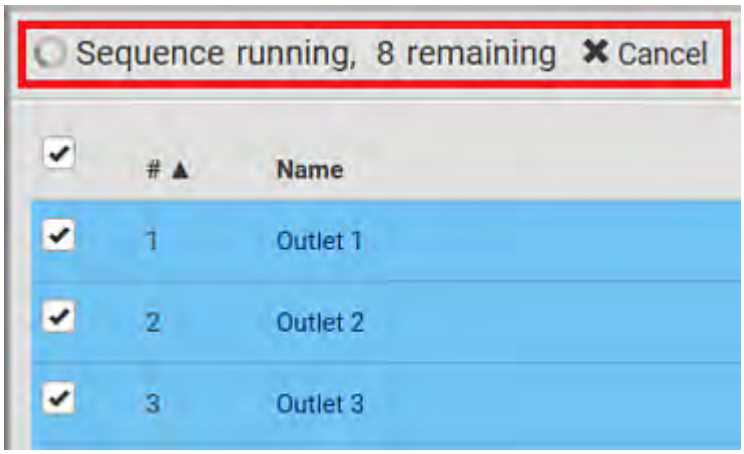
3. Click or select the desired button or command.

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 133).*

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 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 . See ***Outlets*** (on page 123).

- 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 130).
false	The outlet is a critical outlet, which will remain unchanged in the load shedding mode.

- Sequence order
- Sequence delay (seconds)

Note: To set critical and non-critical outlets, or set sequence-related settings, see **Outlets** *(on page 123).*

- 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 PXC/PXO. 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 PXC/PXO 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 PXC/PXO, 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.

PXC/PXO will insert a power-on delay between the configured outlet and the one following it during the power-on process.

Raritan
A brand of legrand

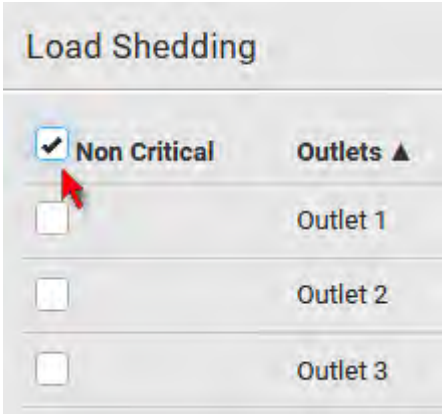
Setting Non-Critical Outlets

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 130).

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.



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 133).*

Load Shedding Mode

When a UPS supplying power to PXC/PXO 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 129).

When load shedding is activated, the PXC/PXO turns off all non-critical outlets. When load shedding is deactivated, the PXC/PXO 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 123) or* **Available Data of the Outlets Overview Page** *(on page 127).*

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 PXC/PXO 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.

Raritan
A brand of legrand

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 132).*

- 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.

Tip: To make the Non-Critical column appear when the load shedding mode is not activated yet. See **Outlets** *(on page 123) or* **Available Data of the Outlets Overview Page** *(on page 127).*

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 PXC/PXO, 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 306).

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 remain powered OFF 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 turned on after disabling the load shedding mode.

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

Raritan
A brand of legrand

Individual Outlet Pages

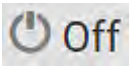
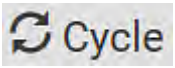
An outlet's data/setup page is opened after clicking the outlet's name on the Outlets overview page. See ***Outlets*** (on page 123).

The individual outlet's page shows this outlet's detailed information. See ***Detailed Information on Outlet Pages*** (on page 136).

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 Switched PDUs support the following power-control operation.

To power control this outlet:

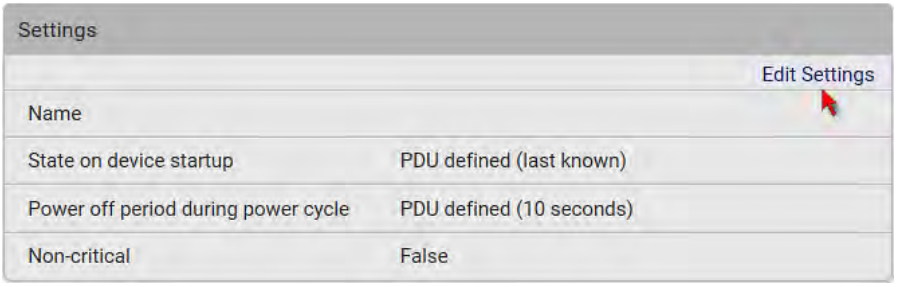
1. Click one of the power-control buttons.

Button/command	Action
	Power ON.
	Power OFF.
	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.



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

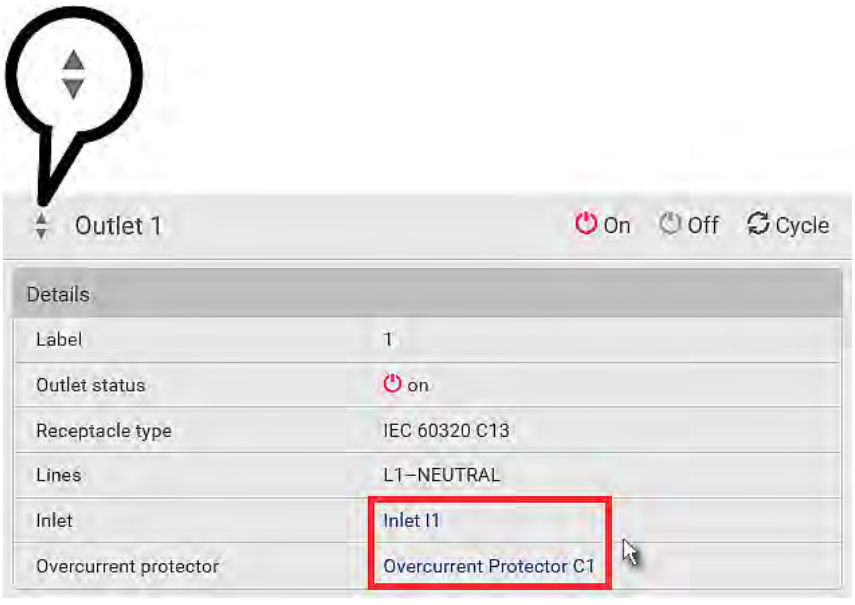
Field	Description
Name	Type an outlet name up to 64 characters long.
*State on device startup	Click this field to select this outlet's initial power state after PXC/PXO powers up. ▪ Options: *on*, *off*, *last known* and *PDU defined*. See ***Options for Outlet State on Startup*** (on page 119). ▪ Note that any option other than "PDU defined" will override the global outlet state setting on this particular outlet.

Field	Description
*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 136). ▪ 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 130).

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 PXC/PXO 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 133).

Option	Function
PDU defined (xxx)	Follows the global power-off period setting, which is set on ***PDU*** (on page 117). 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 120).

Raritan
A brand of legrand

Outlet Groups

This outlet-related section applies to Switched PDUs only.

Choose Outlet Groups in the ***Menu*** (on page 103). The following Outlet Groups page opens.

Required permissions:

You must have one of the permissions below to be able to operate all or some of the outlet group features.

- Administrator Privileges -- *all operations*
- Change Pdu, Inlet, Outlet & Overcurrent Protector Configuration -- *creating, editing and deleting outlet groups*
- Switch Outlet Group -- *powering on, off or cycle outlet groups*

Outlet group operations:

You can group one or multiple outlets on this page using

. See ***Creating an Outlet Group*** (on page 138).

The Outlet Groups page will list all outlet groups you create.

# ▲	Name	Outlet State	Outlets
1	Outlet group 1	2 on	1-2
2	Outlet group 2	1 on , 2 off	1 and 3-4
3	Outlet group 3	1 on , 3 off	1, 3 and 5-6

Then you can perform one of the following actions on one or multiple outlet groups:

- Power on, off or cycle the selected group(s). See ***Outlet Group Power Control*** (on page 139).
- Observe the power status of each outlet group and/or power status of each member outlet.
- Re-name a group or change its member outlets. See ***Modifying an Outlet Group*** (on page 142).

Creating an Outlet Group

You can create an outlet group if you often have to power on, off or cycle the same outlets at a regular interval.

Note that an outlet can be the member outlet of one or multiple groups.

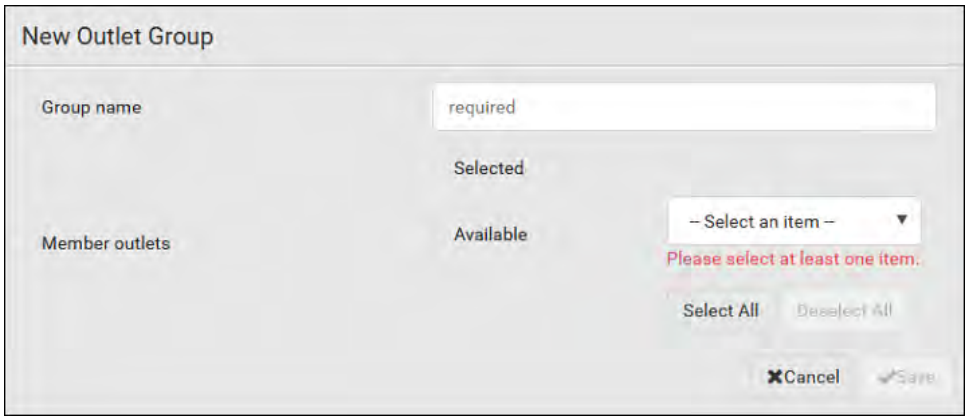
To create an outlet group, you must have either permission below.

- Administrator Privileges
- Change Pdu, Inlet, Outlet & Overcurrent Protector Configuration

▶ **To create an outlet group:**

1. Click

.
2. Type the group name.



3. Select the outlets you want in the Available field.
   - To select all outlets of the PDU, click Select All.
4. To delete any selected outlet(s), click an outlet's ✖ in the Selected field.
   - To remove all selected outlets, click Deselect All.
5. Click Save.

Tip: PXC/PXO allows you to assign the same name to diverse outlet groups. If this really occurs, you still can identify different groups through their unique index numbers.

Raritan
A brand of legrand

Outlet Group Power Control

You must have either permission below to power control any outlet groups.

- Administrator Privileges
- Switch Outlet Group

You can switch one or multiple outlet groups at a time on the Outlet Groups page.

To switch one single outlet group only, there are two methods -- either the Outlet Groups page or individual group page.

To switch one or multiple groups on the Outlet Groups page:

This method allows you to switch more than one outlet group simultaneously.

1. Click to make checkboxes appear in front of outlet groups.

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

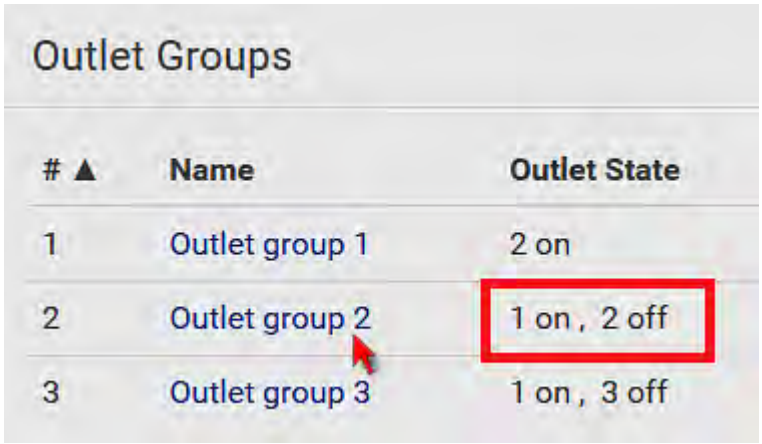
2. Select multiple outlet groups.
   - To select ALL outlet groups, select the topmost checkbox in the header row.

3. Click the desired button.

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.

Confirm the operation when prompted.

4. Verify that the outlet-switching result on the Outlet State column of the Outlet Groups page.
   - For example, if a group's Outlet State reads "1 on, 2 off", it means there are 3 outlets in total -- one of the outlets is turned ON, and two of the outlets are turned OFF.
   - For detailed information about which outlets are turned on and which are turned off, you can open that outlet group's page by clicking on its name.

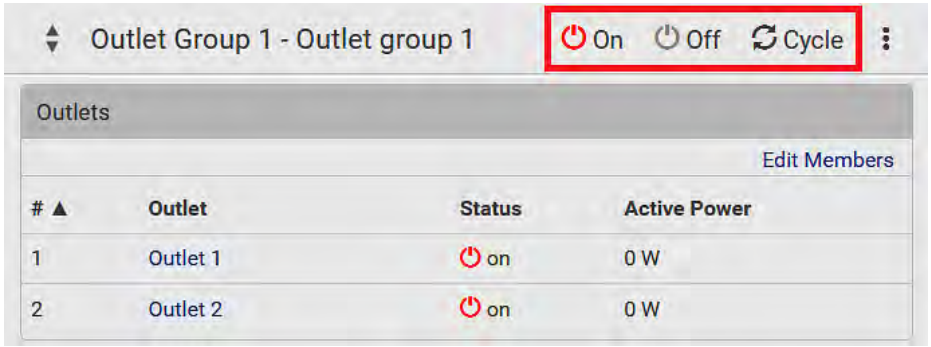


To switch one group on a specific outlet group's page:

This method allows you to switch ONLY one outlet group at a time.

1. Open a specific outlet group's page by clicking on its name.

2. Click the desired power control button on the top-right corner.
   - Confirm the operation when prompted.



If Switchable Outlet Groups are Limited

For the Switch Outlet Group permission, if you assign a role to any user, which permits the user to switch only "specific" outlet groups instead of all outlet groups, the following switching issue may appear.

Issue:

- When an outlet group that the user originally can switch is deleted, and then re-created with the same group name, the user will not be able to switch the "new" outlet group with the same group name.

Solution:

1. Edit the role assigned to the user. See ***Editing or Deleting Roles*** (on page 184).

2. Find the Switch Outlet Group permission, and re-select that newly-created outlet group in its outlet group list.

Note: The above issue does not occur for any role which has "All Outlet Groups" selected for its Switch Outlet Group permission.

Modifying an Outlet Group

To modify an outlet group, you must have either permission below.

- Administrator Privileges
- Change Pdu, Inlet, Outlet & Overcurrent Protector Configuration

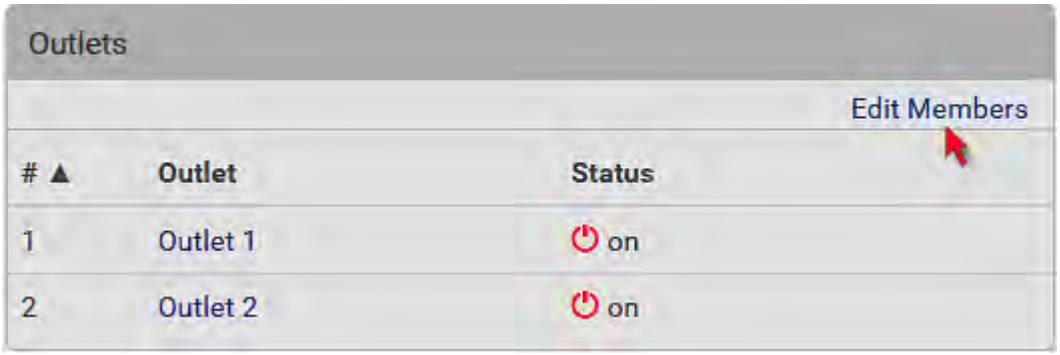
You can do the following on an individual outlet group's page:

- Change its member outlets
- Modify its group name

To open any outlet group's page, click on its name on the Outlet Groups page.

To modify the member outlets:

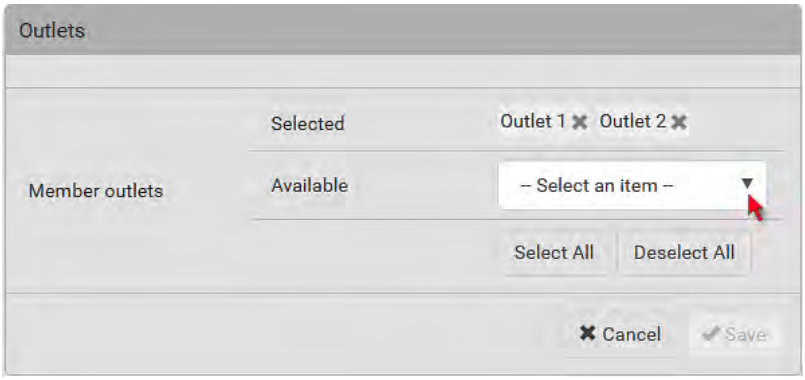
1. Click Edit Members.



2. Add or remove outlets of this group.
   - To select any outlet(s), select them one by one from the Available list.

Raritan
A brand of legrand

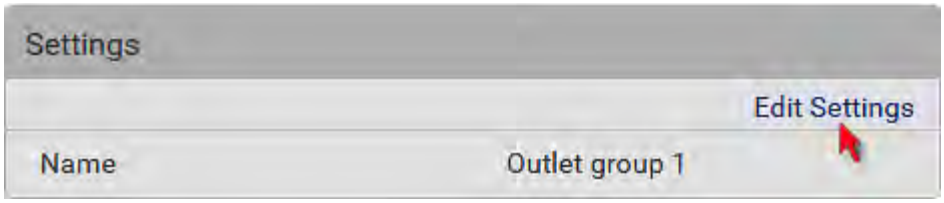
- To select all available outlets, click Select All.
- To remove any outlet(s) from the Selected field, click that outlet's ✖.
- To remove all outlets, click Deselect All.



3. Click Save.

To change the group name:

1. Click Edit Settings.



2. Type a new name.
3. Click Save.

Tip: PXC/PXO allows you to assign the same name to diverse outlet groups. If this really occurs, you still can identify different groups through their unique index numbers.

Deleting an Outlet Group

To delete an outlet group, you must have either permission below.

- Administrator Privileges
- Change Pdu, Inlet, Outlet & Overcurrent Protector Configuration

You can delete one or multiple outlet groups at a time.

To delete a single outlet group only, there are two methods -- either Outlet Groups page or individual group page.

To delete one or multiple groups on the Outlet Groups page:

This method allows you to delete more than one outlet group.

1. Click to make checkboxes appear in front of outlet groups.

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

2. Select multiple outlet groups.
3. To select ALL outlet groups, select the topmost checkbox in the header row.

4. Click > .
   - Confirm the operation when prompted.

Raritan
A brand of legrand

To delete a group on a specific outlet group's page:

This method allows you to delete ONLY one outlet group at a time.

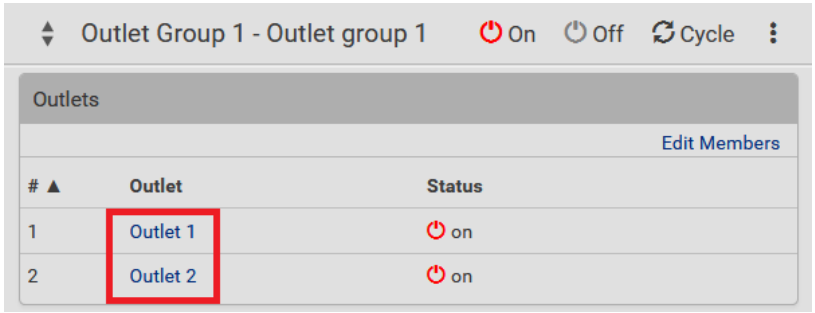
1. Open a specific outlet group's page by clicking on its name.

2. Click ⋮ > 🗑 Delete.
   - Confirm the operation when prompted.

Visiting Other Pages from Current Group

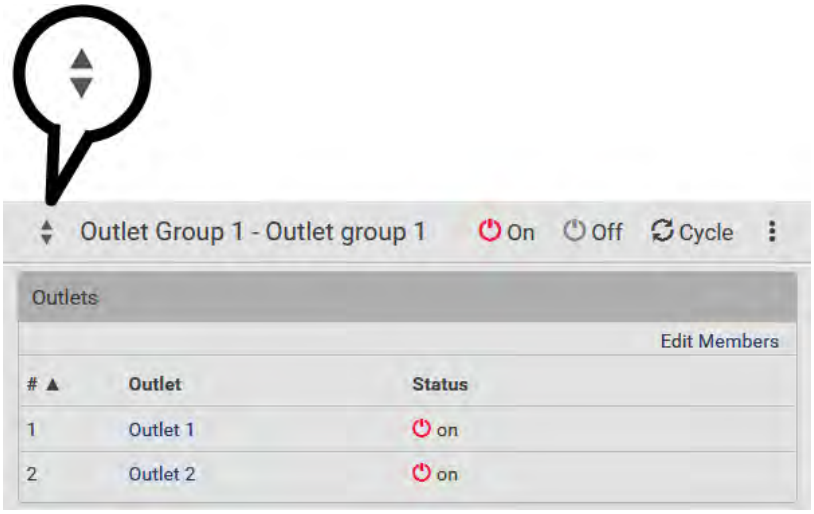
To visit a member outlet's page from the current page:

- On an outlet group's individual page, you can go to a member outlet's page easily. Just click the outlet links in the Outlets section.



To visit a different outlet group's page from the current page:

- On an outlet group's individual page, you can go to another outlet group's page easily. Just click the outlet selector on the top-left corner.



Raritan
A brand of legrand

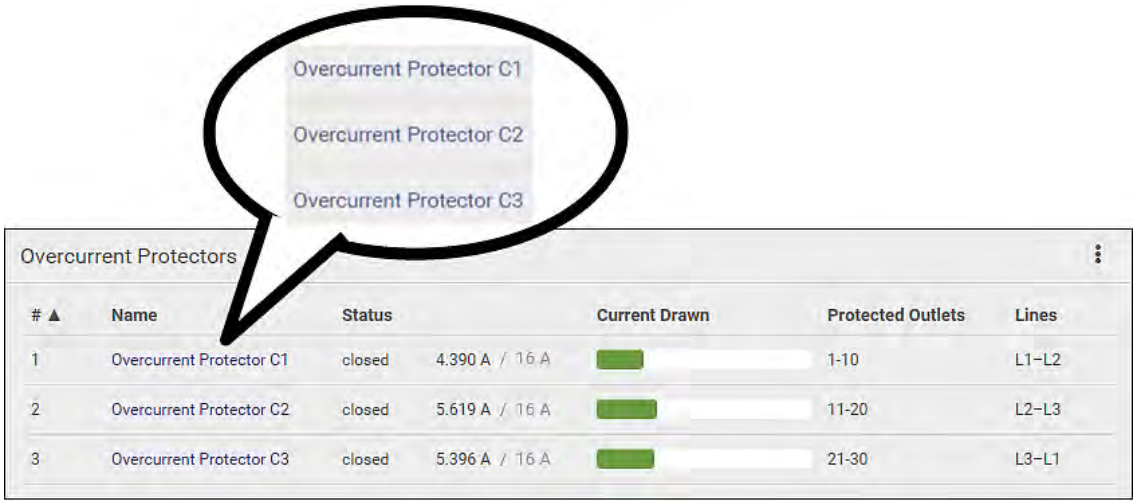
OCPs

The OCPs page is available only when your PXC/PXO 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 160).

To open the OCPs page, click 'OCPs' in the ***Menu*** (on page 103).

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 106).

Overcurrent protector overview:

- OCP status - open (tripped) or closed
- Current drawn, rated current and current bar
  - The smaller, gray text adjacent to "current drawn" is the rated current of each OCP.
  - 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.

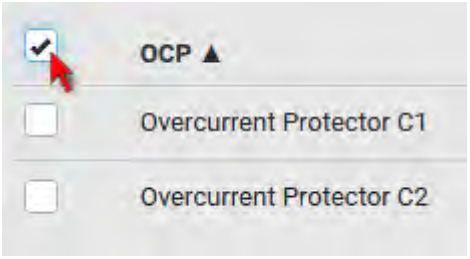
- Protected outlets, which are indicated with outlet numbers
- Associated lines

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 PXC/PXO automatically generate alert notifications for any warning or critical status. See ***Event Rules and Actions*** (on page 259).

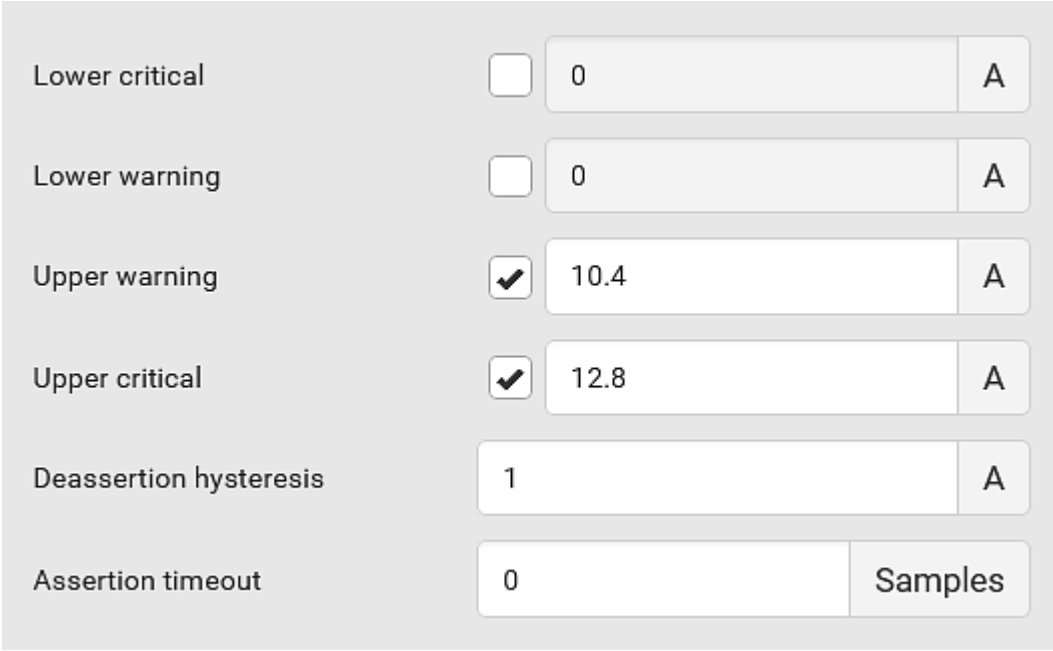
Note: By default, upper thresholds of an OCP's RMS current have been configured. See **Default Voltage and Current Thresholds** *(on page 684). You can modify them as needed.*

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.



For concepts of thresholds, deassertion hysteresis and assertion timeout, see ***Sensor Threshold Settings*** (on page 676).

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 147) or ***Dashboard*** (on page 107).

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.

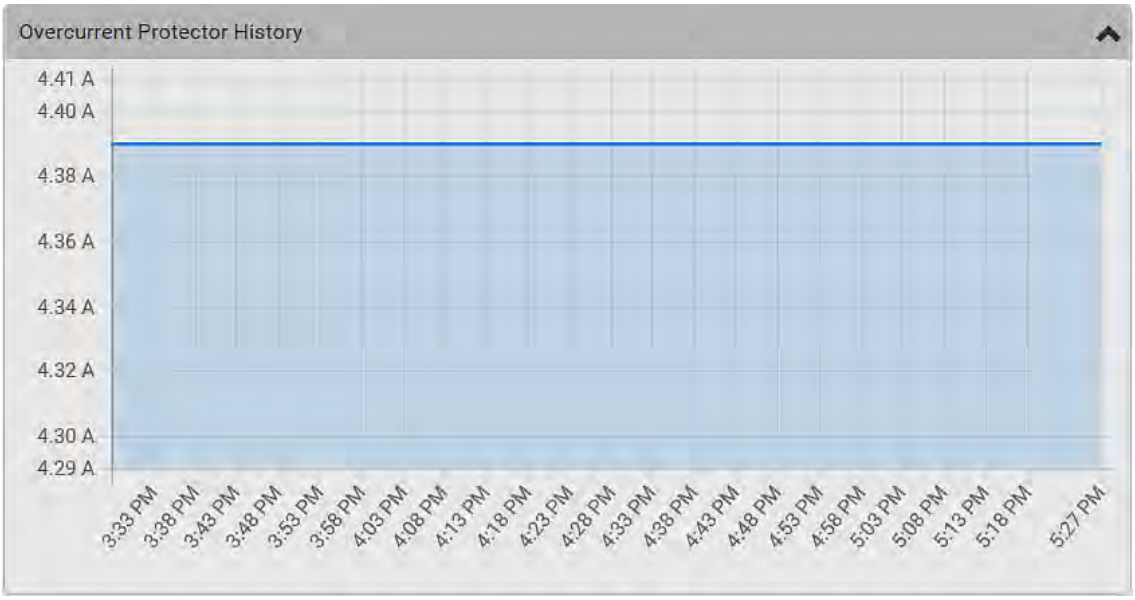
Field	Description
RMS current	This OCP's current state and readings, including current drawn and current remaining.

To customize this OCP's name:

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

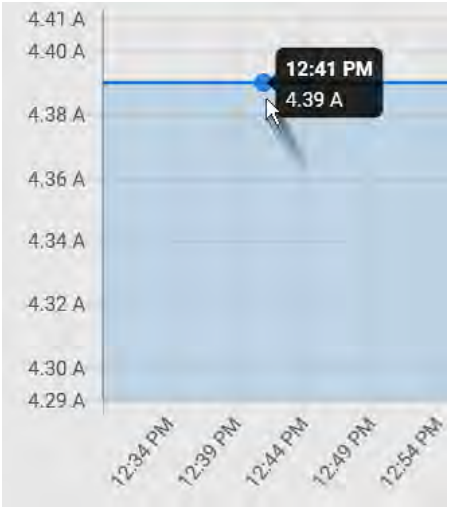
To view this OCP's RMS current chart:

This OCP's data chart is shown in the Overcurrent Protector History section.



Raritan
A brand of legrand

- 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.



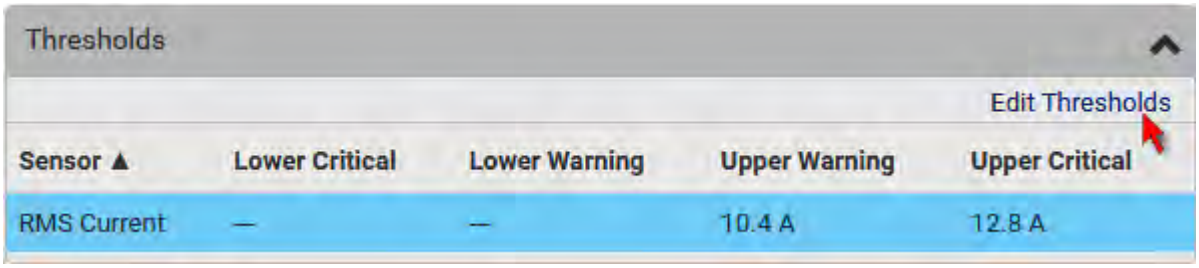
To configure this OCP's threshold settings:

By default, upper thresholds of an OCP's RMS current have been configured. See ***Default Voltage and Current Thresholds*** (on page 684). 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 147).*

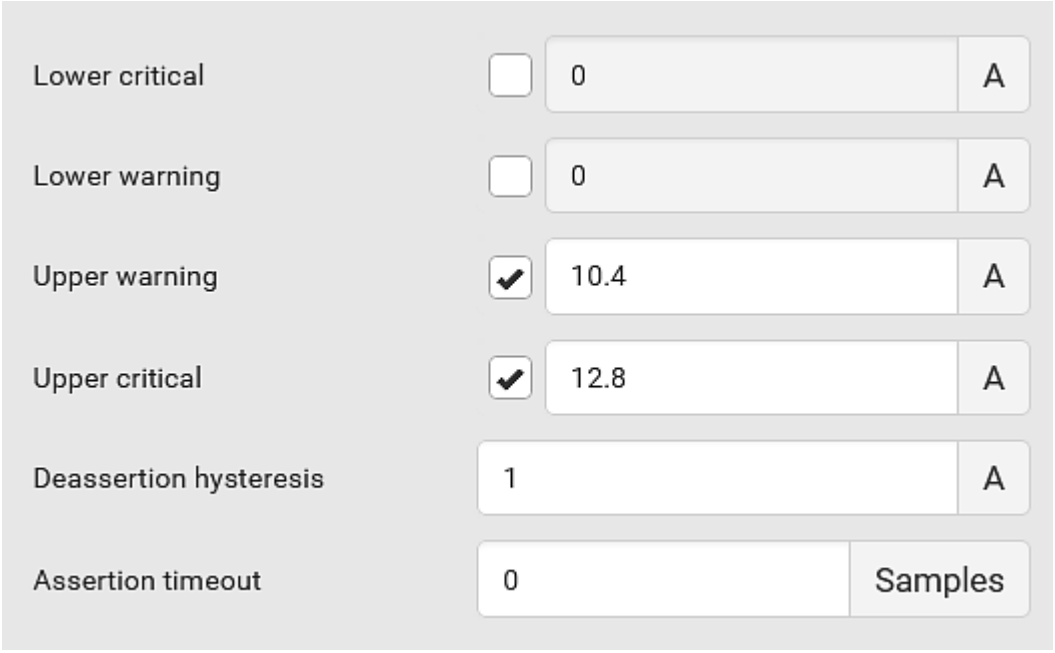
1. Click the Thresholds title bar at the bottom of the page to display the threshold data.

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



3. Make changes as needed.
   - To enable any threshold, select the corresponding checkbox.

- Type a new value in the accompanying text box.



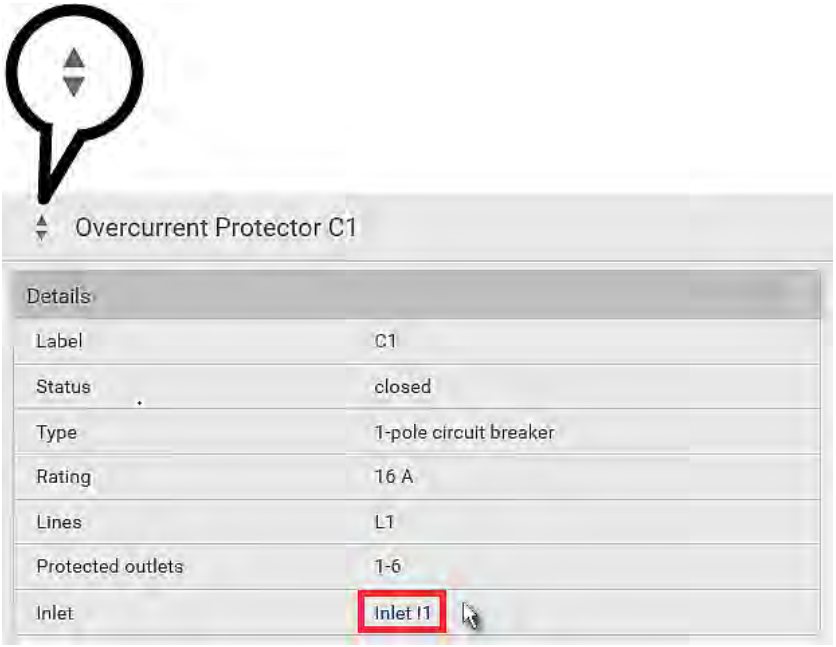
For concepts of thresholds, deassertion hysteresis and assertion timeout, see ***Sensor Threshold Settings*** (on page 676).

4. Click Save.

Raritan
A brand of legrand

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.



Peripherals

If there are Raritan environmental sensor packages connected to the PXC/PXO, they are listed on the Peripherals page. See ***Connecting Raritan Environmental Sensor Packages*** (on page 34).

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.

PXC/PXO 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 162).

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

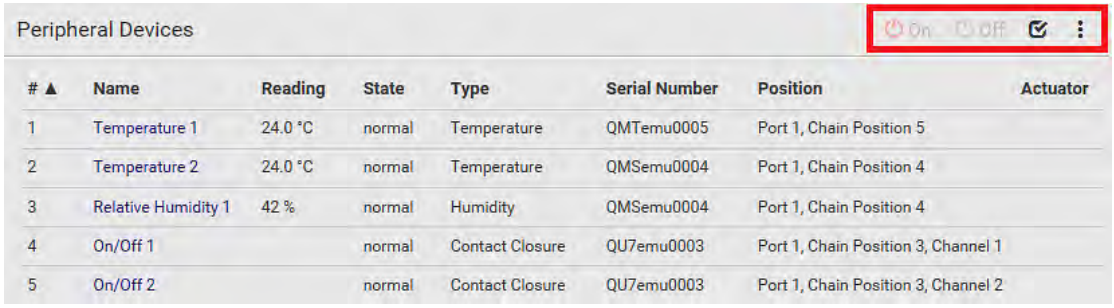
One PXC/PXO can manage a maximum of 32 sensors/actuators.

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

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

Open the Peripheral Devices page by clicking Peripherals in the ***Menu*** (on page 103). Then you can:

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



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

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

If wanted, you can resort the list by clicking the desired column header. See ***Sorting a List*** (on page 106).

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 160). An actuator is never highlighted.

Column	Description
Name	By default the PXC/PXO 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 169).
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 163).
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 164).

Column	Description
Position	The data indicates where this sensor or actuator is located in the sensor chain. See ***Identifying the Sensor Position and Channel*** (on page 165).
Actuator	Indicates whether this sensor package is an actuator or not. If yes, the symbol ✔ is shown.

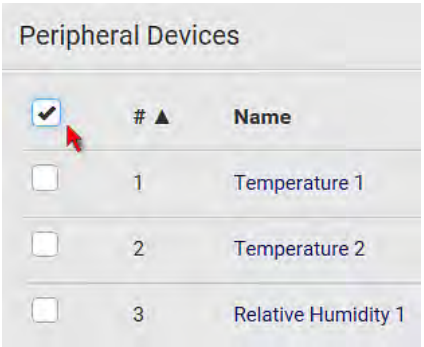
To release or manage sensors/actuators:

When the total of managed sensors/actuators reaches the maximum value, you cannot manage additional ones. The only way to manage any sensor/actuator is to release or replace the managed ones. To replace a managed sensor/actuator, see ***Managing One Sensor or Actuator*** (on page 167). 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 163).
   - To manage sensors/actuators, you must select "unmanaged" ones only.
   - To select ALL sensors/actuators, select the topmost checkbox in the header row.

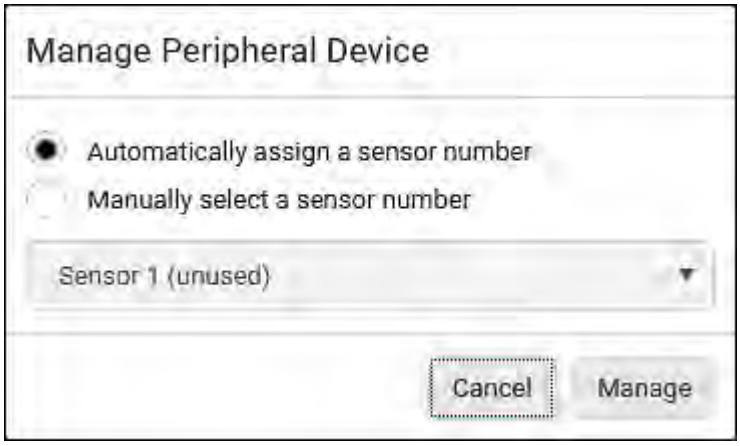


3. To release selected ones, click > Release.

   To manage them, click > Manage.

Raritan
A brand of legrand

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



- If you are managing only *one* sensor/actuator, you can choose to assign an ID number by selecting "Manually select a sensor number." See ***Managing One Sensor or Actuator*** (on page 167).

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

   Managed ones show one of the managed states.

To configure sensor/actuator-related settings:

1. Click ⋮ > Peripheral Device Setup.
2. Now you can configure the fields.
   - Click ▼ to select an option.
   - Adjust the numeric values.
   - Select or deselect the checkbox.

Field	Function	Note
Peripheral device Z coordinate format	Determines how to describe the vertical locations (Z coordinates) of Raritan environmental sensor packages. ▪ *Options: Rack units and Free-form* See ***Z Coordinate Format*** (on page 174).	To specify the location of any sensor/actuators in the data center, see ***Individual Sensor/Actuator Pages*** (on page 169).
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 167).

Field	Function	Note
Altitude	Specifies the altitude of PXC/PXO above sea level when a Raritan's differential air pressure sensor is attached. ▪ *Range: -425 to 3000 meters (-1394 to 9842 feet)* ▪ *Note that it can be a negative value down to -425 meters (-1394 feet) because some locations are below the sea level.*	▪ The device's altitude is associated with the altitude correction factor. See ***Altitude Correction Factors*** (on page 686). ▪ The default altitude measurement unit is meter. See ***Setting Default Measurement Units*** (on page 186). ▪ You can have the measurement unit vary between meter and foot according to user credentials. See ***Setting Your Preferred Measurement Units*** (on page 185).
Active powered dry contact limit	Determines the maximum number of "active" powered dry contact actuators that is permitted concurrently. ▪ *Range: 0 to 24* ▪ *Default:* 1	▪ An "active" actuator is the one that is turned ON, or, if with a door handle connected, is OPENED. ▪ This setting only applies to "powered dry contact" (PD) actuators rather than normal "dry contact" actuators. ▪ You need either 'Change Peripheral Device Configuration' privilege or 'Administrator Privileges' to change its upper limit. ▪ To turn on/off the connected actuators, see ***Peripherals*** (on page 154).

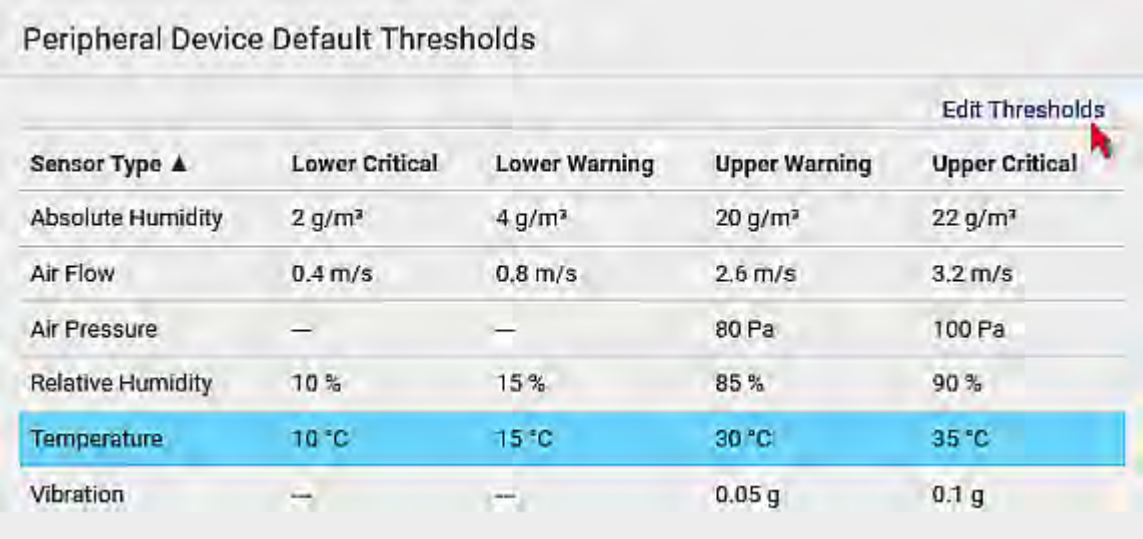
3. Click Save.
4. To return to the sensor list on the Peripheral Devices page, click "Peripheral Devices" on the top.

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 169).

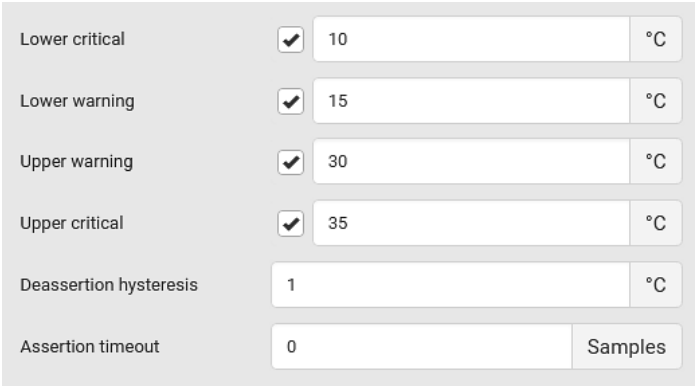
1. Click ⋮ > Default Threshold Setup.

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



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

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



   For concepts of thresholds, deassertion hysteresis and assertion timeout, see ***Sensor Threshold Settings*** (on page 676).

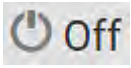
4. Click Save.

Tip: To customize the threshold settings on a per-sensor basis, go to **Individual Sensor/Actuator Pages** *(on page 169).*

To turn on or off any actuator(s):

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

: Turn ON.



: Turn OFF.

Note: Per default you can turn on as many dry contact actuators as you want, but only one "powered dry contact" actuator can be turned on at the same time. To change this limitation of "powered dry contact" actuators, modify the active powered dry contact setting. See **Peripherals** *(on page 154).*

4. Confirm the operation when prompted.

If you select a DX2-DH2C2 door handle lock, then the Open and Close buttons appear. For detailed operations, see ***Door Handle Status and Control*** (on page 374).

Tip: If intending to control the actuator via the front panel, see **Front Panel Settings** *(on page 323).*

Yellow- or Red-Highlighted Sensors

The PXC/PXO 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 676).

# ▲	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.

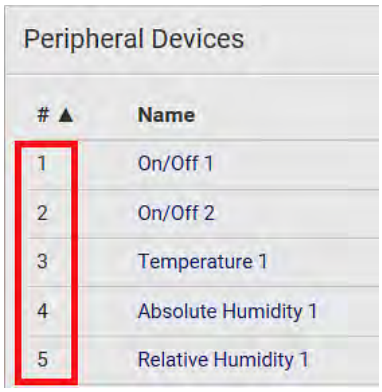
Sensor status	Color	States shown in the interface	Description
		unmanaged	Sensors are not being managed. See ***Managed vs Unmanaged Sensors/Actuators*** (on page 162).
Normal		normal	▪ Numeric or state sensors are within the normal range. -- OR -- ▪ No thresholds have been enabled for numeric sensors.
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 154).

Managed sensors/actuators:

- PXC/PXO 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.



- They show one of the managed states. See ***Sensor/Actuator States*** (on page 163).
- 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:

- PXC/PXO 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 PXC/PXO.

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

Raritan
A brand of legrand

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 160).

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

Managed sensor states:

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

State	Description
normal	▪ For numeric sensors, it means the readings are within the normal range. ▪ For state sensors, it means they enter the normal state.
below lower critical	"R" < Lower Critical threshold
below lower warning	Lower Critical threshold <= "R" < Lower Warning threshold
above upper warning	Upper Warning threshold < "R" <= Upper Critical threshold
above upper critical	Upper Critical threshold < "R"
alarmed	The state sensor enters the abnormal state.
unavailable	▪ Communication with the managed sensor is lost. -- OR -- ▪ DX2 DX, DPX2 or DPX3 sensor packages are upgrading their sensor firmware.

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

Managed actuator states:

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

Unmanaged sensor/actuator states:

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

Note: Unmanaged sensors or actuators will disappear from the web interface after they are no longer physically connected to the PXC/PXO. To manage a sensor/actuator, go to **Peripherals** *(on page 154).*

Finding the Sensor's Serial Number

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

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

Peripheral Devices

# ▲	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 DPX sensor packages cannot be daisy chained.

PXC/PXO can indicate where each sensor or actuator is connected on the Peripheral Devices page.

Peripheral Devices

# ▲	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 sensor hub is involved, the hub port information is also indicated for most sensors.

  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.

Raritan
A brand of legrand

How the Automatic Management Function Works

This setting is configured on ***Peripherals*** (on page 154).

After enabling the automatic management function:

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

PXC/PXO can manage up to 32 sensors/actuators.

After disabling the automatic management function:

PXC/PXO 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 154).

Managing One Sensor or Actuator

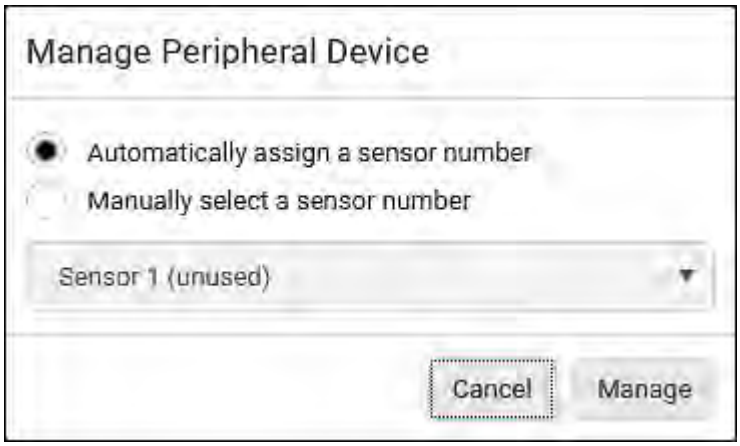
If you are managing only one sensor or actuator, you can assign the desired ID number to it. Note that you cannot assign ID numbers when managing multiple sensors/actuators at a time.

Tip: When the total of managed sensors/actuators reaches the maximum value, you cannot manage additional ones. The only way to manage any sensor/actuator is to release or replace the managed ones. To replace a managed one, assign an ID number to it by following the procedure below. To release any one, see **Peripherals** *(on page 154).*

To manage only one sensor/actuator:

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

2. The Manage Peripheral Device dialog appears.



   - To let PXC/PXO 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:

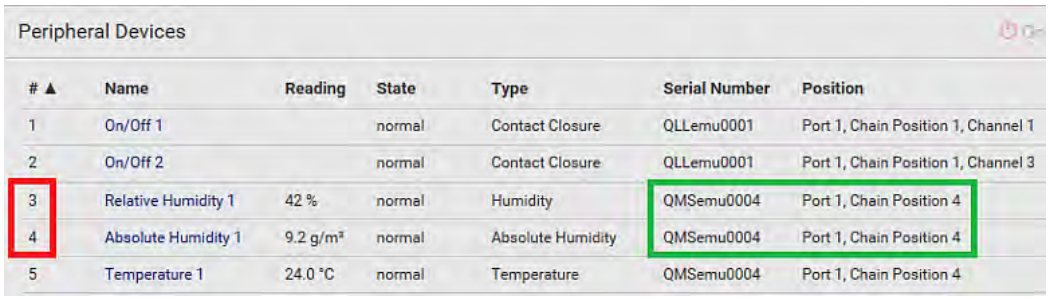
A Raritan humidity sensor is able to provide two measurements - relative and absolute humidity values.

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

Raritan
A brand of legrand

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

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 154).

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

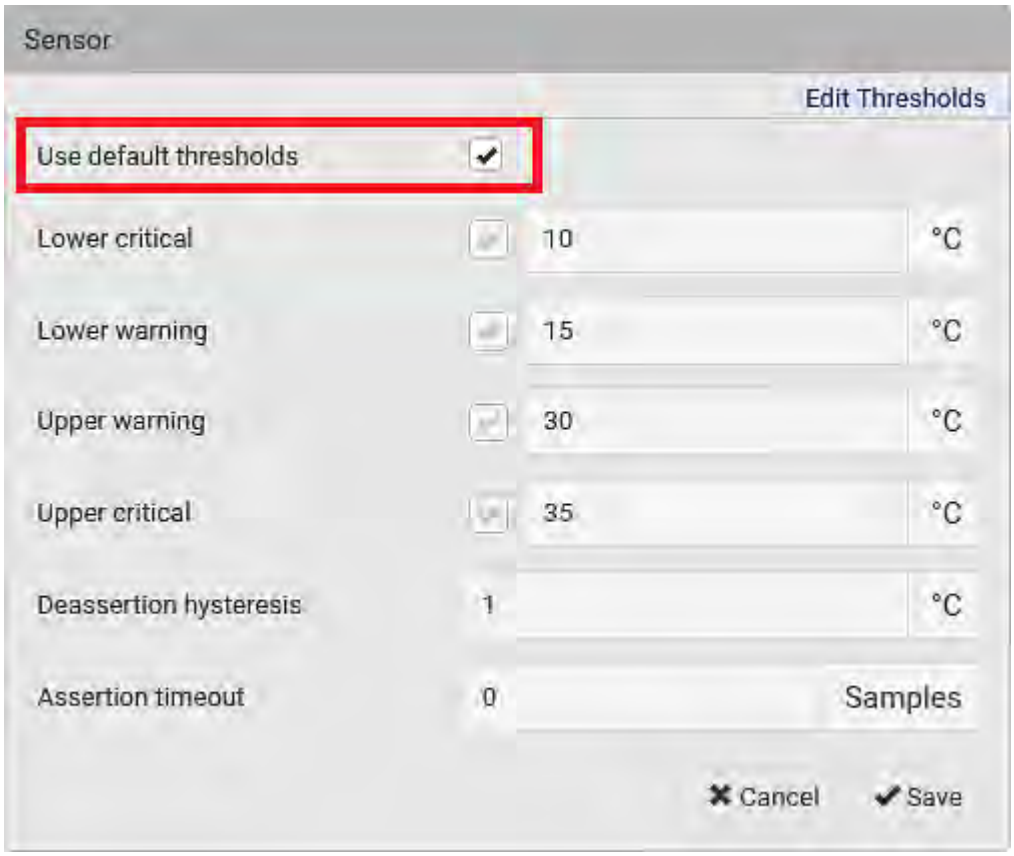
Threshold settings, if enabled, help you identify whether any numeric sensor enters the warning or critical level. See ***Yellow- or Red-Highlighted Sensors*** (on page 160). In addition, you can have PXC/PXO automatically generate alert notifications for any warning or critical status. See ***Event Rules and Actions*** (on page 259).

To configure a numeric sensor's threshold settings:

1. Click Edit Thresholds.

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

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



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

  The default threshold settings are configured on the page of ***Peripherals*** (on page 154).
- To customize the threshold settings for this particular sensor, deselect the 'Use default thresholds' checkbox, and then modify the threshold fields below it.

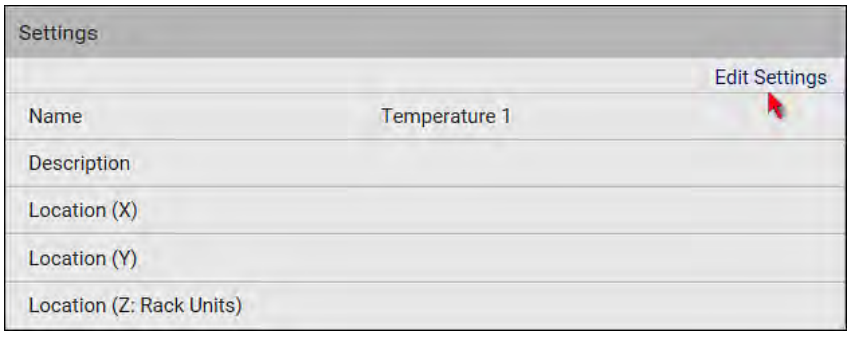
Note: For concepts of thresholds, deassertion hysteresis and assertion timeout, see **Sensor Threshold Settings** *(on page 676).*

3. Click Save.

Raritan
A brand of legrand

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

1. Click Edit Settings.



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

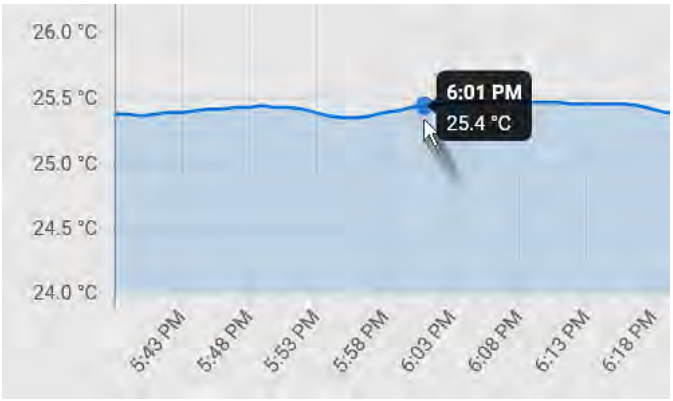
Fields	Description
Name	A name for the sensor or actuator.
Description	Any descriptive text you want.
Location (X, Y and Z)	Describe the sensor's or actuator's location in the data center by typing alphanumeric values for the X, Y and Z coordinates. See ***Sensor/Actuator Location Example*** (on page 175). If the term "Rack Units" appears in parentheses in the Z location, you must type an integer number. The Z coordinate's format is determined on the page of ***Peripherals*** (on page 154).
Alarmed to Normal Delay	This field is available for the DX-PIR presence detector only. It determines the wait time before the PXC/PXO announces that the presence detector is back to normal after it already returns to normal. Adjust the value in seconds.
Binary Sensor Subtype	This field is available for any Raritan contact closure sensor except for DX2-DH2C2's contact closure sensors. Determine the sensor type of your contact closure detector. ▪ *Contact Closure* detects the door lock or door open/closed status. ▪ *Smoke Detection* detects the appearance of smoke. ▪ *Water Detection* detects the appearance of water on the floor. ▪ *Vibration* detects the vibration of the floor.

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

To view a numeric sensor's chart

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

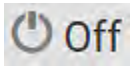
- To retrieve the exact data at a particular time, hover your mouse over the data line in the chart. Both the time and data are displayed as illustrated below.



To turn on or off an actuator:

1. Click the desired control button.

: Turn ON.



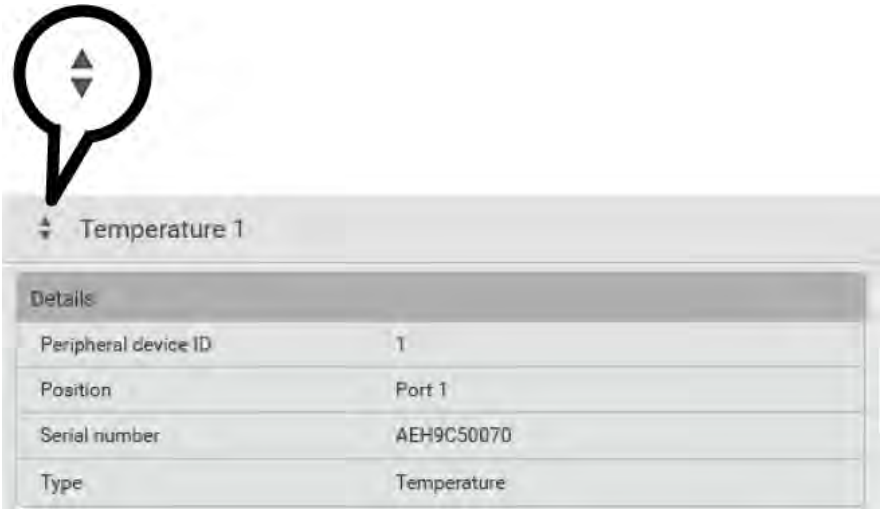
: Turn OFF.

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

Note: Per default you can turn on as many dry contact actuators as you want, but only one "powered dry contact" actuator can be turned on at the same time. To change this limitation of "powered dry contact" actuators, modify the active powered dry contact setting. See **Peripherals** *(on page 154).*

Other operations:

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



Z Coordinate Format

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

For a Z coordinate example, see ***Sensor/Actuator Location Example*** (on page 175).

To configure Z coordinates:

1. Determine the Z coordinate format on ***Peripherals*** (on page 154). 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.

Raritan
A brand of legrand

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

2. Configure Z coordinates on the ***Individual Sensor/Actuator Pages*** (on page 169).

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 169).

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

Example:

X = `Brown Cabinet Row`

Y = `Third Rack`

Z = `Top of Cabinet`

Values of the X, Y and Z coordinates:

- X and Y: They can be any alphanumeric values comprising 0 to 24 characters.
- Z: When the Z coordinate format is set to *Rack units*, it can be any number ranging from 0 to 60. When its format is set to *Free-form*, it can be any alphanumeric value comprising 0 to 24 characters. See ***Peripherals*** (on page 154).

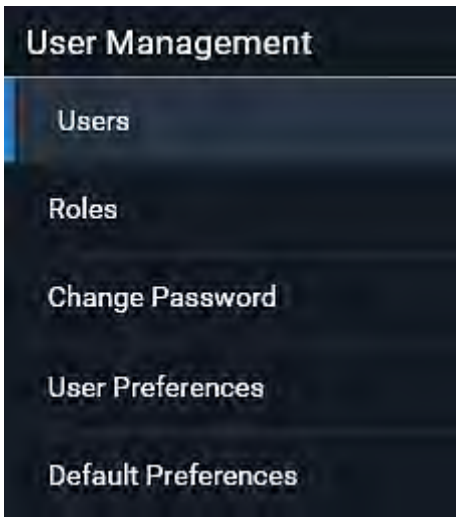
User Management

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

PXC/PXO 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 **must** change its password.

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

Click 'User Management' in the ***Menu*** (on page 103), and the following submenu displays.



Submenu command	Refer to...
Users	***Creating Users*** (on page 177)
Roles	***Creating Roles*** (on page 182)
Change Password	***Changing Your Password*** (on page 98)
User Preferences	***Setting Your Preferred Measurement Units*** (on page 185)
Default Preferences	***Setting Default Measurement Units*** (on page 186)

Raritan
A brand of legrand

Creating Users

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

To add users, choose User Management > Users > .

User information:

Field/setting	Description
User name	The name the user enters to log in to the PXC/PXO. ▪ 4 to 32 characters ▪ Case sensitive ▪ Colon character and spaces are NOT permitted.
Full name	The user's first and last names.
Password, Confirm password	▪ 4 to 64 characters ▪ Case sensitive ▪ Spaces are permitted.
Telephone number	The user's telephone number
Email address	The user's email address ▪ Up to 128 characters ▪ Case sensitive
Enable	When selected, the user can log in to the PXC/PXO.
Force password change on next login	When selected, a password change request automatically appears the next time the user logs in. For details, see ***Changing Your Password*** (on page 98).

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 222).

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 219).*
Security level	Click the field to select a preferred security level from the list: ▪ None: No authentication and no privacy. This is the default. ▪ Authentication: Authentication and no privacy. ▪ Authentication & Privacy: Authentication and privacy.

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

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

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

Field/setting	Description
Same as authentication password	Select this checkbox if the privacy password is identical to the authentication password. To specify a different privacy password, disable the checkbox.

Raritan
A brand of legrand

Field/setting	Description
Password, Confirm password	Type the privacy password if the 'Same as Authentication Password' checkbox is deselected. The password must consist of 8 to 32 ASCII printable characters.

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

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

Preferences:

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

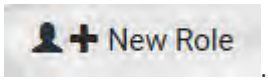
Field	Description
Temperature unit	Preferred units for temperatures -- °C (Celsius) or °F (Fahrenheit).
Length unit	Preferred units for length or height -- Meter or Feet.
Pressure unit	Preferred units for pressure -- Pascal or Psi. ▪ Pascal = one newton per square meter ▪ Psi = pounds per square inch

Note: Users can change the measurement units at any time by setting their own preferences. See **Setting Your Preferred Measurement Units** *(on page 185).*

Roles:

Select one or multiple roles to determine the user's permissions.

To select all roles, select the topmost checkbox in the header row. However, a user can have a maximum of 32 roles only.

If the built-in roles do not satisfy your needs, add new roles by clicking 

. This newly-created role will be then automatically assigned to the user account currently being created. See ***Creating Roles*** (on page 182).

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 PXC/PXO is outlet-switching capable) • Switch Outlet Group (if your PXC/PXO 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.

Raritan
A brand of legrand

Editing or Deleting Users

To edit or delete users, choose User Management > Users to open the Users page, which lists all users.

In the Enabled column:

- ✔: The user is enabled.
- ✖: The user is disabled.

If wanted, you can resort the list by clicking the desired column header. See ***Sorting a List*** (on page 106).

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 177).
   - To change the password, type a new password in the Password and Confirm Password fields. If the password field is left blank, the password remains unchanged.
   - To delete this user, click 🗑, and confirm the operation.

3. Click Save.

To delete multiple user accounts:

1. On the Users page, click to make checkboxes appear in front of user names.

   Tip: To delete only one user, you can simply click that user without making the checkboxes appear. Refer to the above procedure.

2. Select one or multiple users.
   - To select all roles, except for the admin user, select the topmost checkbox in the header row.
3. Click .

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 PXC/PXO provides two built-in roles.

Built-in role	Description
Admin	Provide full permissions.

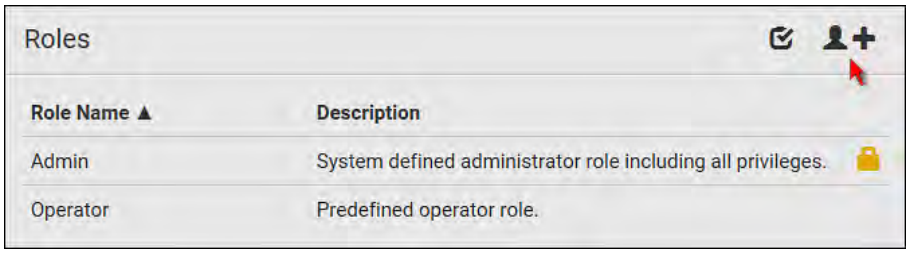
Raritan
A brand of legrand

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

If the two do not satisfy your needs, add new roles. PXC/PXO supports up to 64 roles.

To create a role:

1. Choose User Management > Roles > .

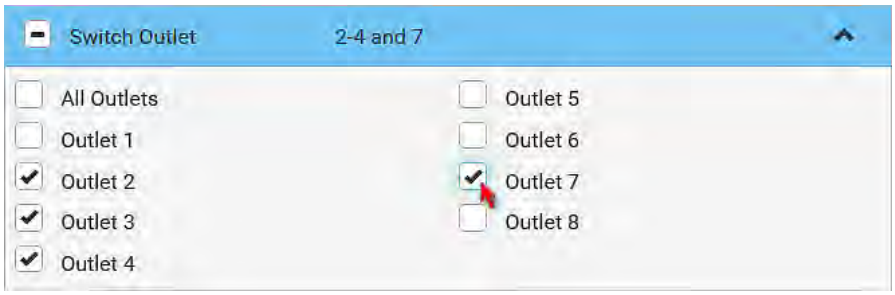


2. Assign a role name.
   - 1 to 32 characters long
   - Case sensitive
   - Spaces are permitted
3. Type a description for the role in the Description field.
4. Select the desired privilege(s).
   - The 'Administrator Privileges' includes all privileges.
   - The 'Unrestricted View Privileges' includes 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.



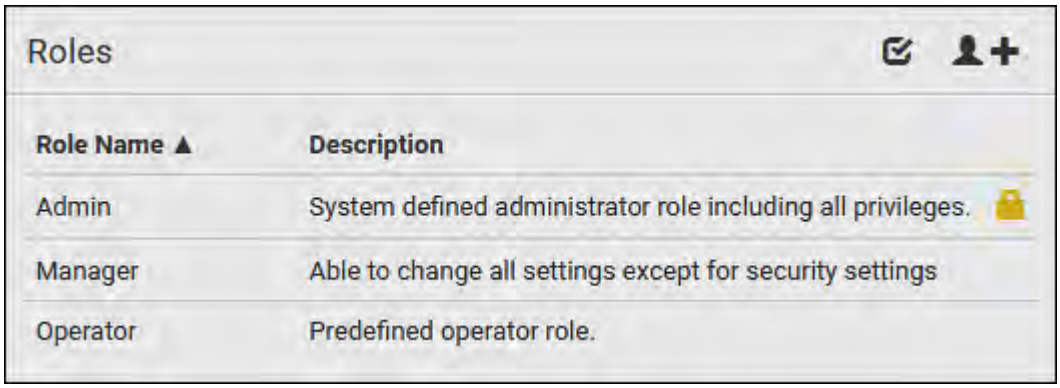
6. Click Save.

Now you can assign the role to any user. See ***Creating Users*** (on page 177) or ***Editing or Deleting Users*** (on page 181).

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 106).



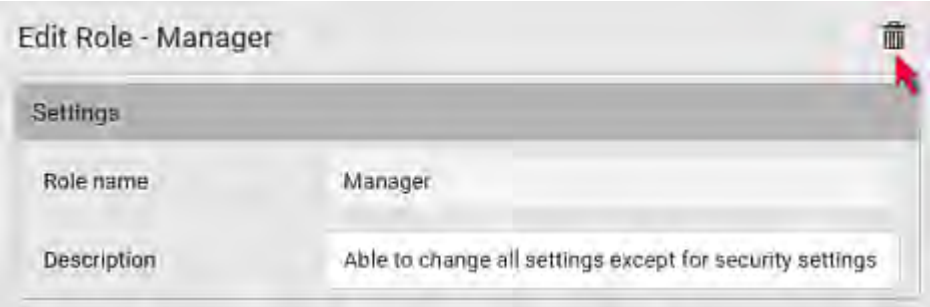
The Admin role is not user-configurable so the lock icon displays, indicating that you are not allowed to configure it.

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.

Raritan
A brand of legrand

- To delete this role, click , and confirm the operation.



3. Click Save.

To delete any roles:

1. On the Roles page, click to make checkboxes appear in front of roles.

Tip: To delete only one role, you can simply click that role without making the checkboxes appear. Refer to the above procedure.

2. Select one or multiple roles.
   - To select all roles, except for the Admin role, select the topmost checkbox in the header row.
3. Click 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 PXC/PXO 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 181).*

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 186).

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).

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

3. Click Save.

Setting Default Measurement Units

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

For a list of affected user interfaces, see ***User Interfaces Showing Default Units*** (on page 187). 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 185) or* **Creating Users** *(on page 177).*

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.

Raritan
A brand of legrand

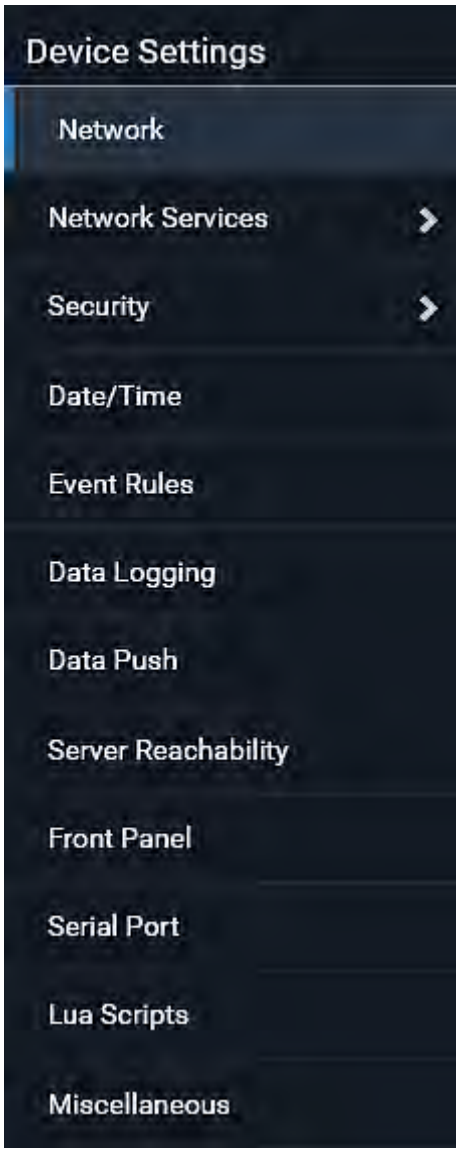
User Interfaces Showing Default Units

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 177).
- 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 283).
- Front panel LCD display.

Device Settings

Click 'Device Settings' in the ***Menu*** (on page 103), and the following submenu displays.



Menu command	Submenu command	Refer to...
Network		***Configuring Network Settings*** (on page 190)
Network Services	HTTP	***Changing HTTP(S) Settings*** (on page 217)
	SNMP	***Configuring SNMP Settings*** (on page 219)

Raritan
A brand of legrand

Menu command	Submenu command	Refer to...
	SMTP Server	***Configuring SMTP Settings*** (on page 221)
	SSH	***Changing SSH Settings*** (on page 222)
	Telnet	***Changing Telnet Settings*** (on page 223)
	Modbus	***Changing Modbus Settings*** (on page 223)
	Server Advertising	***Enabling Service Advertising*** (on page 226)
Security	IP Access Control	***Creating IP Access Control Rules*** (on page 228)
	Role Based Access Control	***Creating Role Based Access Control Rules*** (on page 232)
	TLS Certificate	***Setting Up a TLS Certificate*** (on page 234)
	Authentication	***Setting Up External Authentication*** (on page 239)
	Login Settings	***Configuring Login Settings*** (on page 247)
	Password Policy	***Configuring Password Policy*** (on page 248)
	Service Agreement	***Enabling the Restricted Service Agreement*** (on page 249)
Date/Time		***Setting the Date and Time*** (on page 251)
Event Rules		***Event Rules and Actions*** (on page 259)
Data Logging		***Setting Data Logging*** (on page 310)
Data Push		***Configuring Data Push Settings*** (on page 311)
Server Reachability		***Monitoring Server Accessibility*** (on page 316)
Front Panel		***Front Panel Settings*** (on page 323)
Serial Port		***Configuring the Serial Port*** (on page 324)
Lua Scripts		***Lua Scripts*** (on page 324)
Miscellaneous		***Miscellaneous*** (on page 329)

Configuring Network Settings

Configure wired, wireless, and Internet protocol-related settings on the Network page after ***Connecting the PXC/PXO to Your Network*** (on page 12).

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

However, PXC/PXO 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 193).
   - 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 207) and ***Static Route Examples*** (on page 203).
3. To configure IPv4/IPv6 settings for a *wired* network, click the ETH1/ETH2 or BRIDGE section. See ***Wired Network Settings*** (on page 191).
   - 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 197).
   - You must connect a USB wireless LAN adapter to the PXC/PXO 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 194).
6. Click Save.

Raritan
A brand of legrand

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: PXC/PXO disables TLS 1.0 *and* 1.1 *by default. It enables only TLS* 1.2 *and* 1.3.

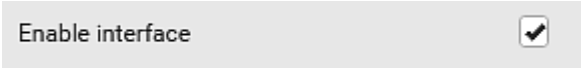
Wired Network Settings

On the Network page, click the ETH1/ETH2 section to configure IPv4/IPv6 settings.

If the device's cascading mode is set to 'Bridging', the BRIDGE section appears. Then you must click the BRIDGE section for IPv4/IPv6 settings. See ***Setting the Cascading Mode*** (on page 207).

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.



IPv4 settings:

Field/setting	Description
Enable IPv4	Enable or disable the IPv4 protocol.
IP auto configuration	Select the method to configure IPv4 settings. ▪ *DHCP*: Auto-configure IPv4 settings via DHCP servers. ▪ *Static*: Manually configure the IPv4 settings.
Preferred hostname	Enter the hostname you prefer for IPv4 connectivity

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

  Example: *192.168.84.99/24*

IPv6 settings:

Field/setting	Description
Enable IPv6	Enable or disable the IPv6 protocol.
IP auto configuration	Select the method to configure IPv6 settings. ▪ *Automatic*: Auto-configure IPv6 settings via DHCPv6. ▪ *Static*: Manually configure the IPv6 settings.
Preferred hostname	▪ Enter the hostname you prefer for IPv6 connectivity

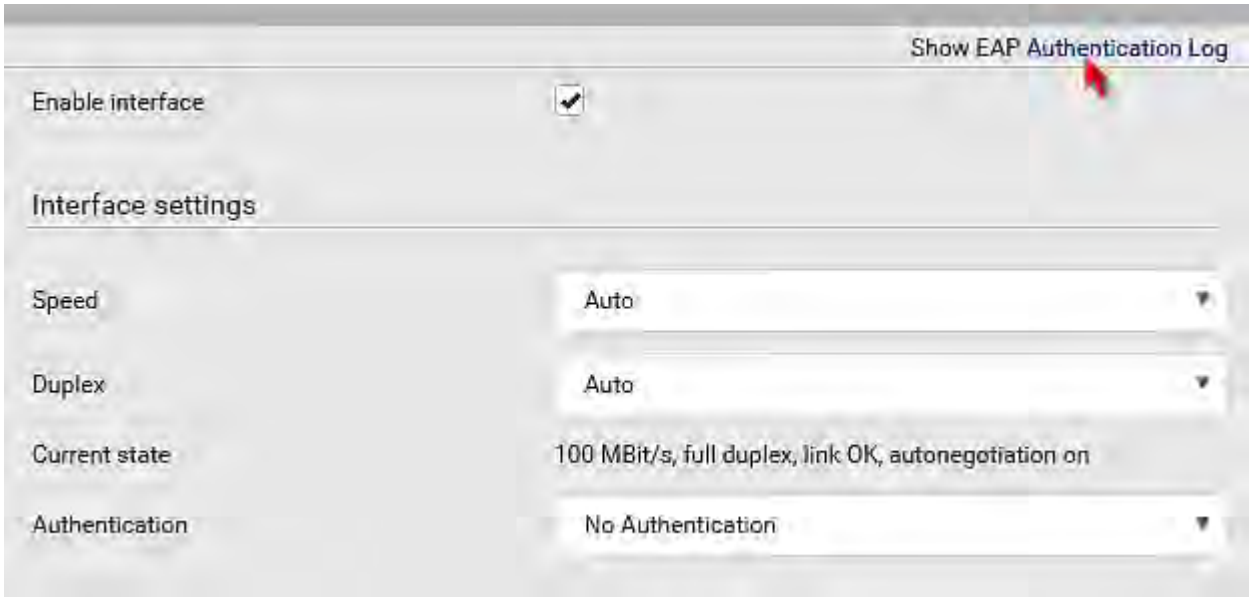
- **Automatic settings:** Optionally specify the preferred hostname, which must meet the above requirements.
- **Static settings:** Assign a static IPv6 address, which follows this syntax "IP address/prefix length".

  Example: *fd07:2fa:6cff:1111::0/128*

Raritan
A brand of legrand

(Optional) To view the diagnostic log for EAP authentication:

- Click Show EAP Authentication Log. See ***Diagnostic Log for Network Connections*** (on page 202).



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 PXC/PXO Devices for Sharing Ethernet Connectivity*** (on page 24) ▪ ***Setting the Cascading Mode*** (on page 207)
DNS resolver preference	Determine which IP address is used when the DNS resolver returns both IPv4 and IPv6 addresses. ▪ IPv4 address: Use the IPv4 addresses. ▪ IPv6 address: Use the IPv6 addresses.
DNS suffixes (optional)	Specify a DNS suffix name if needed.

Field	Description
First/Second/Third DNS server	Manually specify static DNS server(s). ▪ If any static DNS server is specified in these fields, it will override the DHCP-assigned DNS server. ▪ If DHCP (or Automatic) is selected for IPv4/IPv6 settings, and there are NO static DNS servers specified, the PXC/PXO will use DHCP-assigned DNS servers.
IPv4/IPv6 routes	You need to configure these settings only when your local network contains two subnets, and you want PXC/PXO 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 203).

Ethernet Interface Settings

By default both ETH1 and ETH2 interfaces on PXC/PXO are enabled.

Enable Interface:

Make sure the Ethernet interface is enabled, or all networking through this interface fails. This setting is available in the ETH1/ETH2 section, but not available in the BRIDGE section.

Other Ethernet settings:

Field	Description
Speed	Select a LAN speed. • *Auto:* System determines the optimum LAN speed through auto-negotiation. • *10 MBit/s:* Speed is always 10 Mbps. • *100 MBit/s:* Speed is always 100 Mbps.
Duplex	Select a duplex mode. • *Auto:* The PXC/PXO selects the optimum transmission mode through auto-negotiation. • *Full:* Data is transmitted in both directions simultaneously.

Raritan
A brand of legrand

Field	Description
	• *Half:* Data is transmitted in one direction (to or from the PXC/PXO) at a time.
Current state	Show the LAN's current status, including the current speed and duplex mode.
MTU	▪ Set the MTU from 1280 to 1500.
Authentication	Select an authentication method. ▪ *No Authentication:* No authentication data is required. ▪ *EAP:* Use Protected Extensible Authentication Protocol. Enter required authentication data in the fields that appear.
Outer authentication	This field appears when 'EAP' is selected. There are two authentication methods for EAP. ▪ *PEAP:* A TLS tunnel is established, and an inner authentication method can be specified for this tunnel. ▪ *TLS:* Authentication between the client and authentication server is performed using TLS certificates.
Inner authentication	This field appears when both 'EAP' and 'PEAP' are selected. ▪ *MS-CHAPv2:* Authentication based on the given password using MS-CHAPv2 protocol. ▪ *TLS:* Authentication between the client and authentication server is performed using TLS certificates.
Identity	This field appears when 'EAP' is selected. Type your user name.
Password	This field appears only when 'EAP', 'PEAP' and 'MS-CHAPv2' are all selected. Type your password.

Field	Description
Client certificate, Client private key, Client private key password	This field appears when 'EAP', 'PEAP' and 'TLS' are all selected. PEM encoded X.509 certificate and PEM encoded private key are required for certification-based authentication methods. Private key password is optional. ▪ PXC/PXO supports private keys of PKCS#1 and PKCS#8 formats. ▪ Client Private Key Password should be entered only when your private key is encrypted with a password. ▪ To view the uploaded certificate, click Show Client Certificate. ▪ To remove the uploaded certificate and private key, click 'Clear Key/Certificate selection'.
CA certificate	This field appears when 'EAP' is selected. A third-party CA certificate may or may not be needed. If needed, follow the steps below.
RADIUS authentication server name	This field appears when 'EAP' is selected. Type the name of the RADIUS server if it is present in the TLS certificate. ▪ The name must match the fully qualified domain name (FQDN) of the host shown in the certificate.

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

Raritan
A brand of legrand

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 207).

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 PXC/PXO 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.
MTU	Set the MTU from 1280 to 1500.
Enable High Throughput (802.11n)	Enable or disable 802.11n protocol.
Authentication	Select an authentication method. ▪ *No Authentication:* No authentication data is required. ▪ *PSK*: A Pre-Shared Key is required. ▪ *EAP:* Use Protected Extensible Authentication Protocol. Enter required authentication data in the fields that appear.
Pre-Shared Key	This field appears only when PSK is selected. Type the PSK string.

Field/setting	Description
Outer authentication	This field appears when 'EAP' is selected. There are two authentication methods for EAP. ▪ *PEAP:* A TLS tunnel is established, and an inner authentication method can be specified for this tunnel. ▪ *TLS:* Authentication between the client and authentication server is performed using TLS certificates.
Inner authentication	This field appears when both 'EAP' and 'PEAP' are selected. ▪ *MS-CHAPv2:* Authentication based on the given password using MS-CHAPv2 protocol. ▪ *TLS:* Authentication between the client and authentication server is performed using TLS certificates.
Identity	This field appears when 'EAP' is selected. Type your user name.
Password	This field appears only when 'EAP', 'PEAP' and 'MS-CHAPv2' are all selected. Type your password.

Raritan
A brand of legrand

Field/setting	Description
Client certificate, Client private key, Client private key password	This field appears when 'EAP', 'PEAP' and 'TLS' are all selected. PEM encoded X.509 certificate and PEM encoded private key are required for certification-based authentication methods. Private key password is optional. ▪ PXC/PXO supports private keys of PKCS#1 and PKCS#8 formats. ▪ Client Private Key Password should be entered only when your private key is encrypted with a password. ▪ To view the uploaded certificate, click Show Client Certificate. ▪ To remove the uploaded certificate and private key, click 'Clear Key/Certificate selection'.
CA certificate	This field appears when 'EAP' is selected. A third-party CA certificate may or may not be needed. If needed, follow the steps below.
RADIUS authentication server name	This field appears when 'EAP' is selected. Type the name of the RADIUS server if it is present in the TLS certificate. ▪ The name must match the fully qualified domain name (FQDN) of the host shown in the certificate.

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

If the required certificate file is a chain of certificates, and you are not sure about the requirements of a certificate chain, see ***TLS Certificate Chain*** (on page 702).

Field/setting	Description
Enable verification of TLS certificate chain	Select this checkbox for the PXC/PXO to verify the validity of the TLS certificate that will be installed. ▪ For example, the PXC/PXO will check the certificate's validity period against the system time.

Field/setting	Description
Browse...	Click this button to import a certificate file. Then you can: ▪ Click Show to view the certificate's content. ▪ Click Remove to delete the installed certificate if it is inappropriate.
Allow expired and not yet valid certificates	▪ Select this checkbox to make the authentication succeed regardless of the certificate's validity period. ▪ After deselecting this checkbox, the authentication fails whenever any certificate in the selected certificate chain is outdated or not valid yet.
Allow connection if system clock is incorrect	When this checkbox is deselected, and if the system time is incorrect, the installed TLS certificate is considered not valid yet and will cause the wireless network connection to fail. When this checkbox is selected, it will make the wireless network connection successful when the PXC/PXO system time is earlier than the firmware build before synchronizing with any NTP server. ▪ The incorrect system time issue may occur when the PXC/PXO has once been powered off for a long time.

IPv4 settings:

Field/setting	Description
Enable IPv4	Enable or disable the IPv4 protocol.
IP auto configuration	Select the method to configure IPv4 settings. ▪ *DHCP*: Auto-configure IPv4 settings via DHCP servers. ▪ *Static*: Manually configure the IPv4 settings.
Preferred hostname	Enter the hostname you prefer for IPv4 connectivity

- **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

Raritan
A brand of legrand

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

  Example: *192.168.84.99/24*

IPv6 settings:

Field/setting	Description
Enable IPv6	Enable or disable the IPv6 protocol.
IP auto configuration	Select the method to configure IPv6 settings. ▪ *Automatic*: Auto-configure IPv6 settings via DHCPv6. ▪ *Static*: Manually configure the IPv6 settings.
Preferred hostname	▪ Enter the hostname you prefer for IPv6 connectivity

- **Automatic settings:** Optionally specify the preferred hostname, which must meet the above requirements.
- **Static settings:** Assign a static IPv6 address, which follows this syntax "IP address/prefix length".

  Example: *fd07:2fa:6cff:1111::0/128*

(Optional) To view the wireless LAN diagnostic log:

- Click Show WLAN Diagnostic Log. See ***Diagnostic Log for Network Connections*** (on page 202).

Diagnostic Log for Network Connections

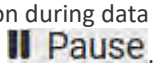
PXC/PXO provides a diagnostic log for inspecting connection errors that occurred during the EAP authentication or the wireless network connection. The information is useful for technical support.

Note that the diagnostic log shows data only after connection errors are detected.

Each entry in the log consists of:

- ID number
- Date and time
- Description

To view the log:

1. Access the diagnostic log with either method below.
   - Choose Device Settings > Network > ETH1/ETH2 > Show EAP Authentication Log. See ***Configuring Network Settings*** (on page 190).
   - Choose Device Settings > Network > WIRELESS > Show WLAN Diagnostic Log.
2. The log is refreshed automatically at a regular interval of five seconds. To avoid any new events' interruption during data browsing, you can suspend the automatic update by clicking 

.
   - To restore automatic update, click

. 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.

4. If wanted, you can resort the list by clicking the desired column header. See ***Sorting a List*** (on page 106).

To clear the diagnostic log:

1. On the top-right corner of the log, click

.
2. Click Clear Log on the confirmation message.

Raritan
A brand of legrand

Static Route Examples

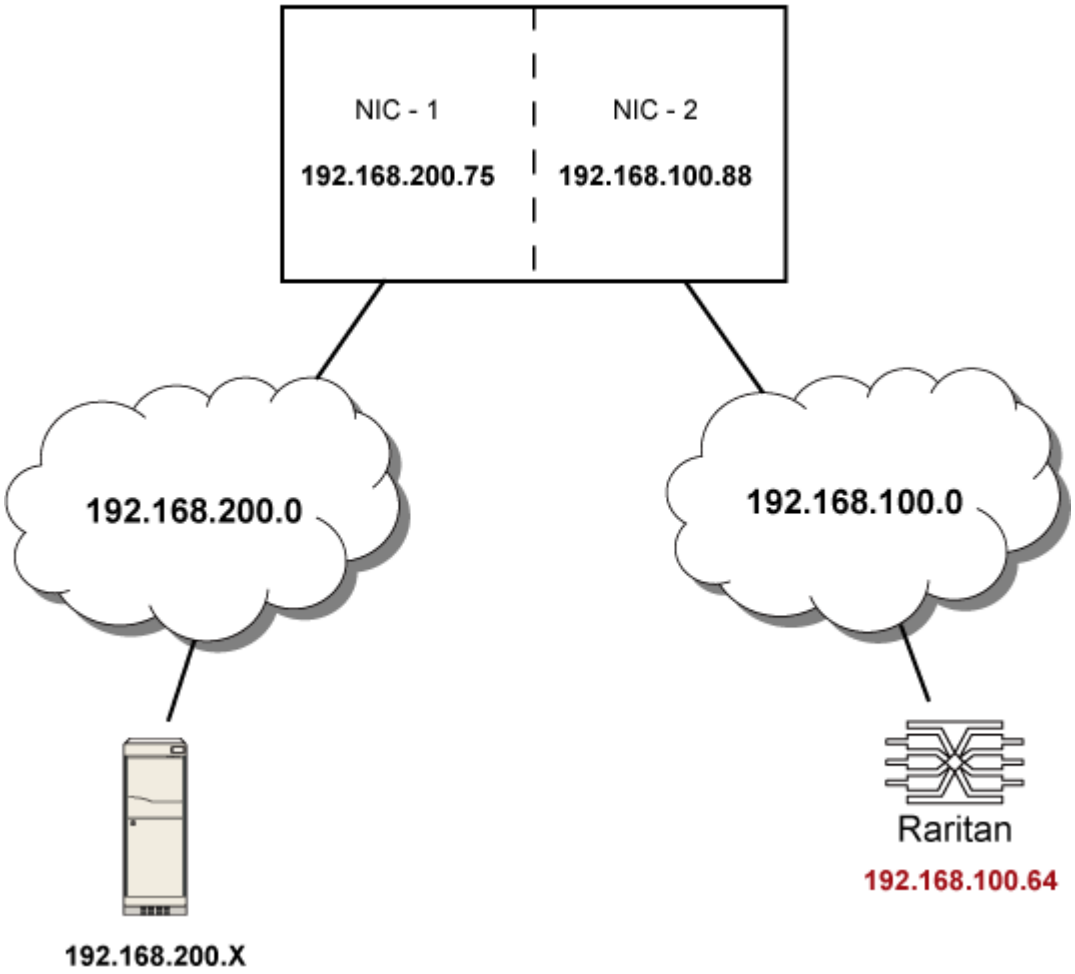
This section describes two static route examples: IPv4 and IPv6. Both examples assume that two network interface controllers (NIC) have been installed in one network server, leading to two available subnets, and IP forwarding has been enabled. All of the NICs and PXC/PXO devices in the examples use static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

Most of local multiple networks are not directly reachable and require the use of a gateway. Therefore, we will select Gateway in the following examples. If your local multiple networks are directly reachable, you should select Interface rather than Gateway.

Note: If Interface is selected, you should select an interface name instead of entering an IP address. See **Interface Names** *(on page 206).*

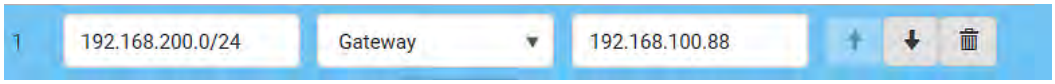
IPv4 example:

- Your PXC/PXO: *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 PXC/PXO to communicate with any device in the other subnet 192.168.200.0.

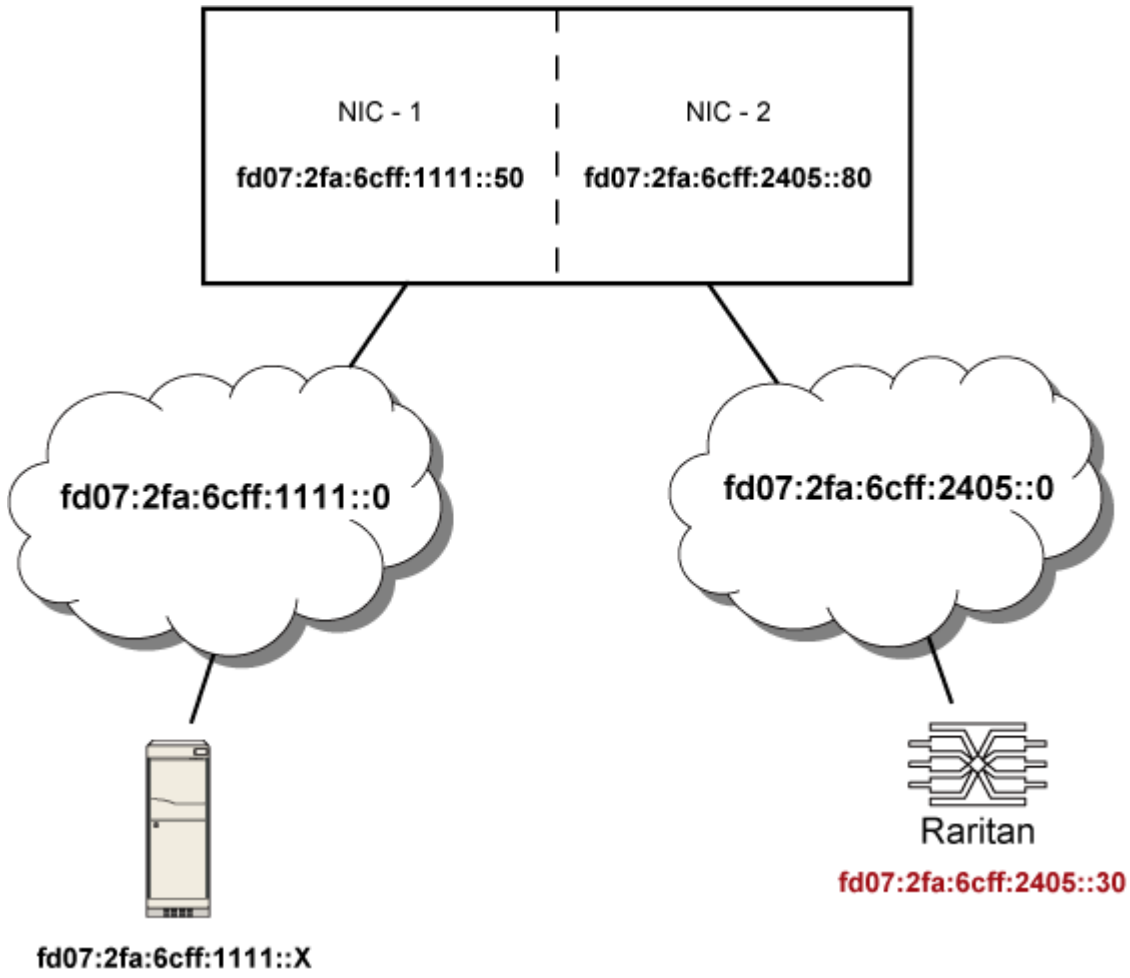
In the IPv4 "Static Routes" section, you should enter the data as shown below. Note that the address in the first field must be of the Classless Inter-Domain Routing (CIDR) notation.



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.*

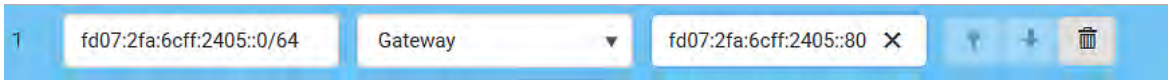
IPv6 example:

- Your PXC/PXO: *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 PXC/PXO to communicate with any device in the other subnet fd07:2fa:6cff:1111::0.

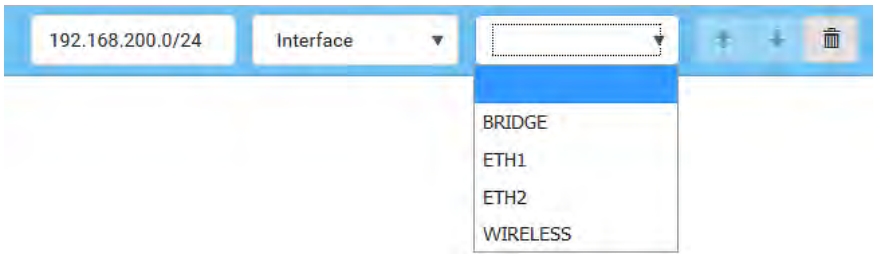
In the IPv6 "Static Routes" section, you should enter the data as shown below. Note that the address in the first field must be of the Classless Inter-Domain Routing (CIDR) notation.



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.



Raritan
A brand of legrand

Interface list:

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

Setting the Cascading Mode

A maximum of 16 PXC/PXO devices can be cascaded to share one Ethernet connection. See ***Cascading Multiple PXC/PXO Devices for Sharing Ethernet Connectivity*** (on page 24).

The cascading mode configured on the master device determines the Ethernet sharing method, which is either network bridging or port forwarding. See ***Overview of the Cascading Modes*** (on page 209).

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: PXC/PXO in the Port Forwarding mode does not support APIPA. See **APIPA and Link-Local Addressing** *(on page 3).*

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 PXC/PXO to a Computer*** (on page 21).
   - To find the IP address, see ***Device Info*** (on page 83).
2. Log in to its web interface. See ***Login*** (on page 96).
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 211).

Tip: If selecting Port Forwarding, the Device Information page will show a list of port numbers for all cascaded devices. Simply choose Maintenance > Device Information > Port Forwarding.

5. For the Port Forwarding mode, one to two more fields have to be configured.

   Note that if either setting below is incorrectly configured, a networking issue occurs.

Field	Description
Port forwarding role (available on all cascaded devices)	*Master or Slave.* This is to determine which device is the master and which ones are slave devices.
Downstream interface (available on the maser device only)	*USB or ETH1/ETH2.* This is to determine which port on the master device is connected to Slave 1. If ETH1 or ETH2 is selected as the downstream interface, make sure the selected Ethernet interface is enabled.

6. (Optional) Configure the network settings by clicking the BRIDGE, ETH1/ETH2, or WIRELESS section on the same page.
   - In the Bridging mode, each cascaded device can have different network settings. You may need to configure each device's network settings in the BRIDGE section.
   - In the Port Forwarding mode, all cascaded devices share the master device's network settings. You only need to configure the master device's network settings in the ETH1/ETH2 and/or WIRELESS section.

   See ***Wired Network Settings*** (on page 191) or ***Wireless Network Settings*** (on page 197)

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 213).

Recommendations for cascade loops:

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

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

AND

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

Online cascading information:

For more information on cascading configurations and restrictions, refer to the *Cascading Guide* on the Raritan ***Support page*** (***http://www.raritan.com/support/***).

Overview of the Cascading Modes

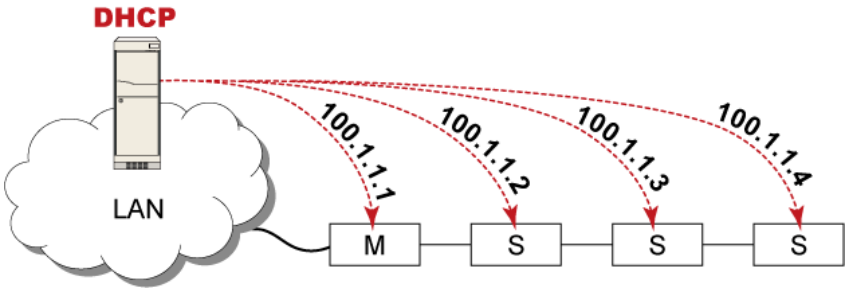
You must apply a cascading mode to the cascading chain. See ***Setting the Cascading Mode*** (on page 207).

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:

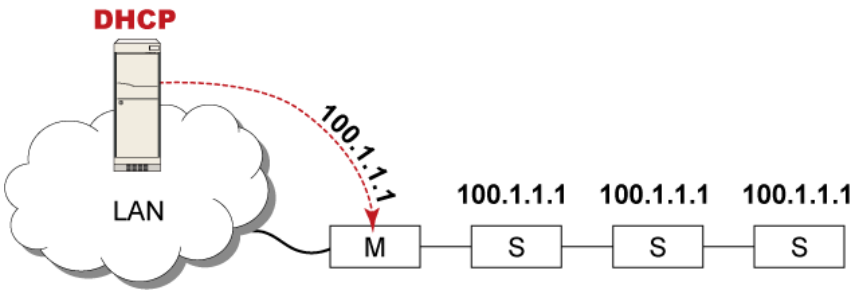
- **"Bridging" mode:**



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 211).

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.

Raritan
A brand of legrand

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 213) 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.

Raritan
A brand of legrand

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 211) 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

Raritan
A brand of legrand

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 688).*

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 207).
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.

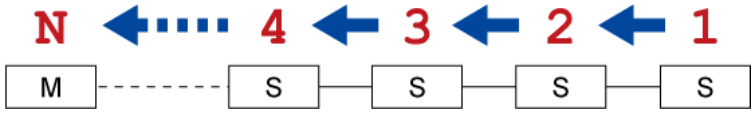
- You must disconnect the LAN cable and ALL cascading cables connected to the two devices first before swapping them, and then reconnecting all cables.

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.

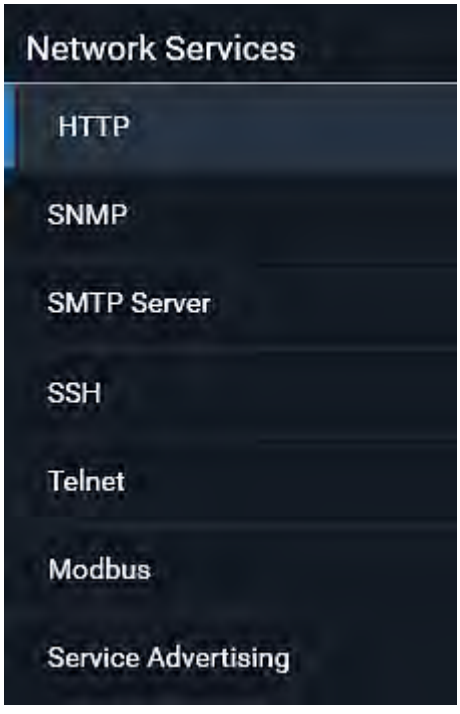
The following diagram indicates the correct sequence. 'N' is the final one.

- M = Master device
- S = Slave device



Configuring Network Services

PXC/PXO supports the following network communication services.



HTTPS and HTTP enable the access to the web interface. Telnet and SSH enable the access to the command line interface. See ***Using the Command Line Interface*** (on page 386).

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 217)
SNMP	***Configuring SNMP Settings*** (on page 219)
SMTP Server	***Configuring SMTP Settings*** (on page 221)
SSH	***Changing SSH Settings*** (on page 222)
Telnet	***Changing Telnet Settings*** (on page 223)
Modbus	***Changing Modbus Settings*** (on page 223)
Server Advertising	***Enabling Service Advertising*** (on page 226)

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

Changing HTTP(S) Settings

HTTPS uses Transport Layer Security (TLS) technology to encrypt all traffic to and from the PXC/PXO so it is a more secure protocol than HTTP. PXC/PXO disables TLS *1.0* and *1.1* by default. It enables only TLS *1.2* and *1.3.*

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

Tip: To force PXC/PXO 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.

Raritan
A brand of legrand

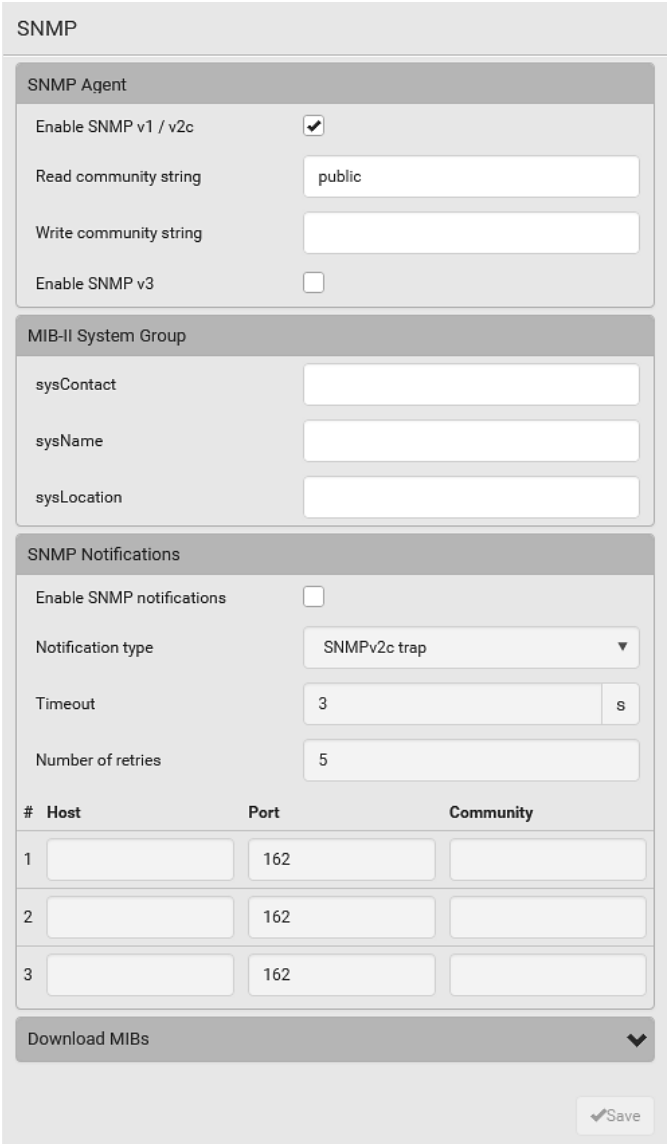
Configuring SNMP Settings

You can enable or disable SNMP communication between an SNMP manager and the PXC/PXO. 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 259).

To configure SNMP communication:

1. Choose Device Settings > Network Services > SNMP.



2. Enable or disable "SNMP v1 / v2c" and/or "SNMP v3" by clicking the corresponding checkbox.
   - The SNMP v1/v2c read-only access is enabled by default. The default 'Read community string' is "public."
   - To enable read-write access, type the 'Write community string.' Usually the string is "private."
3. Enter the MIB-II system group information, if applicable.
   - sysContact - the contact person in charge of the system
   - sysName - the name assigned to the system
   - sysLocation - the location of the system
4. To configure SNMP notifications:
   a. Select the 'Enable SNMP notifications' checkbox.
   b. Select a notification type -- SNMPv2c trap, SNMPv2c inform, SNMPv3 trap, and SNMPv3 inform.
   c. Specify the SNMP notification destinations and enter necessary information. For details, refer to:
      - ***SNMPv2c Notifications*** (on page 379)
      - ***SNMPv3 Notifications*** (on page 380)

   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 273). To add more than three SNMP destinations, you can create new SNMP notification actions. See* **Send an SNMP Notification** *(on page 286).*
5. You must download the SNMP MIB for your PXC/PXO 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 383).
6. Click Save.

Raritan
A brand of legrand

Configuring SMTP Settings

The PXC/PXO can be configured to send alerts or event messages to a specific administrator by email. See ***Event Rules and Actions*** (on page 259).

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 339).

To set SMTP server settings:

1. Choose Device Settings > Network Services > SMTP Server.
2. Enter the information needed.

Field	Description
IP address/host name	Type the name or IP address of the mail server.
Port	Type the port number. ▪ Default is 25
Sender email address	Type an email address for the sender.
Number of sending retries	Type the number of email retries. ▪ Default is 2 retries
Time between sending retries	Type the interval between email retries in minutes. ▪ Default is 2 minutes.
Server requires authentication	Select this checkbox if your SMTP server requires password authentication.
User name, Password	Type a user name and password for authentication after selecting the above checkbox. ▪ The length of user name and password ranges between 4 and 64. Case sensitive. ▪ Spaces are not allowed for the user name, but allowed for the password.
Enable SMTP over TLS (StartTLS)	If your SMTP server supports the Transport Layer Security (TLS), select this checkbox.

- **Settings for the CA Certificate:**

If the required certificate file is a chain of certificates, and you are not sure about the requirements of a certificate chain, see ***TLS Certificate Chain*** (on page 702).

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

Tip: To force PXC/PXO 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.

Raritan
A brand of legrand

- *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 177).

Changing Telnet Settings

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

To change Telnet settings:

1. Choose Device Settings > Network Services > Telnet.
2. To enable the Telnet access, select the checkbox.
3. To use a different port, type a new port number.
4. Click Save.

Changing Modbus Settings

The PXC/PXO supports both the Modbus/TCP and Modbus Gateway features. Enable either or both Modbus features according to your needs.

Modbus/TCP Access:

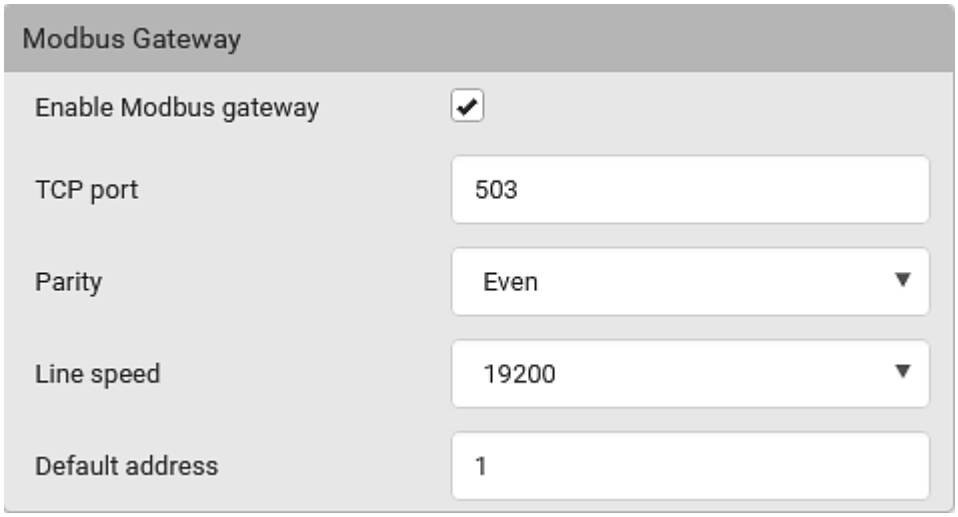
You can enable or disable the Modbus/TCP access to PXC/PXO, set it to the read-only mode, or change the TCP port.

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

Modbus Gateway:

If connecting the Modbus RTU devices to PXC/PXO and enabling the Modbus Gateway feature, the Modbus TCP clients on your network will be able to communicate with those Modbus RTU devices attached to PXC/PXO. See ***Connecting a Modbus RTU Device or Bus*** (on page 54).

1. To allow the Modbus TCP clients on the network to communicate with the Modbus RTU devices connected to the PXC/PXO, select the 'Enable Modbus gateway' checkbox.



2. Now configure the fields shown.

Field	Description
TCP port	Use the default port 503, or assign a different port. Valid range is 1 to 65535. *Note: Port 502 is the default Modbus/TCP port for PXC/PXO, so you cannot use that port for the Modbus Gateway.*
Parity, **Line speed**	Use the default values, or update if the Modbus RTU devices are using different communication parameters.
Default address	If the Modbus TCP client does not support Modbus RTU unit identifier addressing, enter a Default Address. If you must provide a unit identifier address: ▪ Only one Modbus RTU device is supported. ▪ The unit identifier address you provide is applied to the Modbus RTU device connected to PXC/PXO. Note that each Modbus RTU device's unit identifier address must be unique. *Warning: If the connected Modbus RTU device's address does not match the address entered in this field, communications between the Modbus TCP clients and Modbus RTU device fail.*

Enabling Service Advertising

The PXC/PXO 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 3).

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 PXC/PXO. 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 191).*

To enable or disable service advertising:

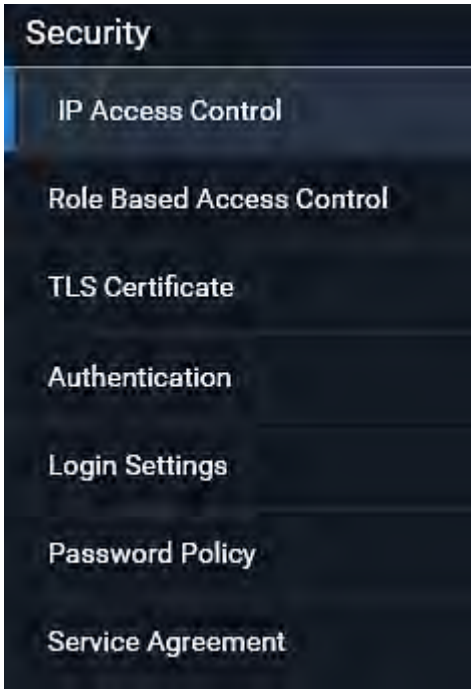
1. Choose Device Settings > Network Services > Service Advertising.
2. To enable the service advertising, select either or both checkboxes.
   - To advertise via MDNS, select the Multicast DNS checkbox.
   - To advertise via LLMNR, select the Link-Local Multicast Name Resolution checkbox.
3. Click Save.

Raritan
A brand of legrand

Configuring Security Settings

The PXC/PXO 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 PXC/PXO to be redirected to HTTPS, see **Changing HTTP(S) Settings** *(on page 217).*



Submenu command	Refer to
IP Access Control	***Creating IP Access Control Rules*** (on page 228)
Role Based Access Control	***Creating Role Based Access Control Rules*** (on page 232)
TLS Certificate	***Setting Up a TLS Certificate*** (on page 234)
Authentication	***Setting Up External Authentication*** (on page 239)
Login Settings	***Configuring Login Settings*** (on page 247)
Password Policy	***Configuring Password Policy*** (on page 248)
Service Agreement	***Enabling the Restricted Service Agreement*** (on page 249)

Creating IP Access Control Rules

IP access control rules (firewall rules) determine whether to accept or discard traffic to/from the PXC/PXO, 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 PXC/PXO, 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 PXC/PXO.
   - Outbound rules control the data sent from the PXC/PXO.
5. Create rules. Refer to the tables below for different operations.

Raritan
A brand of legrand

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.

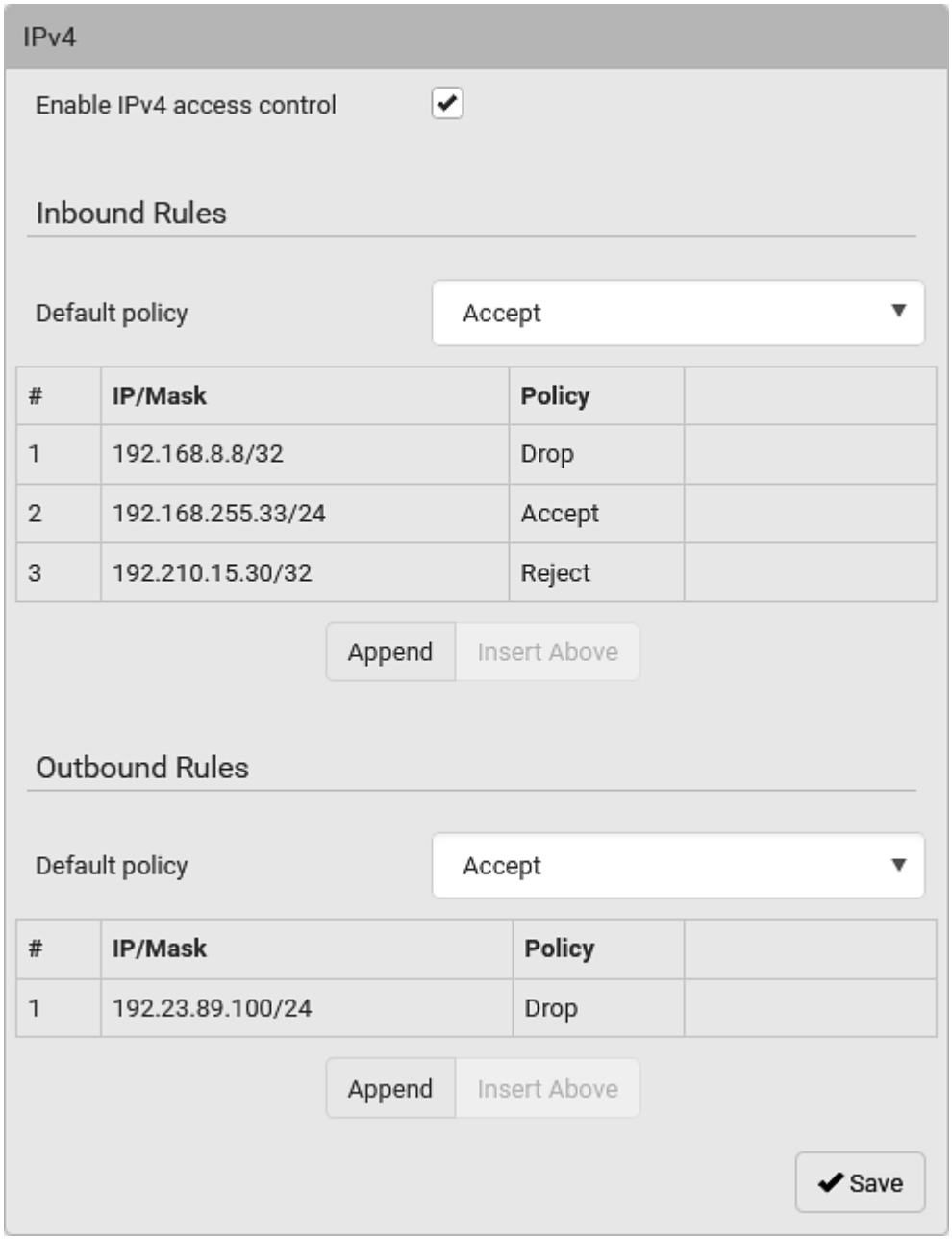
INSERT a rule between two rules

- 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.



7. Click Save. The rules are applied.

To configure IPv6 access control rules:

1. On the same page, select the 'Enable IPv6 access control' checkbox to enable IPv6 access control rules.
2. Follow the same procedure as the above IPv4 rule setup to create IPv6 rules.
3. **Make sure you click the Save button in the IPv6 section**, or the changes made to IPv6 rules are not saved.

Editing or Deleting IP Access Control Rules

When an existing IP access control rule requires updates of IP address range and/or policy, modify them accordingly. Or you can delete any unnecessary rules.

To modify or delete a rule:

1. Choose Device Settings > Security > IP Access Control.
2. Go to the IPv4 or IPv6 section.
3. Select the desired rule in the list.
   - Ensure the IPv4 or IPv6 checkbox has been selected, or you may not edit or delete any rule.
4. Perform the desired action.
   - Make changes to the selected rule, and then click Save. For information on each field, see ***Creating IP Access Control Rules*** (on page 228).
   - 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.

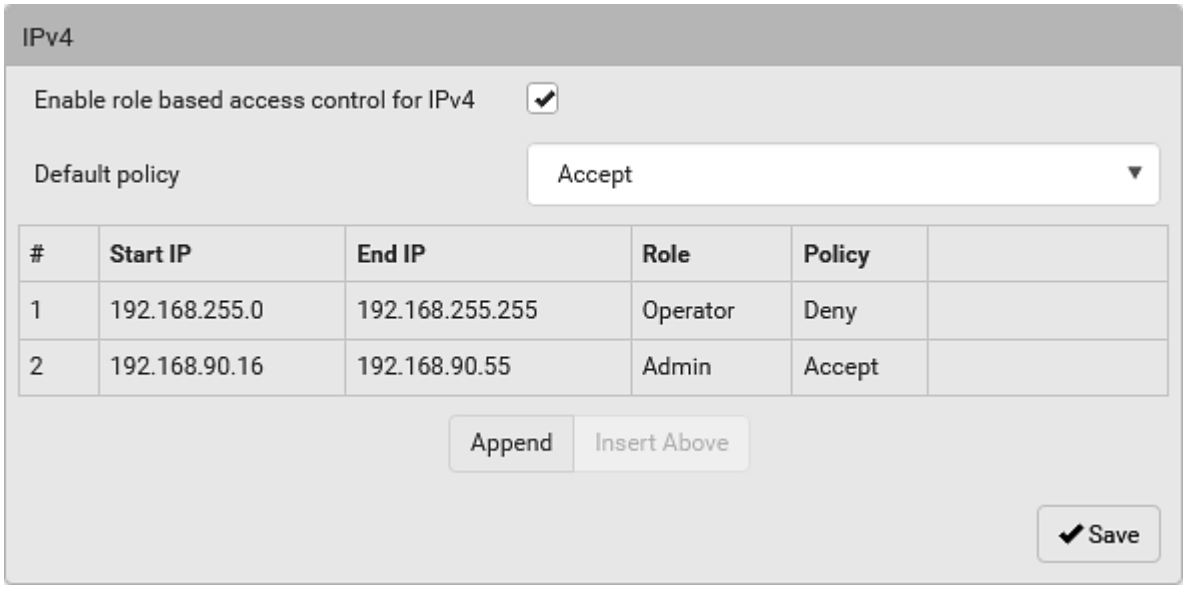
INSERT a rule between two rules
▪ Select the rule above which you want to insert a new rule. For example, to insert a rule between rules #3 and #4, select #4. ▪ Click Insert Above. ▪ Type a starting IP address in the Start IP field. ▪ Type an ending IP address in the End IP field. ▪ Select a role in 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.

Raritan
A brand of legrand

- You can select any existing rule and then click or to change its priority.



6. Click Save. The rules are applied.

To configure IPv6 access control rules:

1. On the same page, select the 'Enable role based access control for IPv6' checkbox to enable IPv6 access control rules.
2. Follow the same procedure as the above IPv4 rule setup to create IPv6 rules.
3. **Make sure you click the Save button in the IPv6 section**, or the changes made to IPv6 rules are not saved.

Editing or Deleting Role Based Access Control Rules

You can modify existing rules to update their roles/IP addresses, or delete them when they are no longer needed.

To modify a role-based access control rule:

1. Choose Device Settings > Security > Role Based Access Control.
2. Go to the IPv4 or IPv6 section.
3. Select the desired rule in the list.
   - Ensure the IPv4 or IPv6 checkbox has been selected, or you may not edit or delete any rule.
4. Perform the desired action.

- Make changes to the selected rule, and then click Save. For information on each field, see ***Creating Role Based Access Control Rules*** (on page 232).
- Click to remove it.
- To resort its order, click or .

5. Click Save.
   - IPv4 rules: **Make sure you click the Save button in the IPv4 section**, or the changes made to IPv4 rules are not saved.
   - IPv6 rules: **Make sure you click the Save button in the IPv6 section**, or the changes made to IPv6 rules are not saved.

Setting Up a TLS Certificate

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

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

Besides, you can create or apply for a multi-domain certificate with subject alternative names.

To obtain a CA-signed certificate:

1. Create a Certificate Signing Request (CSR) on the PXC/PXO. See ***Creating a CSR*** (on page 235).
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 PXC/PXO. See ***Installing a CA-Signed Certificate*** (on page 236).

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 PXC/PXO create a *self-signed* certificate. See ***Creating a Self-Signed Certificate*** (on page 237).
- Appropriate, valid certificate and key files are already available, and you only need to import them. See ***Installing or Downloading Existing Certificate and Key*** (on page 238).

Creating a CSR

Follow this procedure to create the CSR for your PXC/PXO.

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

To create a CSR:

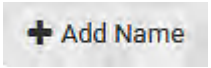
1. Choose Device Settings > Security > TLS Certificate.
2. Provide the information requested.
   - **Subject:**

Field	Description
Country	The country where your company is located. Use the standard ISO country code, which comprises two uppercase letters. For a list of ISO codes, google ISO 3166 country codes.
State or province	The full name of the state or province where your company is located.
Locality	The city where your company is located.
Organization	The registered name of your company.
Organizational unit	The name of your department.
Common name	The fully qualified domain name (FQDN) of your PXC/PXO.
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 

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 PXC/PXO. ▪ Only 2048 is available now.
Self-sign	**For requesting a certificate signed by the CA, ensure this checkbox is NOT selected.**
Challenge, Confirm challenge	Type a password. The password is used to protect the certificate or CSR. This information is optional. The value should be 4 to 64 characters long. Case sensitive.

3. Click Create New TLS Key to create both the CSR and private key. This may take several minutes to complete.
4. Click Download Certificate Signing Request to download the CSR to your computer.
   a. You are prompted to open or save the file. Click Save to save it onto your computer.
   b. Submit it to a CA to obtain the digital certificate.
   c. If the CSR contains incorrect data, click Delete Certificate Signing Request to remove it, and then repeat the above steps to re-create it.
5. To store the newly-created private key on your computer, click Download Key in the **New TLS Certificate** section.

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

   ▪ You are prompted to open or save the file. Click Save to save it onto your computer.
6. After getting the CA-signed certificate, install it. See ***Installing a CA-Signed Certificate*** (on page 236).

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 235).

After receiving the CA-signed certificate, install it onto the PXC/PXO.

To install the CA-signed certificate:

1. Choose Device Settings > Security > TLS Certificate.
2. Click

to navigate to the CA-signed certificate file.
3. Click Upload to install it.

Raritan
A brand of legrand

4. To verify whether the certificate has been installed successfully, check the data shown in the Active TLS Certificate section.

Creating a Self-Signed Certificate

When appropriate certificate and key files for PXC/PXO 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 > TLS Certificate.
2. Enter information.

Field	Description
Country	The country where your company is located. Use the standard ISO country code, which comprises two uppercase letters. For a list of ISO codes, google ISO 3166 country codes.
State or province	The full name of the state or province where your company is located.
Locality	The city where your company is located.
Organization	The registered name of your company.
Organizational unit	The name of your department.
Common name	The fully qualified domain name (FQDN) of your PXC/PXO.
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 PXC/PXO. ▪ Only 2048 is available now.
Self-sign	**Ensure this checkbox is selected, which indicates that you are creating a self-signed certificate.**
Validity in days	This field appears after the Self-sign checkbox is selected. Type the number of days for which the self-signed certificate will be valid.

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

3. Click Create New TLS Key to create both the self-signed certificate and private key. This may take several minutes to complete.
4. Once complete, do the following:

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

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

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

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

5. (Optional) To download the self-signed certificate and/or private key, click Download Certificate or Download Key in the New TLS Certificate section.
   - You are prompted to open or save the file. Click Save to save it onto your computer.

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

Installing or Downloading Existing Certificate and Key

You can download the already-installed certificate and private key from any PXC/PXO for backup or file transfer. For example, you can install the files onto a replacement PXC/PXO, 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 PXC/PXO 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 PXC/PXO:

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

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

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

To install available key and certificate files onto PXC/PXO:

1. Choose Device Settings > Security > TLS Certificate.
2. Select the "Upload key and certificate" checkbox at the bottom of the page.
3. The 'Key File' and 'Certificate file' buttons appear. Click each button to select the key and/or certificate file.

Raritan
A brand of legrand

4. Click Upload. The selected files are installed.
5. To verify whether the certificate has been installed successfully, check the data shown in the Active TLS Certificate section.

Setting Up External Authentication

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

For security purposes, users attempting to log in to PXC/PXO must be authenticated. PXC/PXO supports the following authentication mechanisms:

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

By default, PXC/PXO is configured for local authentication. If you use this method, you only need to create user accounts. See ***Creating Users*** (on page 177).

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

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

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

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 339).

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 240).
2. Enter required data for external AA server(s) on the PXC/PXO. See ***Adding LDAP/LDAPS Servers*** (on page 241) or ***Adding Radius Servers*** (on page 244).
   - For illustrations, see ***LDAP Configuration Illustration*** (on page 621) or ***RADIUS Configuration Illustration*** (on page 636).
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 246).

Special note about the AES cipher:

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

Tip: To force PXC/PXO 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 PXC/PXO 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.

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 PXC/PXO. 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.
Security	Determine whether you would like to use Transport Layer Security (TLS) encryption, which allows the PXC/PXO to communicate securely with the LDAPS server. Three options are available: ▪ StartTLS ▪ TLS ▪ None
Port (None/StartTLS)	▪ The default Port is 389. Either use the standard LDAP TCP port or specify another port.
Port (TLS)	**Configurable only when "TLS" is selected in the Security field.** The default is 636. Either use the default port or specify another one.
Enable verification of LDAP server certificate	Select this checkbox if it is required to validate the LDAP server's certificate by the PXC/PXO prior to the connection. If the certificate validation fails, the connection is refused.

Field/setting	Description
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 702).*
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`.

Raritan
A brand of legrand

Field/setting	Description
User search subfilter	Search criteria for finding LDAP user objects within the directory tree.
Group lookup using memberOf attribute	▪ Select this checkbox to determine group membership by consulting the user's memberOf attribute(s). ▪ Deselect this checkbox to determine group membership by doing a non-recursive search for groups containing the user's DN as member.
Group member attribute	▪ Required only when "Group lookup using memberOf attribute" is not selected. ▪ Required for OpenLDAP only.
Group entry object class	▪ Required only when "Group lookup using memberOf attribute" is not selected. ▪ Required for OpenLDAP only.
Group search subfilter	▪ Required only when "Group lookup using memberOf attribute" is not selected. ▪ Required for OpenLDAP only.
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 PXC/PXO 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 246).*

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 PXC/PXO, 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 PXC/PXO 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 PXC/PXO 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.'

To add Radius servers:

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

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

Raritan
A brand of legrand

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 PXC/PXO 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 246).*

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.

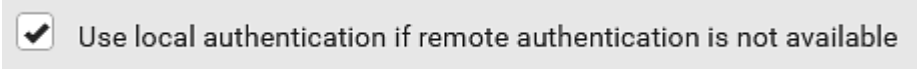
Access Order	IP Address / Hostname	Security	Port	LDAP Server Type
1	192.168.91.100	None	389	OpenLDAP
2	192.168.1.33	StartTLS	389	OpenLDAP
3	192.168.8.95	None	389	Microsoft Active Directory

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 241) or ***Adding Radius Servers*** (on page 244).
   - 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 PXC/PXO 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 PXC/PXO always tries external authentication first. Whenever the external authentication fails, the PXC/PXO switches to local authentication.



3. Click Save.

Raritan
A brand of legrand

To disable external authentication:

1. In the 'Authentication type' field, select Local.
2. Click Save.

Configuring Login Settings

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

- Configure the user blocking feature.

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

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

To configure user blocking:

1. To enable the user blocking feature, select the 'Block user on login failure' checkbox.
2. In the 'Block timeout' field, type a value or click to select a time option. This setting determines how long the user is blocked.
   - If you type a value, the value must be followed by a time unit, such as '4 min.' See ***Time Units*** (on page 120).
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 PXC/PXO.
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 553).*

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 120).
   - 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 PXC/PXO.

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 PXC/PXO.

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 120).
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 PXC/PXO is 64 characters.

2. Make changes to the default settings as needed.

Raritan
A brand of legrand

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 PXC/PXO.

Users must accept the agreement, or they cannot log in.

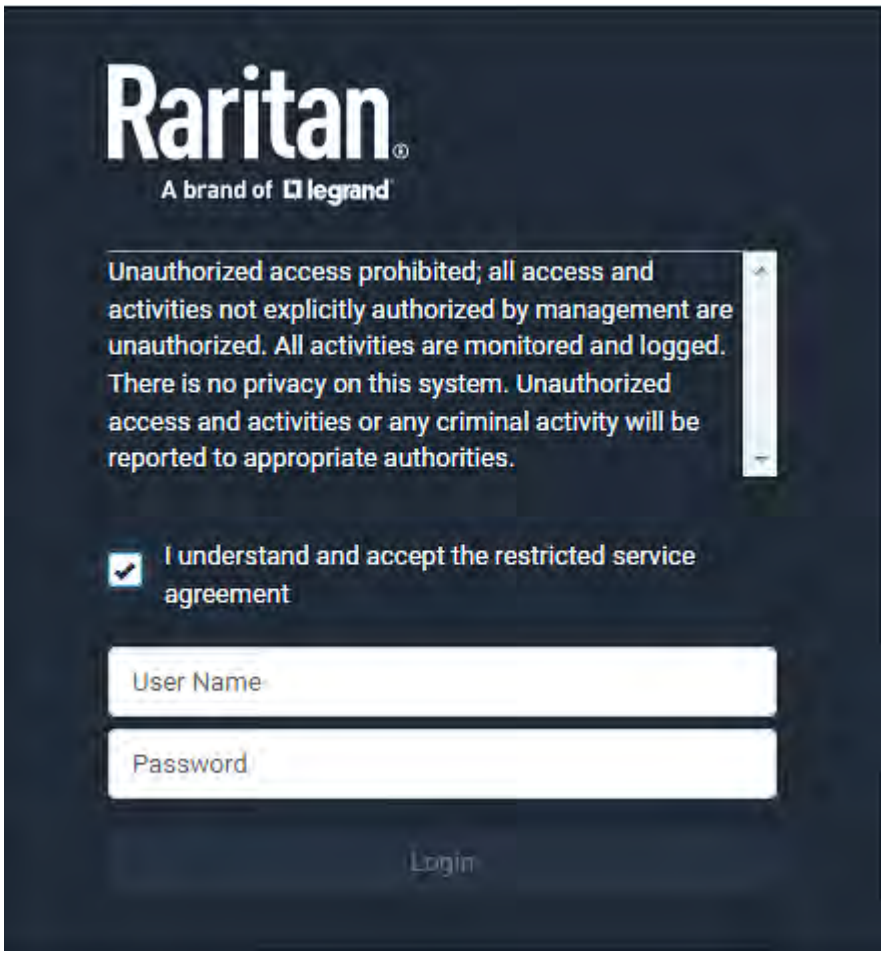
An event notifying you if a user has accepted or declined the agreement can be generated. See ***Default Log Messages*** (on page 265)

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 PXC/PXO manually, or link to a Network Time Protocol (NTP) server.

Note: If you are using Sunbird's Power IQ to manage the PXC/PXO, you must configure Power IQ and the PXC/PXO 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 253).
- Determine the time format you want by clicking 12H or 24H button.
  - **12H** represents the 12-hour format.
  - **24H** represents the 24-hour format.

- If selecting 12-hour format, then determine the current period by clicking the AM or PM button.

- Type values in the Time field using the hh:mm:ss format, or click to adjust values.
  - When 12H is being applied, the hour cannot exceed the maximum number 12. If exceeding 12, the time change cannot be saved.

Use the NTP server

▪ Select "Synchronize with NTP server."
▪ There are two ways to assign the NTP servers:
  ▪ To use the DHCP-assigned NTP servers, DO NOT enter any NTP servers for the First and Second time server.
  DHCP-assigned NTP servers are available only when either IPv4 or IPv6 DHCP is enabled.
  ▪ To use the manually-specified NTP servers, specify the primary NTP server in the "First time server" field. A secondary NTP server is optional.
  Click Check NTP Servers to verify the validity and accessibility of the manually-specified NTP servers.

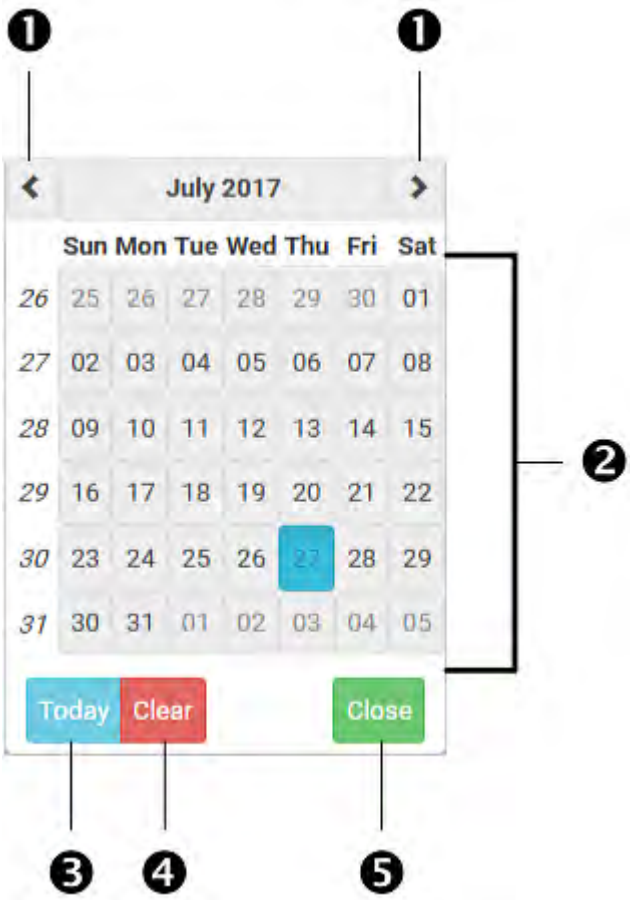
5. Click Save.

PXC/PXO follows the NTP server sanity check per the IETF RFC. If your PXC/PXO has problems synchronizing with a Windows NTP server, see ***Windows NTP Server Synchronization Solution*** (on page 254).

Raritan
A brand of legrand

Calendar

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 PXC/PXO follows the NTP RFC so the PXC/PXO 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 PXC/PXO.

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 PXC/PXO. 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.

Raritan
A brand of legrand

Door Access Control

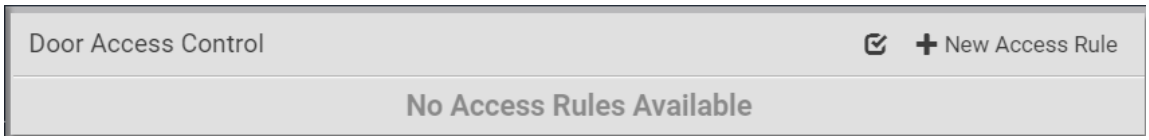
SmartLock enabled cabinets integrated with PowerIQ or other third party systems authorize door access control remotely. In the event that the remote authorization is not accessible, you can configure local door access control rules as a fallback method.

A door access control rule can contain the following components:

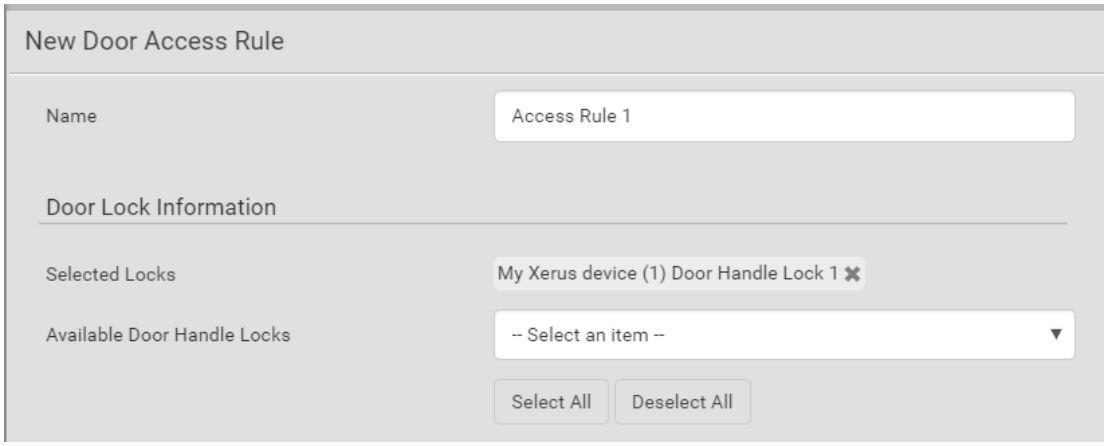
- Selected door locks: must be configured in advance. See ***SmartLock*** (on page 371).
- Authorization via card: specify which card ID and card reader must be used
- Authorization via keypad: specify the PIN and keypad that must be used
- Two-factor authorization: a timeout that requires both card and keypad conditions to be met. For example: when a certain card is inserted, the correct PIN must be entered in the next 10 seconds.
- Absolute time conditions: grant access for a specific date and time
- Periodic time conditions: grant access on certain days of the week and certain times

To create a door access control rule:

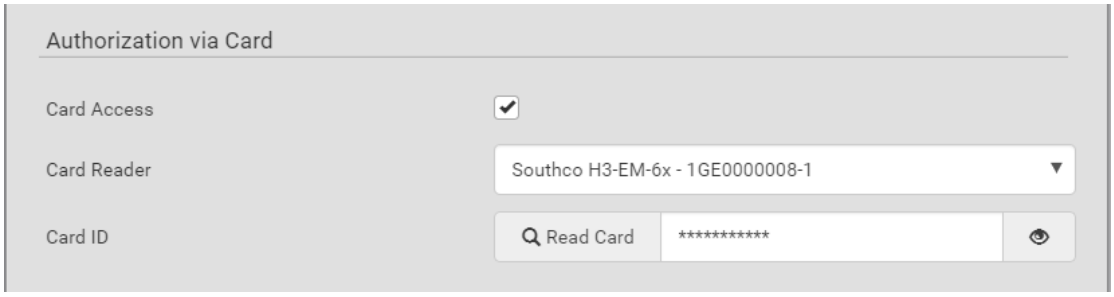
1. Choose Device Settings > Door Access.
2. Click New Access Rule.



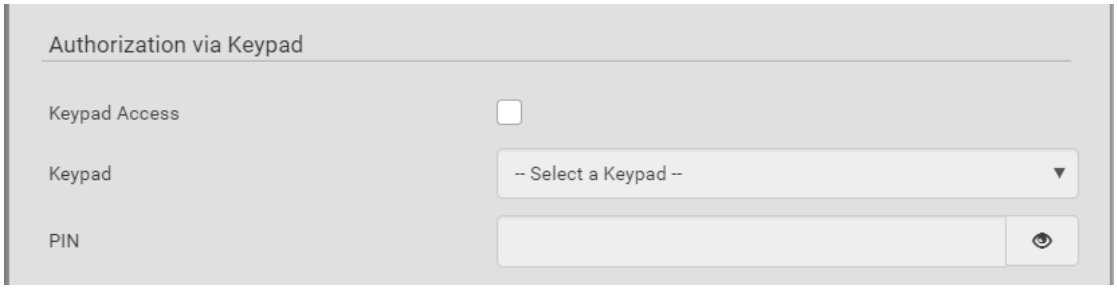
3. The New Door Access Rule page opens. Enter a name for the rule. 128 characters maximum.
4. Select the door locks this rule applies to in the Available Door Handle Locks list. Each selected door lock appears in the Selected Locks section.



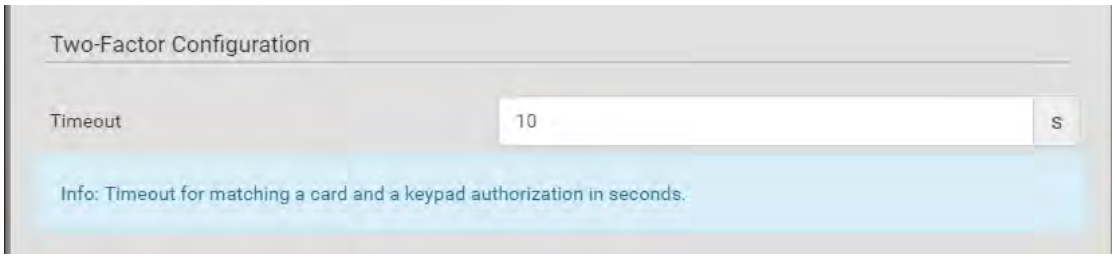
5. To allow authorization via card reader, select the Card Access checkbox, then select the correct Card Reader and click Read Card to retrieve the Card ID. Card IDs are hidden for security. Click the eyeball icon to reveal and verify the Card ID.



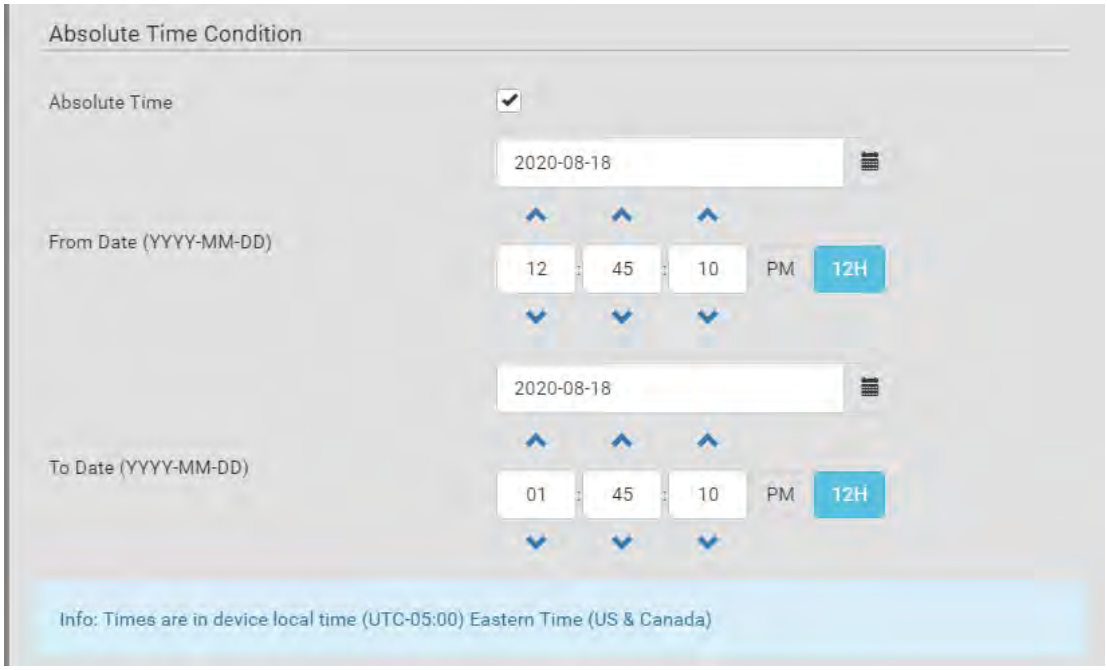
6. To allow Authorization via Keypad, select the Keypad Access checkbox, then select the correct keypad and enter the PIN. PINs are hidden for security. Click the eyeball icon to reveal and verify the PIN. PIN length varies by keypad, and a minimum PIN length of 4 is required.



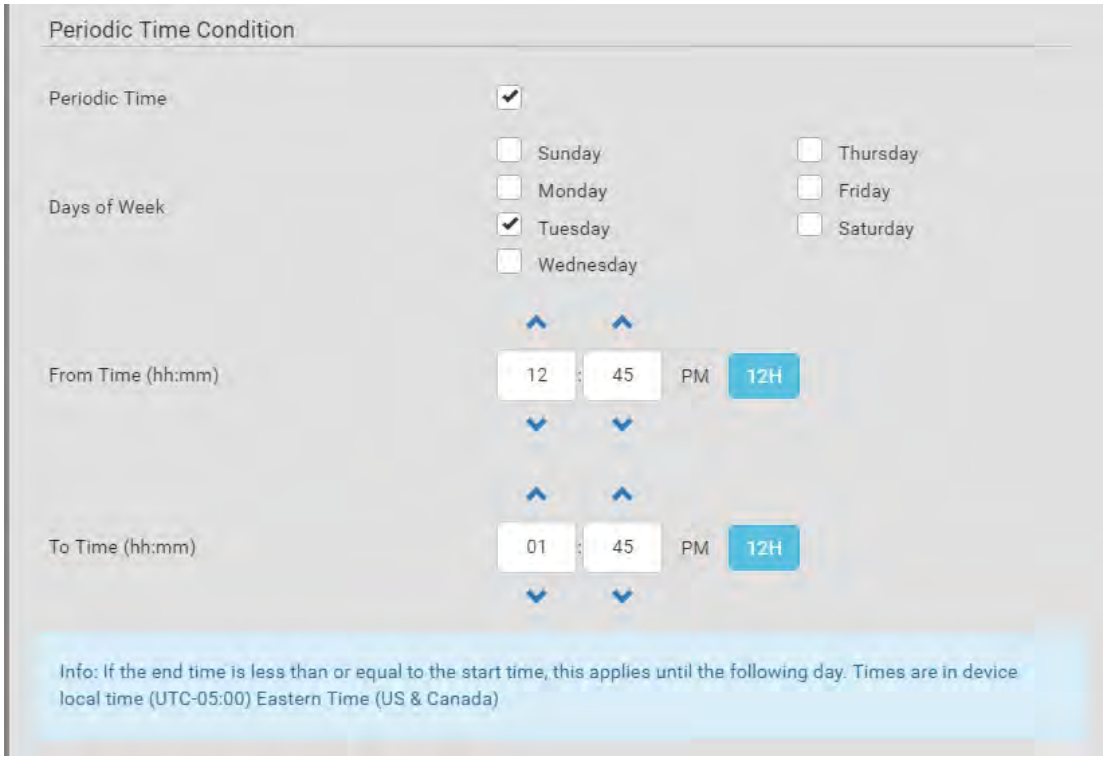
7. When both Card and Keypad authorization are required, the Two-Factor Configuration controls are required. Enter a Timeout in seconds during which both Card and Keypad authorization must occur.



8. To allow authorization with an Absolute Time Condition, select the Absolute Time checkbox, then use the calendar tool to set the start and end dates, and the clock tools to set the start and end times during which access is granted. Note: Click the 12H/24H icon to toggle between clock styles.



9. To allow authorization with a Periodic Time Condition, select the Periodic Time checkbox, then select the Days of Week and range of hours on which access is granted. Note: Click the 12H/24H icon to toggle between clock styles.



10. Click Create to save the rule. All rules appear on the main Door Access Control page.

Raritan
A brand of legrand

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 PXC/PXO 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 PXC/PXO notifies the system administrator of the event via email.

If you want the PXC/PXO 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 PXC/PXO 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

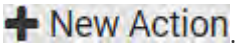
   a. Assign a name to this action.
   b. Select the desired action and configure it as needed.
   c. Click Create.

   For details, see ***Available Actions*** (on page 273).
3. Click

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 PXC/PXO to react.
   d. In the 'Available actions' field, select the desired action(s) to respond to the selected event.
   e. Click Create.

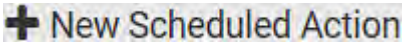
   For details, see ***Built-in Rules and Rule Configuration*** (on page 260).

To create a scheduled action:

1. If the needed action is not available yet, create it by clicking 

. 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  to schedule the desired action.
   a. Assign a name to this scheduled action.
   b. Make sure the Enabled checkbox is selected, or the PXC/PXO 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 291).

Built-in Rules and Rule Configuration

PXC/PXO 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 PXC/PXO 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 265).*

- *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 PXC/PXO. It is disabled by default.

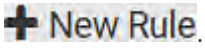
- *System Tamper Detection Alarmed:*

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

- *System Tamper Detection Unavailable:*

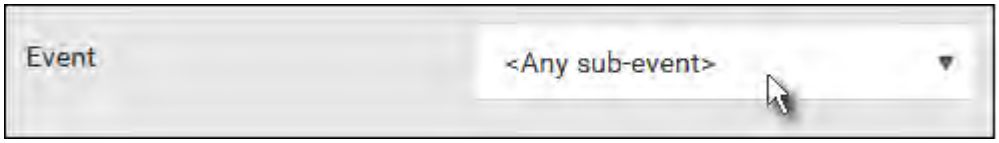
  This causes the PXC/PXO to send alarm notifications if a DX tamper sensor was once connected or remains connected but then the PXC/PXO does not detect the presence of the tamper sensor. It is enabled by default.

Event rule configuration illustration:

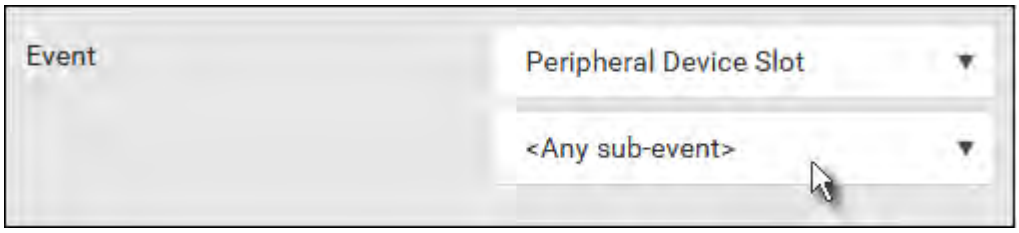
1. Choose Device Settings > Event Rules >  .
2. Click the Event field to select an event type.
   - <Any sub-event> means all events shown on the list.

Raritan
A brand of legrand

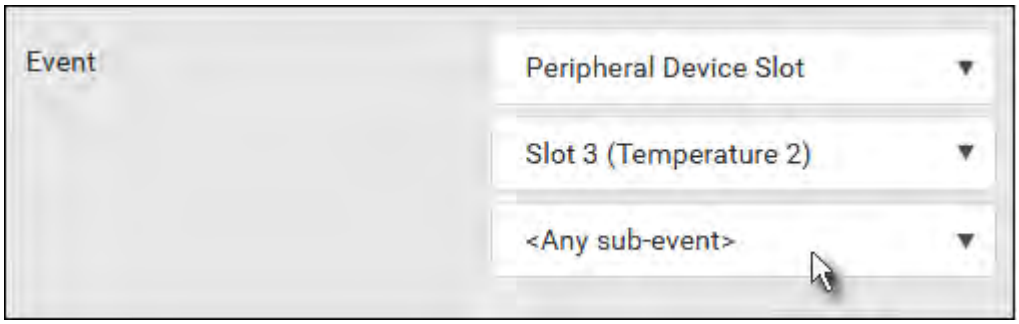
- <Any Numeric Sensor> means all numeric sensors of the PXC/PXO, including internal and environmental sensors. <Any Numeric Sensor> is especially useful if you want to receive the notifications when any numeric sensor's readings pass through a specific threshold.



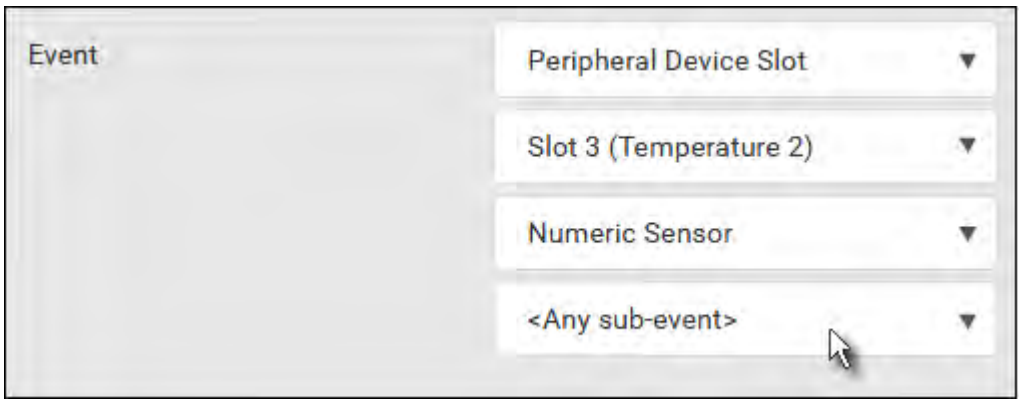
3. In this example, the Peripheral Device Slot is selected, which is related to the environmental sensor packages. Then a sensor ID field for this event type appears. Click this additional field to specify which sensor should be the subject of this event.



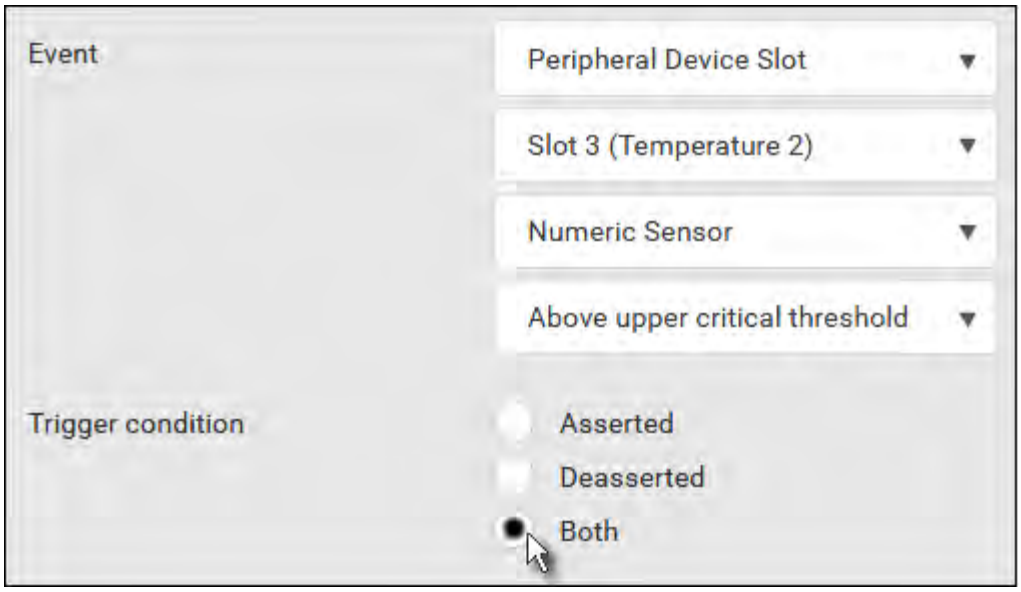
4. In this example, sensor ID 3 (Slot 3) is selected, which is a temperature sensor. Then a new field for this sensor appears. Click this field to specify the type of event(s) you want.



5. In this example, Numeric Sensor is selected because we want to select numeric-sensor-related event(s). Then a field for numeric-sensor-related events appears. Click this field to select one of the numeric-sensor-related events from the list.



6. In this example, 'Above upper critical threshold' is selected because we want the PXC/PXO 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 303).
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: PXC/PXO takes the action only when the selected event occurs. That is, the status of the event transits from FALSE to TRUE. ▪ Deasserted: PXC/PXO 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: PXC/PXO takes the action both when the event occurs (asserts) and when the event stops/disappears (deasserts).
State sensor state change	Available radio buttons include "Alarmed/Open/On," "No longer alarmed/Closed/Off" and "Both." ▪ Alarmed/Open/On: PXC/PXO takes the action only when the chosen sensor enters the alarmed, open or on state. ▪ No longer alarmed/Closed/Off: PXC/PXO takes the action only when the chosen sensor returns to the normal, closed, or off state. ▪ Both: PXC/PXO takes the action whenever the chosen sensor switches its state.
Sensor availability	Available radio buttons include "Unavailable," "Available" and "Both." ▪ Unavailable: PXC/PXO takes the action only when the chosen sensor is NOT detected and becomes unavailable. ▪ Available: PXC/PXO takes the action only when the chosen sensor is detected and becomes available. ▪ Both: PXC/PXO takes the action both when the chosen sensor becomes unavailable or available.

Event types	Radio buttons
Network interface link state	▪ Link state is up: PXC/PXO takes the action only when the network link state changes from down to up. ▪ Link state is down: PXC/PXO takes the action only when the network link state changes from up to down. ▪ Both: PXC/PXO takes the action whenever the network link state changes.
Function enabled or disabled	▪ Enabled: PXC/PXO takes the action only when the chosen function is enabled. ▪ Disabled: PXC/PXO takes the action only when the chosen function is disabled. ▪ Both: PXC/PXO takes the action when the chosen function is either enabled or disabled.
Restricted service agreement	▪ Accepted: PXC/PXO takes the action only when the specified user accepts the restricted service agreement. ▪ Declined: PXC/PXO takes the action only when the specified user rejects the restricted service agreement. ▪ Both: PXC/PXO takes the action both when the specified user accepts or rejects the restricted service agreement.
Server monitoring event	▪ Monitoring started: PXC/PXO takes the action only when the monitoring of any specified server starts. ▪ Monitoring stopped: PXC/PXO takes the action only when the monitoring of any specified server stops. ▪ Both: PXC/PXO takes the action when the monitoring of any specified server starts or stops.
Server reachability	▪ Unreachable: PXC/PXO takes the action only when any specified server becomes inaccessible. ▪ Reachable: PXC/PXO takes the action only when any specified server becomes accessible. ▪ Both: PXC/PXO takes the action when any specified server becomes either inaccessible or accessible.

Raritan
A brand of legrand

Event types	Radio buttons
Device connection or disconnection, such as a USB-cascaded slave device	▪ Connected: PXC/PXO takes the action only when the selected device is physically connected to it. ▪ Disconnected: PXC/PXO takes the action only when the selected device is physically disconnected from it. ▪ Both: PXC/PXO 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 PXC/PXO events occur (are TRUE) or, in some cases, stop or become unavailable (are FALSE). See ***Send Email*** (on page 281) to configure email messages.

Event/context	Default message when the event = TRUE	Default message when the event = FALSE
Card Reader Management > Card Reader > * > Card inserted	Card of type '[SMARTCARDTYPE]' with ID '[SMARTCARDID]' inserted at Card Reader '[CARDREADERID]'.	
Card Reader Management > Card Reader > * > Card removed	Card of type '[SMARTCARDTYPE]' with ID '[SMARTCARDID]' removed at Card Reader '[CARDREADERID]'.	
Card Reader Management > Card Reader attached	Card Reader with id '[CARDREADERID]' disconnected.	
Card Reader Management > Card Reader detached	Card of type '[SMARTCARDTYPE]' with ID '[SMARTCARDID]' inserted.	
Device > System started	System started.	
Device > System reset	System reset performed by user '[USERNAME]' from host '[USERIP]'.	
Device > Firmware validation failed	Firmware validation failed by user '[USERNAME]' from host '[USERIP]'.	
Device > Firmware update started	Firmware upgrade started from version '[OLDVERSION]' to version '[VERSION]' by user '[USERNAME]' from host '[USERIP]'.	

Event/context	Default message when the event = TRUE	Default message when the event = FALSE
Device > Firmware update completed	Firmware upgraded successfully from version '[OLDVERSION]' to version '[VERSION]' by user '[USERNAME]' from host '[USERIP]'.	
Device > Firmware update failed	Firmware upgrade failed from version '[OLDVERSION]' to version '[VERSION]' by user '[USERNAME]' from host '[USERIP]'.	
Device > Hardware failure present	Failure '[FAILURETYPESTR]' asserted for component '[COMPONENTID]'.	Failure '[FAILURETYPESTR]' deasserted for component '[COMPONENTID]'.
Device > Device identification changed	Config parameter '[CONFIGPARAM]' changed to '[CONFIGVALUE]' by user '[USERNAME]' from host '[USERIP]'.	
Device > Device settings saved	Device settings saved by user '[USERNAME]' from host '[USERIP]'.	
Device > Device settings restored	Device settings restored from host '[USERIP]'.	
Device > Data push failed	Data push to URL [DATAPUSH_URL] failed. [ERRORDESC].	
Device > Event log cleared	Event log cleared by user '[USERNAME]' from host '[USERIP]'.	
Device > Bulk configuration saved	Bulk configuration saved by user '[USERNAME]' from host '[USERIP]'.	
Device > Bulk configuration copied	Bulk configuration copied by user '[USERNAME]' from host '[USERIP]'.	
Device > Network interface link state is up	The [IFNAME] network interface link is now up.	The [IFNAME] network interface link is now down.
Device > Peripheral Device Firmware Update	Firmware update for peripheral device [EXTSENSORSERIAL] from [OLDVERSION] to [VERSION] [SENSORSTATENAME].	
Device > Sending SMTP message failed	Sending SMTP message to '[SMTPRECIPIENTS]' using server '[SMTPSERVER]' failed. [ERRORDESC].	
Device > Sending SNMP inform failed or no response	Sending SNMP inform to manager [SNMPMANAGER]:[SNMPMANAGERPORT] failed or no response. [ERRORDESC].	

Raritan
A brand of legrand

Event/context	Default message when the event = TRUE	Default message when the event = FALSE
Device > Sending Syslog message failed	Sending Syslog message to server [SYSLOGSERVER]:[SYSLOGPORT] ([SYSLOGTRANSPORTPROTO]) failed. [ERRORDESC].	
Device > An LDAP error occurred	An LDAP error occurred: [ERRORDESC].	
Device > A Radius error occurred	A Radius error occurred: [ERRORDESC].	
Device > Raw configuration downloaded	Raw configuration downloaded by user '[USERNAME]' from host '[USERIP]'.	
Device > Raw configuration updated	Raw configuration updated by user '[USERNAME]' from host '[USERIP]'.	
Device > Unknown peripheral device attached	An unknown peripheral device with rom code '[ROMCODE]' was attached at position '[PERIPHDEVPOSITION]'.	
Device > Slave connected	Slave connected.	Slave disconnected.
Device > WLAN authentication over TLS with incorrect system clock	Established connection to wireless network '[SSID]' via Access Point with BSSID '[BSSID]' using '[AUTHPROTO]' authentication with incorrrect system clock.	
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].

Event/context	Default message when the event = TRUE	Default message when the event = FALSE
Peripheral Device Slot > * > Numeric Sensor > Below lower critical threshold	Peripheral device '[EXTSENSORNAME]' in slot [EXTSENSORSLOT] asserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT].	Peripheral device '[EXTSENSORNAME]' in slot [EXTSENSORSLOT] deasserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT].
Peripheral Device Slot > * > State Sensor/Actuator > Unavailable	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' unavailable.	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' available.
Peripheral Device Slot > * > State Sensor/Actuator > Alarmed/Open/On	Peripheral device '[EXTSENSORNAME]' in slot [EXTSENSORSLOT] is [SENSORSTATENAME].	Peripheral device '[EXTSENSORNAME]' in slot [EXTSENSORSLOT] is [SENSORSTATENAME].
Peripheral Device Slot > * > State Sensor/Actuator > Switched by user	Peripheral device '[EXTSENSORNAME]' in slot [EXTSENSORSLOT] has been switched to [SENSORSTATENAME] by user '[USERNAME]' from host.	
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]'.	

Event/context	Default message when the event = TRUE	Default message when the event = FALSE
Inlet > * > Sensor > * > Normal	Sensor '[INLETSENSOR]' on inlet '[INLET]' entered normal state.	Sensor '[INLETSENSOR]' on inlet '[INLET]' exited normal 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.
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.

Event/context	Default message when the event = TRUE	Default message when the event = FALSE
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.
Outlet > * > Sensor > Outlet State > Unavailable	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' unavailable.	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' available.
Outlet Grouping > Outlet Group > * > Outlet Group Modified	Outlet group '[OUTLETGROUPID]' was modified.	
Outlet Grouping > Outlet Group > * > Power control > Power cycled	Outlet group '[OUTLETGROUPID]' power cycle initiated by user '[USERNAME]' from host '[USERIP]'.	
Outlet Grouping > Outlet Group > * > Power control > Powered off	Outlet group '[OUTLETGROUPID]' has been powered off by user '[USERNAME]' from host '[USERIP]'.	
Outlet Grouping > Outlet Group > * > Power control > Powered on	Outlet group '[OUTLETGROUPID]' has been powered on by user '[USERNAME]' from host '[USERIP]'.	
Outlet Grouping > Outlet Group Created	Outlet group '[OUTLETGROUPID]' was created.	
Outlet Grouping > Outlet Group Deleted	Outlet group '[OUTLETGROUPID]' was deleted.	
Overcurrent Protector > * > Sensor > * > Unavailable	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' unavailable.	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' available.

Event/context	Default message when the event = TRUE	Default message when the event = FALSE
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 > [MONITOREDHOST] > Power	Power control operation for '[MONITOREDHOST]' finished with result:	

Event/context	Default message when the event = TRUE	Default message when the event = FALSE
control completed	[SERVERPOWERRESULT]	
Server Monitoring > [MONITOREDHOST] > Power control initiated	User '[USERNAME]' initiated a power control operation for '[MONITOREDHOST]': [SERVERPOWEROPERATION]	
Server Monitoring > * > Unreachable	Server '[MONITOREDHOST]' is unreachable.	Server '[MONITOREDHOST]' is reachable.
Server Monitoring > * > Unrecoverable	Connection to server '[MONITOREDHOST]' could not be restored.	
User Activity > * > User logon state	User '[USERNAME]' from host '[USERIP]' logged in.	User '[USERNAME]' from host '[USERIP]' logged out.
User Activity > * > Authentication failure	Authentication failed for user '[USERNAME]' from host '[USERIP]'.	
User Activity > * > User accepted the Restricted Service Agreement	User '[USERNAME]' from host '[USERIP]" accepted the Restricted Service Agreement.	User '[USERNAME]' from host '[USERIP]" declined the Restricted Service Agreement.
User Activity > * > User blocked	User '[USERNAME]' from host '[USERIP]' was blocked.	
User Activity > * > Session timeout	Session of user '[USERNAME]' from host '[USERIP]' timed out.	
User Administration > User added	User '[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]'.	

Event/context	Default message when the event = TRUE	Default message when the event = FALSE
User Administration > Role deleted	Role '[UMTARGETROLE]' deleted by user '[USERNAME]' from host '[USERIP]'.	
Webcam Management > Image upload started	A snapshot upload of webcam '[WEBCAMNAME]' to folder '[PATH]' was started.	
Webcam Management > Webcam attached	Webcam '[WEBCAMNAME]' ('[WEBCAMUVCID]') added to port '[WEBCAMUSBPORT]'.	
Webcam Management > Webcam detached	Webcam '[WEBCAMNAME]' ('[WEBCAMUVCID]') removed from port '[WEBCAMUSBPORT]'.	
Webcam Management > Webcam settings changed	Webcam '[WEBCAMNAME]' settings changed by user '[USERNAME]'.	

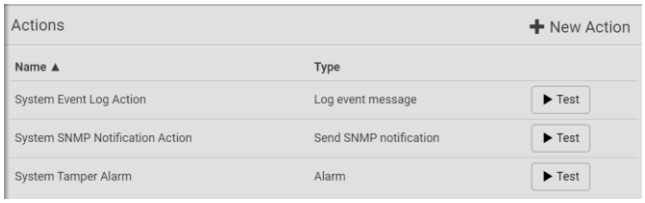
The asterisk symbol (*) represents anything you select for the 'trigger' events.

Available Actions

The PXC/PXO comes with three built-in actions, which cannot be deleted. You can create additional actions for responding to different events.

To test an action:

- Click the Test button next to the Action. The action is triggered and you can verify it.



Built-in actions:

- *System Event Log Action:*

  This action records the selected event in the internal log when the event occurs.

- *System SNMP Notification Action:*

  This action sends SNMP notifications to one or multiple IP addresses after the selected event occurs.

Note: No IP addresses are specified for this notification action by default so you must enter IP addresses before applying this action to any event rule. See **Editing or Deleting a Rule/Action** *(on page 302). 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 219).*

- *System Tamper Alarm:*

  This action causes the PXC/PXO to show the alarm for the Raritan tamper sensor, if any, on the Dashboard page until a person acknowledges it. By default, this action has been assigned to the built-in tamper detection event rules. For information on acknowledging an alarm, see ***Dashboard - Alarms*** (on page 115).

Actions you can create:

1. Choose Device Settings > Event Rules > ➕ New Action.
2. Click the Action field to select an action type from the list.

3. Below is the list of available actions.

Note: The "Change load shedding state", "Power control server" ,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 276).
Change load shedding state	Enters or quits the load shedding mode. See ***Change Load Shedding State*** (on page 277).
Execute an action group	Creates a group of actions comprising existing actions. See ***Action Group*** (on page 277).
Log event message	Records the selected events in the internal log. See ***Log an Event Message*** (on page 278).

Action	Function
Power control server	Two operations are available. ▪ Shuts down a monitored server and then powers off the outlet(s) associated with that server. ▪ Powers up the outlet(s) associated with a monitored server. See ***Shut down a Server and Control its Power*** (on page 278).
Push out sensor readings	Sends internal sensor log or environmental sensor log to a remote server using HTTP POST requests. See ***Push Out Sensor Readings*** (on page 279).
Record snapshots to webcam storage	Makes a connected webcam start or stop taking snapshots. See ***Record Snapshots to Webcam Storage*** (on page 279).
Send email	Emails a textual message. See ***Send Email*** (on page 281).
Send sensor report	Reports the readings or status of the selected sensors, including internal or external sensors. See ***Send Sensor Report*** (on page 283).
Send snapshots via email	Emails the snapshots captured by a connected Logitech® webcam (if available). See ***Send Snapshots via Email*** (on page 284).
Send SNMP notification	Sends SNMP traps or informs to one or multiple SNMP destinations. See ***Send an SNMP Notification*** (on page 286).
Start/stop Lua script	If you are a developer who can create a Lua script, you can upload it to the PXC/PXO, and have the PXC/PXO automatically perform or stop the script in response to an event. See ***Start or Stop a Lua Script*** (on page 288).
Switch outlets	Switches on, off or cycles the power to the specified outlet(s). See ***Switch Outlets*** (on page 289).
Switch outlet group	Switches on, off or cycles the power to all outlets of the specified outlet group. See ***Switch Outlet Group*** (on page 288).
Switch peripheral actuator	Switches on or off the mechanism or system connected to the specified actuator. See ***Switch Peripheral Actuator*** (on page 289).

Action	Function
Syslog message	Makes the PXC/PXO automatically forward event messages to the specified syslog server. See ***Syslog Message*** (on page 290).

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 259).

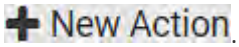
Alarm

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 PXC/PXO 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 107).

Operation:

1. Choose Device Settings > Event Rules > 

.
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 PXC/PXO 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 273).

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 PXC/PXO 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 130).

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 265).

Shut down a Server and Control its Power

The "Power control server" action is available only when your PXC/PXO is outlet-switching capable.

You can configure the PXC/PXO to shut down a specific server and then turn off its outlet(s), or turn on that server's outlet(s) after a certain event occurs.

The only restriction is a server must be one of the servers being monitored by your PXC/PXO and the same PXC/PXO supplies power to it. To have any server monitored, see ***Monitoring Server Accessibility*** (on page 316).

Tip: If the server has multiple power cords, make sure all of its power cords are connected to the same PXC/PXO and you have created an outlet group for controlling all outlets simultaneously. See **Outlet Groups** *(on page 137).*

Operation:

1. Choose Device Settings > Event Rules >

.
2. Select 'Power control server' from the Action list.
3. In the Operation field, select an action for the server.
   - Power up: Turns on the outlet or outlet group associated with the selected server.
   - Graceful shutdown: Shuts down the selected server first and then turn off its associated outlet or outlet group.
4. Select the server you want in the Server field.
   - If PXC/PXO cannot power control any server, a message 'Power control not configured' is shown in the end of the server's host name or IP address.

Push Out Sensor Readings

You can configure the PXC/PXO to push sensor log to a remote server after a certain event occurs, including logs of internal sensors, environmental sensors and actuators.

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 311).

Tip: To send the data at a regular interval, schedule this action. See **Scheduling an Action** *(on page 291).*

Operation:

1. Choose Device Settings > Event Rules > + New Action.
2. Select 'Push out sensor readings' from the Action list.
3. Select a server or host which receives the data in the Destination field.
   - If the desired destination is not available yet, go to the Data Push page to specify it.

Record Snapshots to Webcam Storage

This option allows you to define an action that starts or stops a specific webcam from taking snapshots.

Per default the snapshots are stored on the PXC/PXO. See ***Viewing and Managing Locally-Saved Snapshots*** (on page 363).

It is recommended to specify a remote server to store as many snapshots as possible. See ***Changing Storage Settings*** (on page 365).

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 PXC/PXO is 10. If you set it for a number greater than 10 and the storage location is on the PXC/PXO, after the 10th snapshot is taken and stored, the oldest snapshots are overwritten. Storing snapshots on a remote server does not have such a limitation.
   - Time before first snapshot - the amount of time in seconds between when the event is triggered and the webcam begins taking snapshots.
   - Time between snapshots - the amount of time in seconds between when each snapshot is taken.

- Folder - names of the folders that will be automatically created to store webcam snapshots after the recording action is triggered by the rule you will configure.

  Note that the Folder field is available only when the selected webcam has been configured to store its snapshots on an "FTP" server. See ***Changing Storage Settings*** (on page 365).

Folder name options	Definition
Serial number / Webcam name	Two folders will be created. ▪ The parent folder's name is the serial number of PXC/PXO. ▪ The subfolder's name is the selected webcam's name.
Serial number / Webcam name / Rule name	Three folders will be created. ▪ Definitions of the parent folder and first subfolder are the same as the first row. ▪ The final subfolder's name is the name of event rule that triggers this recording action.
Serial number / Webcam name / Timestamp	Three folders will be created. ▪ Definitions of the parent folder and first subfolder are the same as the first row. ▪ The final subfolder's name is the time when the recording event occurs, which is the accumulated time in seconds since 1970/1/1.
Serial number / Webcam name / Rule name / Timestamp	Four folders will be created. ▪ Definitions of the parent folder and first subfolder are the same as the first row. ▪ The second subfolder's name is the name of event rule that triggers this recording action. ▪ The final subfolder's name is the time when the recording event occurs, which is the accumulated time in seconds since 1970/1/1.
Serial number / Webcam name / Formatted timestamp	Three folders will be created. ▪ Definitions of the parent folder and first subfolder are the same as the first row. ▪ The final subfolder's name is the time when the recording event occurs, which is a format comprising year, month, date, hour, minute, second and timezone.
Serial number / Webcam name / Rule name / Formatted timestamp	Four folders will be created. ▪ Definitions of the parent folder and first subfolder are the same as the first row. ▪ The second subfolder's name is the name of event rule that triggers this recording action. ▪ The final subfolder's name is the time when the recording event occurs, which is a format comprising year, month, date, hour, minute, second and timezone.

No matter which timestamp you choose, the timestamp is based on the time you have configured on the PXC/PXO. See ***Setting the Date and Time*** (on page 251).

To find the serial number of your PXC/PXO, see ***Device Information*** (on page 333). To change the webcam's name, see ***Configuring Webcams and Viewing Live Images*** (on page 358).

Tip: If you choose "Timestamp" as the final subfolder's name and do not understand the occurrence time indicated by the timestamp, you can always easily convert it to a readable formatted time by googling Unix timestamp converter.

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 PXC/PXO placeholders. The placeholders represent information which is pulled from the PXC/PXO and inserted into the message.

For example:

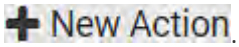
```
[USERNAME] logged into the device on [TIMESTAMP]
```

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 299).

Operation:

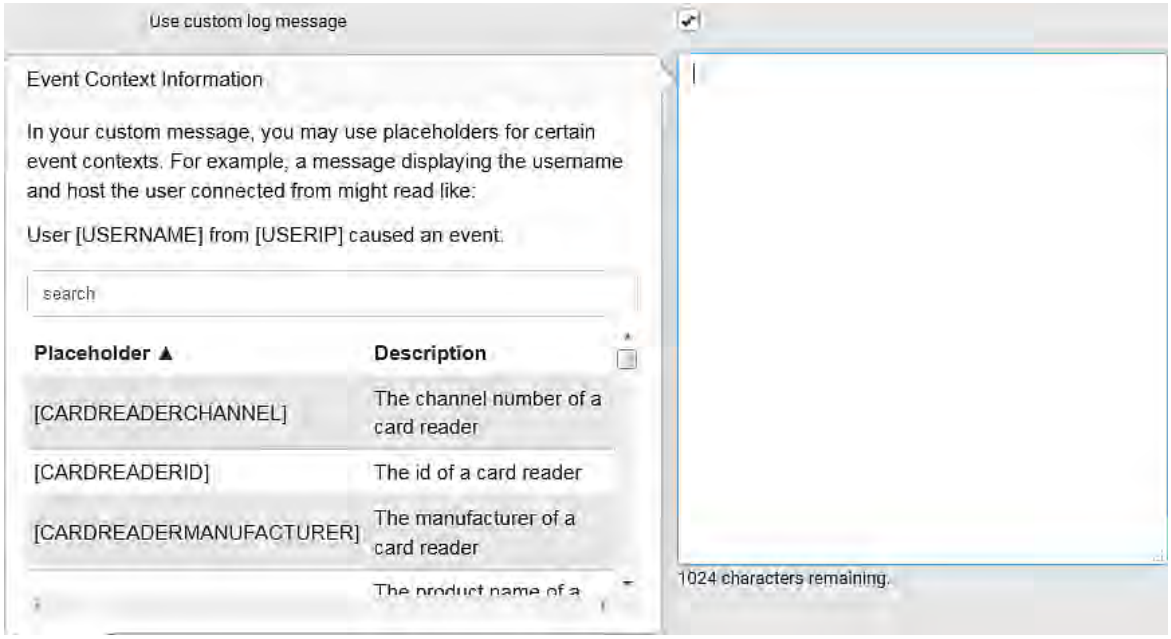
1. Choose Device Settings > Event Rules > 

.
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 221).

   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 265).
5. If needed, you can customize the subject and messages sent via this email.
   - Select the 'Custom subject' checkbox, and enter the text you prefer as this email's subject.

6. 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 299).



   - 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.

Raritan
A brand of legrand

Send Sensor Report

You may set the PXC/PXO 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 PXC/PXO, such as temperature or humidity sensors.

An example of this action is available in the section titled ***Send Sensor Report Example*** (on page 293).

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:

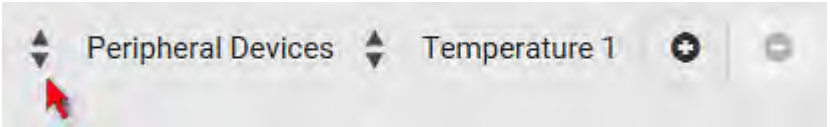
   - Log event message
   - Syslog message
   - Send email
4. If no messaging actions are available, create them now. See ***Available Actions*** (on page 273).
   a. To select any methods, select them one by one in the Available field.

      To add all available methods, simply click Select All.

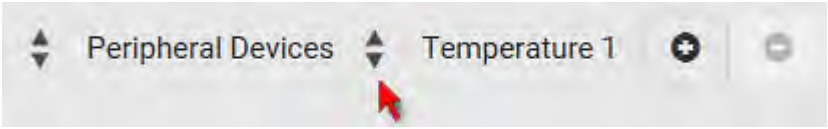
   b. To delete any methods, click a method's ✖ in the Selected field.

      To remove all methods, simply click Deselect All.
5. In the 'Available sensors' field, select the desired target's sensor.

   a. Click the first ⇕ to select a target component from the list.

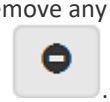


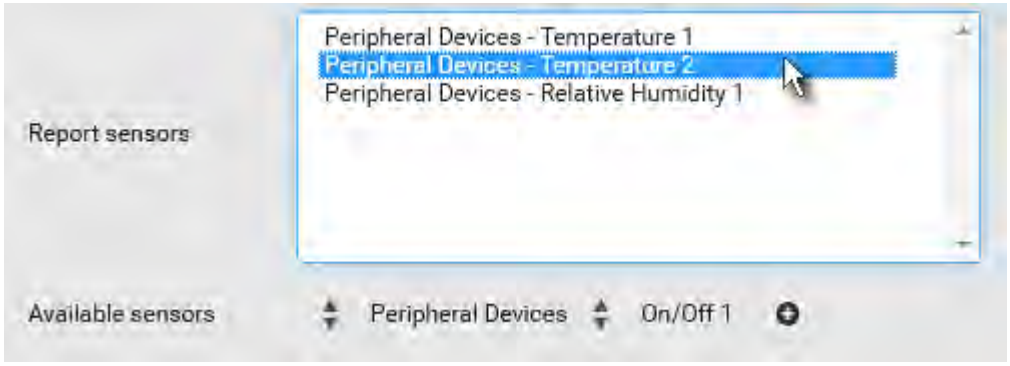
b. Click the second to select the specific sensor for the target from the list.



c. Click to add the selected sensor to the Report Sensors list box.

For example, to monitor the current reading of the Inlet 1, select Inlet 1 from the left field, and then select RMS Current from the right field.

6. To report additional sensors simultaneously, repeat the above step to add more sensors.
   - To remove any sensor from the 'Report sensors' list box, select it and click  . To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.



   - 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 299).*

Send Snapshots via Email

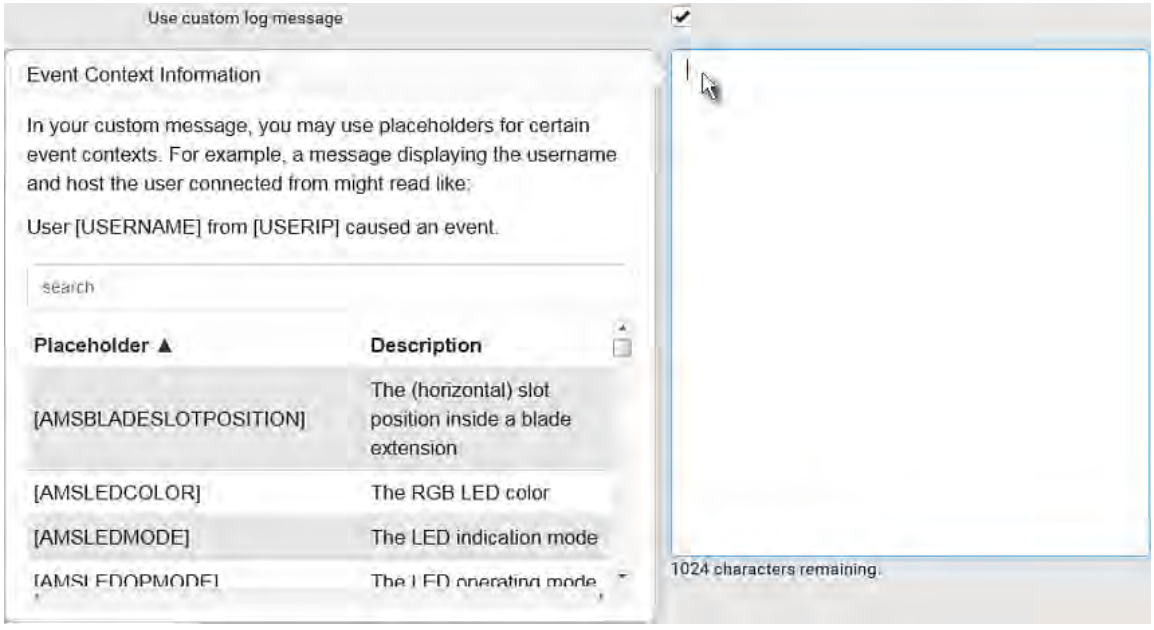
This option notifies one or multiple persons for the selected events by emailing snapshots or videos captured by a connected Logitech® webcam.

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 221).
5. Select the webcam that is capturing the images you want sent in the email.
6. Adjust the values of the following:
   - Number of snapshots - the number of snapshots to be taken when the event occurs. For example, you can specify 10 images be taken once the event triggers the action.
   - Snapshots per mail - the number of snapshots to be sent at one time in the email.
   - Time before first snapshot - the amount of time in seconds between when the event is triggered and the webcam begins taking snapshots.
   - Time between snapshots - the amount of time in seconds between when each snapshot is taken.
7. If needed, you can customize the subject and messages sent via this email.
   - Select the 'Custom subject' checkbox, and enter the text you prefer as this email's subject.
   - Select the 'Use custom log message' checkbox, and then create a custom message up to 1024 characters in the provided field.



   - To start a new line in the text box, press Enter.

Note: In case you need to type any square brackets "[" and "]" in the custom message for non-placeholder words, always add a backslash in front of the square bracket. That is, \[or \]. Otherwise, the message sent will not display the square brackets.

Send an SNMP Notification

This option sends an SNMP notification to one or multiple SNMP destinations.

Operation:

1. Choose Device Settings > Event Rules > + New Action.
2. Select 'Send SNMP notification' from the Action list.
3. Select the type of SNMP notification. See either procedure below according to your selection.

To send SNMP v2c notifications:

1. In the 'Notification type' field, select 'SNMPv2c trap' or 'SNMPv2c inform.'
2. For SNMP INFORM communications, leave the resend settings at their default or do the following:
   a. In the Timeout field, specify the interval of time, in seconds, after which a new inform communication is resent if the first is not received. For example, resend a new inform communication once every 3 seconds.
   b. In the 'Number of retries' field, specify the number of times you want to re-send the inform communication if it fails. For example, inform communications are re-sent up to 5 times when the initial communication fails.
3. In the Host fields, enter the IP address of the device(s) you want to access. This is the address to which notifications are sent by the SNMP system agent.
4. In the Port fields, enter the port number used to access the device(s).
5. In the Community fields, enter the SNMP community string to access the device(s). The community is the group representing the PXC/PXO 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.

Raritan
A brand of legrand

3. For SNMP INFORM communications, leave the resend settings at their default or do the following:
   a. In the Timeout field, specify the interval of time, in seconds, after which a new inform communication is resent if the first is not received. For example, resend a new inform communication once every 3 seconds.
   b. In the 'Number of retries' field, specify the number of times you want to re-send the inform communication if it fails. For example, inform communications are re-sent up to 5 times when the initial communication fails.
4. For both SNMP TRAPS and INFORMS, enter the following as needed and then click OK to apply the settings:
   a. Host name
   b. Port number
   c. User ID for accessing the host -- make sure the User ID has the SNMPv3 permission.
   d. Select the host security level

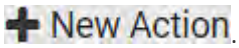
Security level	Description
"noAuthNoPriv"	Select this if no authorization or privacy protocols are needed.
"authNoPriv"	Select this if authorization is required but no privacy protocols are required. • Select the authentication protocol - MD5 or SHA • Enter the authentication passphrase and then confirm the authentication passphrase
"authPriv"	Select this if authentication and privacy protocols are required. • Select the authentication protocol - MD5 or SHA • Enter the authentication passphrase and confirm the authentication passphrase • Select the Privacy Protocol - DES or AES • Enter the privacy passphrase and then confirm the privacy passphrase

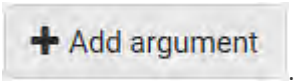
Start or Stop a Lua Script

If you have created or loaded a Lua script file into the PXC/PXO, 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 324).

To automatically start or stop a Lua script:

1. Choose Device Settings > Event Rules > 

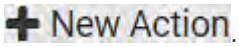
.
2. Select 'Start/stop Lua script' from the Action list.
3. In the Operation field, select 'Start script' or 'Stop script.'
4. In the Script field, select the script that you want it to be started or stopped when an event occurs.
   - No script is available if you have not created or loaded it into the PXC/PXO.
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 

.
   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 Outlet Group

The "Switch outlet group" action is available only when your PXC/PXO is outlet-switching capable. This action turns on, off or power cycles a specific outlet group.

Operation:

1. Choose Device Settings > Event Rules > 

.
2. Select 'Switch outlet group' from the Action list.
3. To specify the outlet group where this action will be applied, select it from the 'Group to switch' list.
4. In the Operation field, select an operation for the selected outlet group.
   - Turn on all outlets in group: Turns on the selected outlet group.
   - Turn off all outlets in group: Turns off the selected outlet group.
   - Cycle all outlets in group: Cycles power to the selected outlet group.

Switch Outlets

The "Switch outlets" action is available only when your PXC/PXO 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 123).

Switch Peripheral Actuator

If you have any actuator connected to the PXC/PXO, you can set up the PXC/PXO so it automatically turns on or off the system controlled by the actuator when a specific event occurs.

Note: For information on connecting actuators, see **DX2 Sensor Packages** *(on page 35).*

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.

PXC/PXO 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 339).

Operation:

1. Choose Device Settings > Event Rules > ✚ New Action.
2. Select 'Syslog message' from the Action list.
3. In the 'Syslog server' field, specify the IP address to which the syslog is forwarded.
4. In the 'Transport protocol' field, select one of the syslog protocols: TCP, UDP or TCP+TLS. The default is UDP.

Transport protocols	Next steps
UDP	▪ In the 'UDP port' field, type an appropriate port number. Default is 514. ▪ Select the 'Legacy BSD syslog protocol' checkbox if applicable.
TCP	NO TLS certificate is required. Type an appropriate port number in the 'TCP port' field.
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 702).*

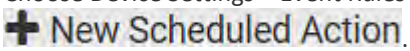
Scheduling an Action

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 PXC/PXO 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 273).

Operation:

1. Choose Device Settings > Event Rules > 

2. To select any action(s), select them one by one from the 'Available actions' list.
   - To select all available actions, click Select All.
3. To remove any action(s) from the 'Selected actions' field, click that action's .
   - To remove all actions, click Deselect All.
4. Select the desired frequency in the 'Execution time' field, and then specify the time interval or a specific date and time in the field(s) that appear.

Execution time	Frequency settings
Minutes	Click the Frequency field to select an option. The frequency ranges from every minute, every 5 minutes, every 10 minutes and so on until every 30 minutes.
Hourly	Type a value in the Minute field, which is set to either of the following: ▪ The Minute field is set to 0 (zero). Then the action is performed at 1:00 am, 2:00 am, 3:00 am and so on. ▪ The Minute field is set to a non-zero value. For example, if it is set to 30, then the action is performed at 1:30 am, 2:30 am, 3:30 am and so on.
Daily	Type values or click ▲ ▼. The time is measured in 12-hour format so you must correctly specify AM or PM by clicking the AM/PM button. For example, if you specify 01:30PM, the action is performed at 13:30 pm every day.
Weekly	Both the day and time must be specified for the weekly option. ▪ Days range from Sunday to Saturday. ▪ The time is measured in 12-hour format so you must correctly specify AM or PM by clicking the AM/PM button.
Monthly	Both the date and time must be specified for the monthly option. ▪ The dates range from 1 to 31. ▪ The time is measured in 12-hour format so you must correctly specify AM or PM by clicking the AM/PM button. Note that NOT every month has the date 31, and February in particular does not have the date 30 and probably even 29. Check the calendar when selecting 29, 30 or 31.
Yearly	This option requires three settings: ▪ Month - January through December. ▪ Day of month - 1 to 31. ▪ Time - the value is measured in 12-hour format so you must correctly specify AM or PM by clicking the AM/PM button.

An example of the scheduled action is available in the section titled ***Send Sensor Report Example*** (on page 293).

Raritan
A brand of legrand

Send Sensor Report Example

To create a scheduled action for emailing a temperature sensor report hourly, it requires:

- A 'Send email' action
- A 'Send sensor report' action
- A timer - that is, the scheduled action

Steps:

1. Click

to create a 'Send email' action that sends an email to the desired recipient(s). For details, see ***Send Email*** (on page 281).
   - In this example, this action is named *Email a Sensor Report*.

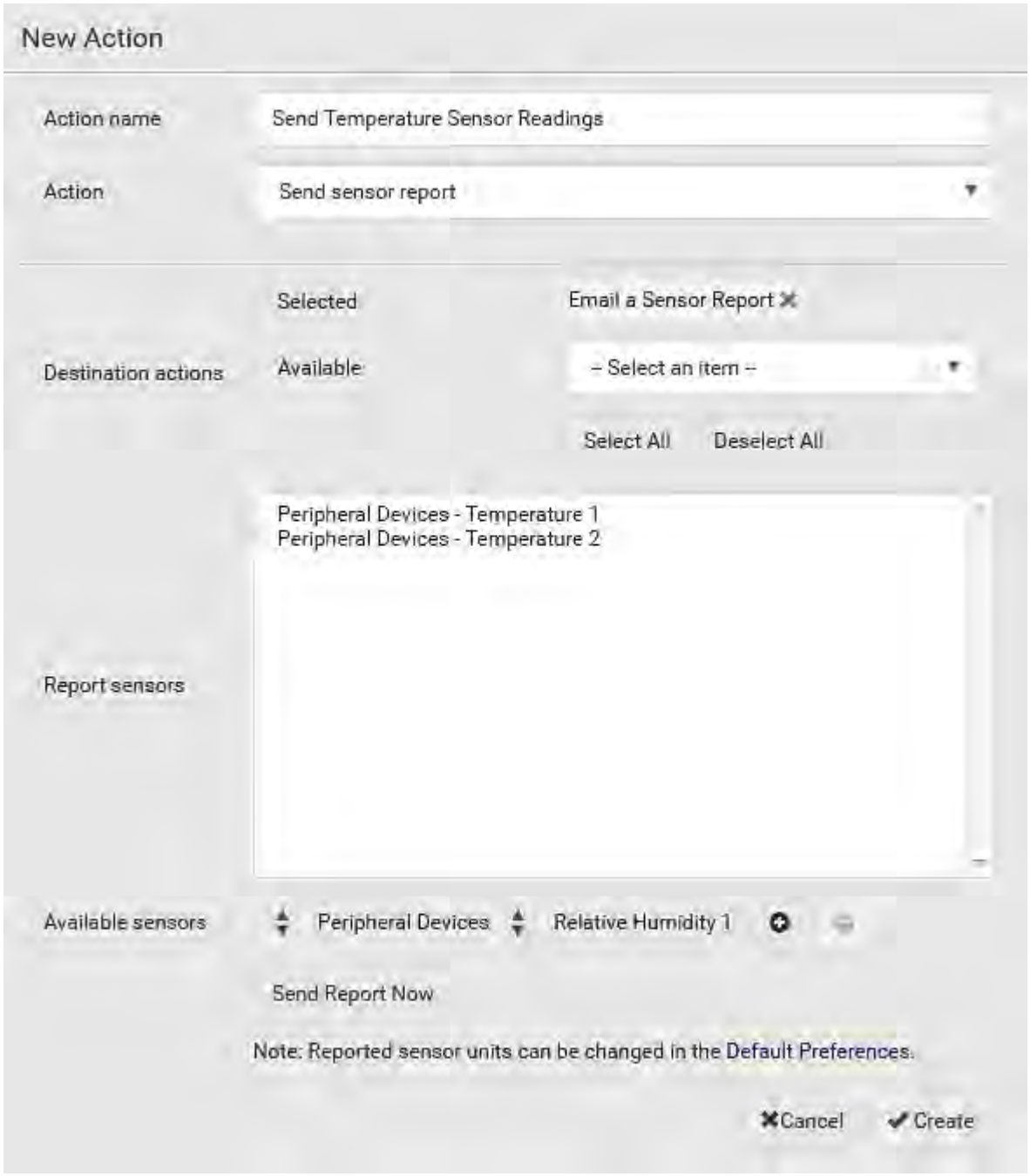
- If wanted, you can customize the subject and content of this email in this action.

New Action
Action name
Email a Sensor Report
Action
Send email
Recipient email addresses
IT-manager@raritan.com
SMTP server
Use default settings
Server name: 192.168.5.50
Sender email address: manager@raritan.com
Settings can be changed in SMTP Server settings.
Use custom settings
Custom subject
Sensor Report: [EXTSENSOR] - [EXTSENSORNAME]
Use custom log message
Custom log message
The following is the complete sensor report –
[SENSORREPORT]
962 characters remaining.
Cancel
Create

2. Click

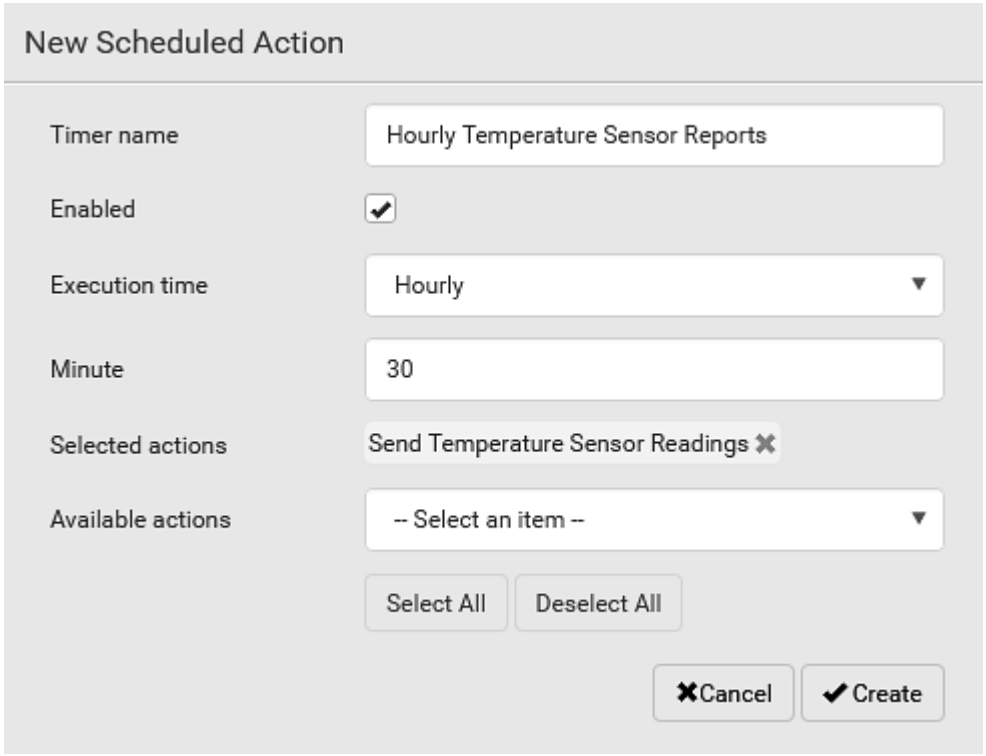
to create a 'Send sensor report' action that includes the 'Email a Sensor Report' action as its destination action. For details, see ***Send Sensor Report*** (on page 283).
   - In this example, this action is named *Send Temperature Sensor Readings*.

- You can specify more than one temperature sensor as needed in this action.



3. Click **+ New Scheduled Action** to create a timer for performing the 'Send Temperature Sensor Readings' action hourly. For details, see ***Scheduling an Action*** (on page 291).

- 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 PXC/PXO will send out an email containing the specified temperature sensor readings hourly every day.

Whenever you want the PXC/PXO to stop sending the temperature report, deselect the Enabled checkbox in the timer.

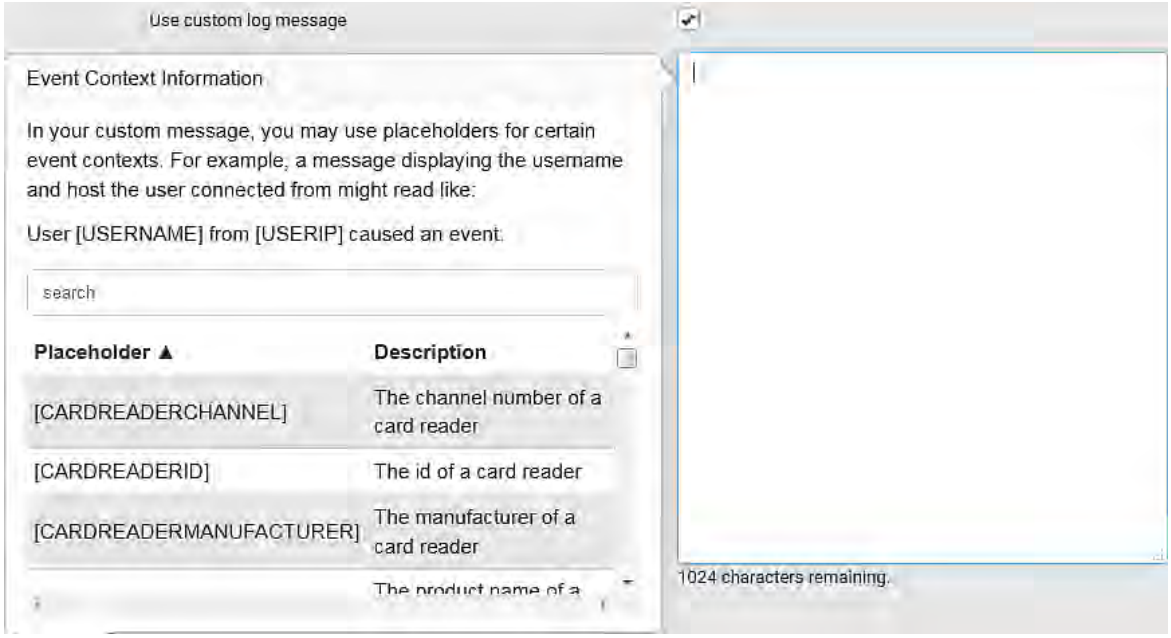
Raritan
A brand of legrand

Placeholders for Custom Messages

The action "Send email" allows you to customize event messages. See ***Send Email*** (on page 281).

When clicking anywhere inside the text box, the Event Context Information displays, showing a list of placeholders and their definitions. Simply drag the scroll bar and then click the desired placeholder to insert it into the custom message. Or you can type a keyword in the "search" box to quickly find the desired placeholder.

Note that available placeholders are model dependent.



If wanted, you can resort the list by clicking the desired column header. See ***Sorting a List*** (on page 106).

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
[CARDREADERCHANNEL]	The channel number of a card reader
[CARDREADERID]	The id of a card reader
[CARDREADERMANUFACTURER]	The manufacturer of a card reader
[CARDREADERPRODUCT]	The product name of a card reader
[CARDREADERSERIALNUMBER]	The serial number of a card reader

Placeholder	Definition
[COMPONENTID]	The ID of a hardware component
[CONFIGPARAM]	The name of a configuration parameter
[CONFIGVALUE]	The new value of a parameter
[DATETIME]	The human readable timestamp of the event occurrence
[DEVICEIP]	The IP address of the device the event occurred on
[DEVICENAME]	The name of the device the event occurred on
[DEVICESERIAL]	The unit serial number of the device the event occurred on
[ERRORDESC]	The error message
[EVENTRULENAME]	The name of the matching event rule
[EXTSENSOR]	The peripheral device identifier
[EXTSENSORNAME]	The name of a peripheral device
[EXTSENSORSLOT]	The ID of a peripheral device slot
[FAILURETYPE]	The numeric hardware failure type
[FAILURETYPESTR]	The textual hardware failure type
[IFNAME]	The human readable name of a network interface
[INLET]	The inlet label
[INLETPOLE]	The inlet power line identifier
[INLETSENSOR]	The inlet sensor name
[ISASSERTED]	Boolean flag whether an event condition became true (1) or false (0)
[LDAPERRORDESC]	The LDAP error occurred
[LOGMESSAGE]	The original log message
[MONITOREDHOST]	The name or IP address of a monitored host
[NETAUTHRESULTSTR]	The network authentication result string ('succeeded' or 'failed')
[OCP]	The overcurrent protector label
[OCPSENSOR]	The overcurrent protector sensor name
[OCPTRIPCAUSELABEL]	The label of the outlet that likely caused the OCP trip

Raritan
A brand of legrand

Placeholder	Definition
[OLDVERSION]	The firmware version the device is being upgraded from
[OUTLET]	The outlet label
[OUTLETGROUPID]	The outlet group ID
[OUTLETGROUPNAME]	The outlet group name
[OUTLETGROUPSENSOR]	The outlet group sensor name
[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
[PERIPHDEVPOSITION]	The position of an attached peripheral device
[PHONENUMBER]	The destination phone number of an outgoing SMS message
[PORTID]	The label of the external port the event-triggering device is connected to
[PORTTYPE]	The type of the external port (e.g. 'feature' or 'auxiliary') the event-triggering device is connected to
[RADIUSERRORDESC]	The Radius error message
[ROMCODE]	The romcode of an attached peripheral device
[SENSORREADING]	The value of a sensor reading
[SENSORREADINGUNIT]	The unit of a sensor reading
[SENSORREPORT]	The formatted sensor report contents
[SENSORSTATENAME]	The human readable state of a sensor
[SENSORTHRESHOLDNAME]	The name of the threshold being crossed
[SENSORTHRESHOLDVALUE]	The value of the threshold being crossed
[SERVERPOWEROPERATION]	The power control operation that was initiated on a server (on/off)
[SERVERPOWERRESULT]	The result of a power control operation

Placeholder	Definition
[SMARTCARDID]	The id of a smart card
[SMARTCARDTYPE]	The type of a smart card
[SMTPRECIPIENTS]	The list of recipients of an outgoing mail
[SMTPSERVER]	The name or IP address of an SMTP server
[SYSCONTACT]	SNMP MIB-II sysContact field
[SYSLOCATION]	SNMP MIB-II sysLocation field
[SYSNAME]	SNMP MIB-II sysName field
[TIMEREVENTID]	The id of a timer event
[TIMESTAMP]	The timestamp of the event occurrence
[UMTARGETROLE]	The target role of a user management operation
[UMTARGETUSER]	The target user of a user management operation
[USERIP]	The IP address a user connected from
[USERNAME]	The user who performed an operation
[VERSION]	The firmware version the device is upgrading to

Note: In case you need to type any square brackets "[" and "]" in the custom message for non-placeholder words, always add a backslash in front of the square bracket. That is, \[or \]. Otherwise, the message sent will not display the square brackets.

Editing or Deleting a Rule/Action

You can change the settings of an event rule, action or scheduled action, or delete them.

Exception: Some settings of the built-in event rules or actions are not user-configurable. You cannot delete built-in rules and actions. See **Built-in Rules and Rule Configuration** *(on page 260) or* **Available Actions** *(on page 273).*

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.

Raritan
A brand of legrand

- 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

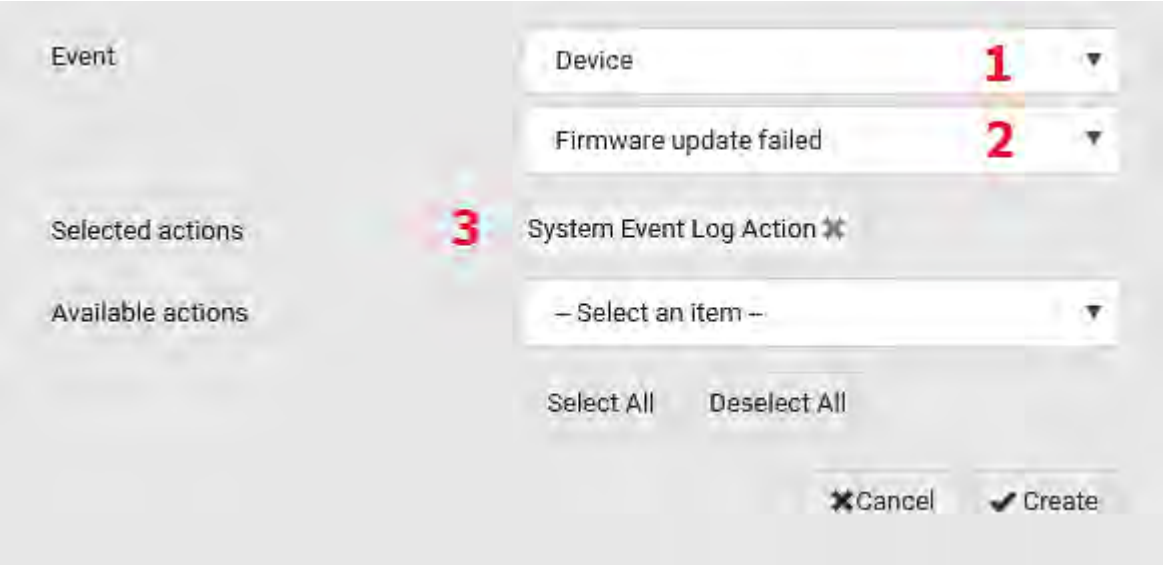
In this example, we want the PXC/PXO to record the firmware upgrade failure in the internal log when it happens.

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 PXC/PXO responds to the event related to firmware upgrade failure.
3. To make PXC/PXO record the firmware update failure event in the internal log, select "System Event Log Action" in the 'Available actions' field.



Sample Outlet-Level Event Rule

In this example, we want the PXC/PXO to send SNMP notifications to the SNMP manager for any sensor change event of outlet 3.

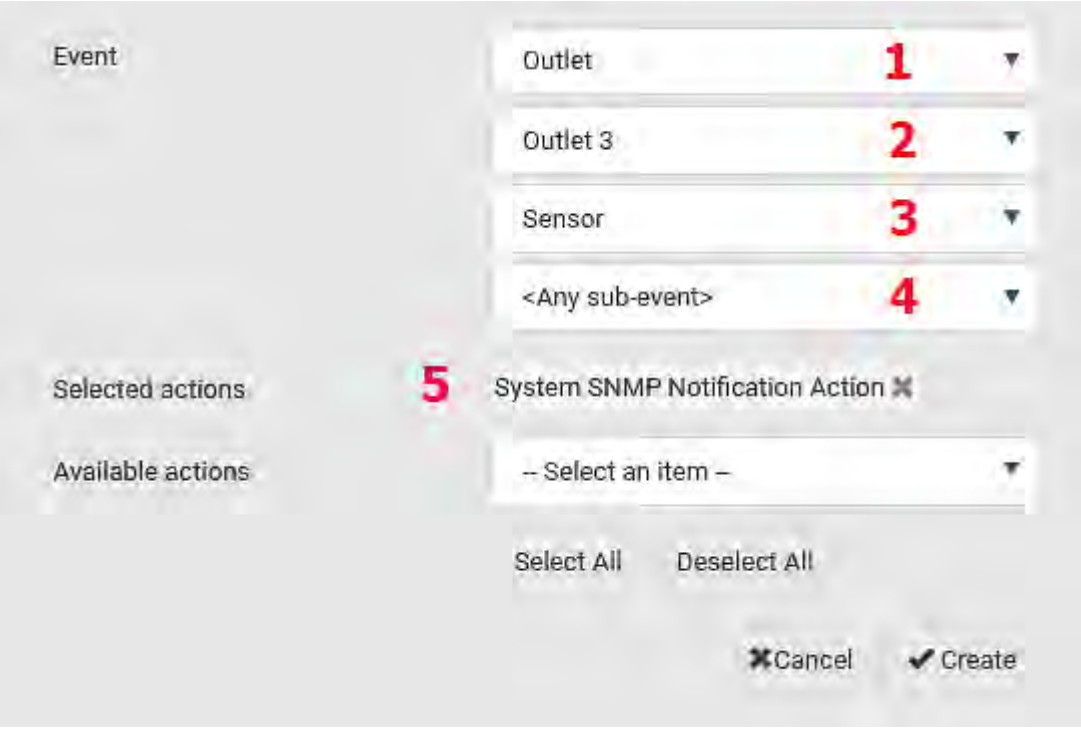
The event rule involves:

- 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 PXC/PXO 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 378).*



Then the SNMP notifications are sent when:

Raritan
A brand of legrand

- 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 PXC/PXO 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 PXC/PXO send SNMP notifications, select "System SNMP Notification Action" in the 'Available actions' box.

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 378).*

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

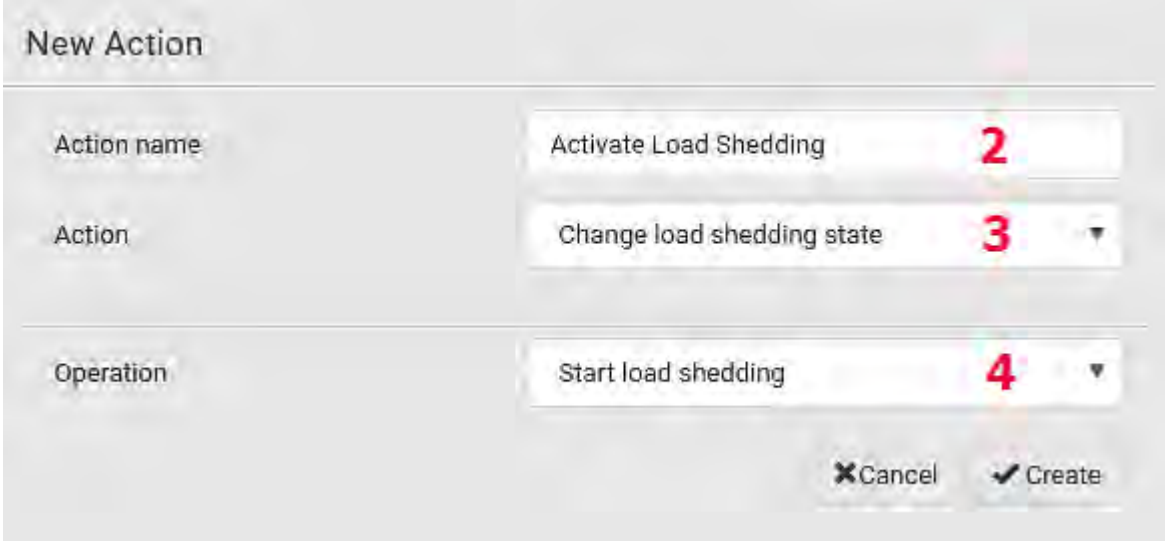
This section applies to outlet-switching capable models only.

In this example, we want PXC/PXO 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:

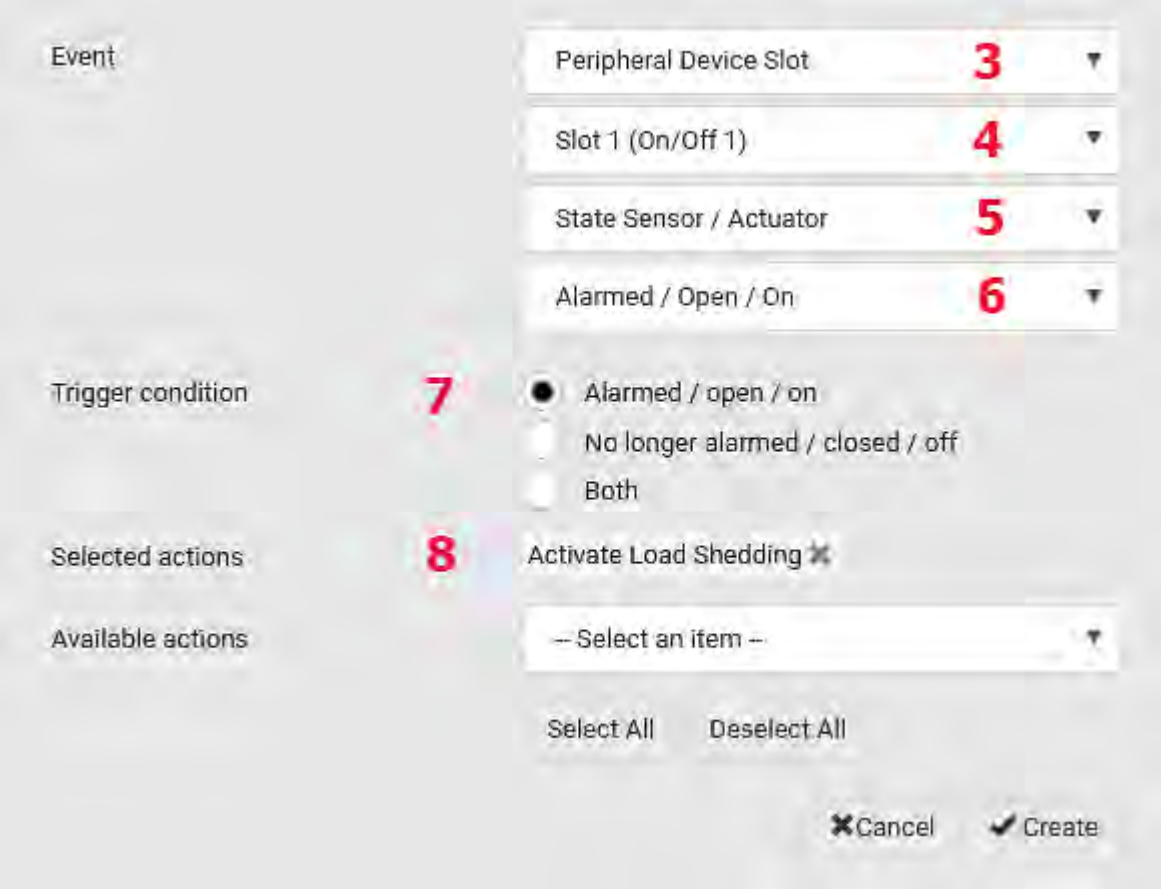
- Event: Peripheral Device Slot > Slot 1 > State Sensor/Actuator > Alarmed/Open/On
- Trigger condition: Alarmed
- Action: Activate Load Shedding

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 154).*
5. Select "State Sensor/Actuator" because the contact closure sensor is a state sensor.

6. Select "Alarmed" since we want the PXC/PXO 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 PXC/PXO 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.

Raritan
A brand of legrand

Example 1

This example illustrates an event rule which continuously causes the PXC/PXO 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 PXC/PXO 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

Example 3

This example illustrates a situation where two event rules combined regarding the outlet state changes causes the PXC/PXO 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 PXC/PXO to generate an alert. The measurement then returns to a value within the threshold, but the PXC/PXO does not generate an alert message for the Deassertion event. Such scenarios can occur due to the hysteresis tracking the PXC/PXO uses. See ***"To De-assert" and Deassertion Hysteresis*** (on page 681).

Setting Data Logging

The PXC/PXO 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 PXC/PXO 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 PXC/PXO device's SNMP agent must be enabled for this feature to work. See **Enabling and Configuring SNMP** *(on page 378). 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.

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 PXC/PXO, 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 destination and authentication for data push have to be configured properly on the PXC/PXO.

The data will be sent in JSON format using HTTP POST requests. For more information on its format, see ***Data Push Format*** (on page 312).

After configuring the destination and authentication settings, do either or both of the following:

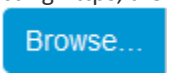
- To perform the data push after the occurrence of a certain event, create the data push action and assign it to an event rule.
- To push the data at a regular interval, schedule the data push action.

  See ***Event Rules and Actions*** (on page 259).

To configure data push settings:

1. Choose Device Settings > Data Push.
2. To specify a destination, click

.
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 

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 702).*
5. If the destination server requires authentication, select the 'Use authentication' checkbox, and enter the following data.
   - User name comprising up to 64 characters
   - Password comprising up to 128 characters
6. In the 'Entry type' field, determine the data that will be transmitted.
   - *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 310).
7. Click Create.
8. Repeat the same steps for additional destinations. Up to 64 destinations are supported.

To immediately push out the data:

1. On the Data Push page, choose the one whose data you want to push out.
2. Click its

.

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

, and then confirm it on the confirmation message.

Data Push Format

Each push message contains exactly one JSON object. The data format is formally defined in IDL files, sharing several definitions from the JSON-RPC data model.

IDL files are available by launching ***JSON-RPC online help*** (***https://help.raritan.com/json-rpc/pdu//namespacedatapush.html***).

To have an overview of the data format, see the following topic.

- ***Sensor Log*** (on page 313)

Raritan
A brand of legrand

Sensor Log

The root object of the message is a `SensorLogPushMessage` structure. It comprises a list of sensor descriptors and a list of log rows.

Sensor descriptors:

The sensor descriptor vector contains static information of all logged sensors, including:

- The electrical component a sensor is associated with. For example, an inlet pole or an overcurrent protector.
- The sensor's type. For example, RMS current or active energy.
- Unit and range of the sensor's readings.

See ***Sensor Descriptors for Inlet Active Power*** (on page 314)

Log rows:

Each log row consists of a time stamp (accumulated seconds since 1/1/1970) and a list of log records -- one for each logged sensor.

The length and order of the record list is the same as the sensor descriptor vector.

See ***Log Rows*** (on page 315).

Sensor Descriptors for Inlet Active Power

The following illustrates a descriptor for an inlet active power sensor.

The `metadata` field is relevant only to numeric sensors so the `readingtype` field is displayed twice in the illustration.

Note that a Raritan-provided explanation, which is the comment beginning with // in each line, is added to the following illustration for you to understand it better.

```
{
    "device": {
        "type": 0,              // Inlet sensor (see DeviceType enumeration)
        "label": "I1",          // Inlet label: I1
        "line": 0               // Power line; not applicable for inlet sensors
    },
    "id": "activePower",        // Sensor identification
    "readingtype": 0,           // Reading type: numeric
    "metadata": {
        "type": {
            "readingtype": 0,   // Reading type: numeric
            "type": 5,          // Sensor type: Active power
            "unit": 3           // Reading unit: Watt
        },
        "decdigits": 0,         // No decimal digits
        "accuracy": 1.0,        // Accuracy: 1 percent
        "resolution": 1.0,      // Reading resolution: 1 W
        "tolerance": 1.5,       // Reading tolerance: +/- 1.5 W
        "range": {
            "lower": 0.0,       // Minimum reading: 0 W
            "upper": 30000.0    // Maximum reading: 30 kW
        }
    }
}
```


Raritan
A brand of legrand

Log Rows

The following illustrates log rows with only one sensor record shown.

The actual length and order of log rows will be the same as those of sensors descriptors.

Note that a Raritan-provided explanation, which is the comment beginning with // in each line, is added to the following illustration for you to understand it better.

```
{
    "timestamp": 1334052852,            // Time stamp (seconds since 1/1/1970)
    "records": [
        {
            "available": true,          // This record is available
            "takenValidSamples": 60,    // Number of valid samples in this log period
            "state": 5,                 // Sensor was in normal range
            "minValue": 5800.0,         // Minimum sensor value: 5.8 kW
            "avgValue": 5900.0,         // Average sensor value: 5.9 kW
            "maxValue": 6100.0          // Maximum sensor value: 6.1 kW
        },
        {
            // [...] record for next sensor
        }
    ]
}
```

Monitoring Server Accessibility

You can monitor whether specific IT devices are alive by having the PXC/PXO 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.

PXC/PXO can monitor any IT device, such as database servers, remote authentication servers, power distribution units (PDUs), and so on. It supports monitoring a maximum of 64 IT devices.

To perform this feature, you need the Administrator Privileges.

The default ping settings may not be suitable for monitoring devices that require high connection reliability so it is strongly recommended that you should adjust the ping settings for optimal results.

In addition, if your PXC/PXO is outlet switching capable, you can even connect a monitored IT device to one or multiple outlets of PXC/PXO and then have PXC/PXO perform the following two actions as needed, in addition to monitoring its status:

- First shut down the monitored IT device.
- After the IT device is shut down, power off the outlet(s) where that device is connected.

Important: Not every IT device can be shut down by PXC/PXO so it is suggested to verify whether the device can be shut down using a shutdown command. For example, PXC/PXO cannot shut down a PDU with a shutdown command.

Tip: To make the PXC/PXO 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 259). An example is available in* **Example: Ping Monitoring and SNMP Notifications** *(on page 321).*

To add IT equipment for ping monitoring:

1. Choose Device Settings > Server Reachability.
2. Click

.
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.

Field	Description
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 PXC/PXO resumes pinging after the monitored equipment is declared "Unreachable." Valid range is 1 to 1200 (seconds).
Number of consecutive failures before disabling feature (0 = unlimited)	The number of times the monitored equipment is declared "Unreachable" consecutively before the PXC/PXO disables the ping monitoring feature for it and shows "Waiting for reliable connection." Valid range is 0 to 100.

5. On a PDU with outlet switching capability, there is one more checkbox available -- *Power control enabled*.

   To be able to shut down and power control the monitored IT device via the Server Reachability page, enable this checkbox and configure related settings, which are explained in the following table.
6. Click Create.
7. To add more IT devices, repeat the same steps.

To configure the shutdown and power control settings:

Restriction: To make the power control feature work properly, the power cord(s) of the monitored IT device must be connected to the "same" PDU which is monitoring the IT device.

Field	Description
Shutdown command	This is the command which is sent to the monitored IT device via SSH for shutting it down after you press the Shutdown button on PXC/PXO. ▪ *GNU/Linux*: This option sends the GNU/Linux shutdown command. ▪ *Windows*: This option sends the Windows shutdown command. ▪ *Custom*: If the monitored device's system is neither GNU/Linux nor Windows, choose this option to specify a proper shutdown command, which can comprise a maximum of 1024 ASCII characters.
User name, Password	Specify user credentials for logging in to the monitored device via SSH. ▪ *User name*: The name comprises up to 128 non-empty ASCII characters. ▪ *Password*: The password comprises up to 128 ASCII characters.
SSH port	The monitored device's SSH port. ▪ Default is 22.
Power target to switch	Select the outlet or outlet group that is powering the monitored device.

Raritan
A brand of legrand

Field	Description
Method of checking successful shutdown	This field determines when PXC/PXO will power off the outlet(s) that supplies power to the monitored device, after PXC/PXO issues the shutdown command to that device. ▪ *Timer*: PXC/PXO will power off the selected outlet or outlet group after the time specified in the 'Timer delay' field expires.
Timer delay	This field appears for the 'Timer' method. Valid values range between 5 and 10,000 seconds.

Server Status Checking or Power Control

It is model dependent whether your PXC/PXO supports the shutdown and power control features via the Server Reachability page.

After adding IT equipment for monitoring, all IT devices are listed on the Server Reachability page.

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 PXC/PXO can declare that the monitored device is reachable or unreachable.

To check the server monitoring states and results:

1. The column labeled "Ping Enabled" indicates whether the monitoring for the corresponding IT device is activated or not.
2. The column labeled "Status" indicates the accessibility of monitored equipment.

Status	Description
Reachable	The monitored equipment is accessible.
Unreachable	The monitored equipment is inaccessible.
Waiting for reliable connection	The connection between the PXC/PXO device and the monitored equipment is not reliably established yet.

3. If your PXC/PXO supports outlet switching, one more column displays -- *Power Control*.

Power control status	Description
(disabled)	Power control is not enabled for the monitored equipment.
Server power is on	The outlet or outlet group associated with the monitored equipment is being powered on. ▪ In the scenario where an 'outlet group' is associated with the equipment, the message 'Server power is on' is shown as long as one of the outlets in the outlet group remains powered on.
Server power is off	The outlet or all outlets of the outlet group associated with the monitored equipment are being powered off.
Server is shutting down	PXC/PXO has sent the shutdown command to the monitored equipment, but the shutdown operation has not completed or succeeded yet.
Power state unknown	PXC/PXO cannot determine the power state of the outlet(s) associated with the monitored device. For example, maybe the outlet group associated with the monitored device has been deleted.

To shut down a monitored device:

1. Select the IT device that you want to shut down.
2. Click

.
3. Confirm the operation when prompted.
4. Observe the Power Control status of the monitored device to make sure the shutdown operation succeeds.

To power on a monitored device:

1. Select the IT device that you want to turn on.
2. Click

.
3. Confirm the operation when prompted.

Raritan
A brand of legrand

4. Observe the Power Control status of the monitored device to make sure the power-on operation succeeds.

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 316).
   - 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 PXC/PXO to make sure that PDU is properly operating all the time, and the PXC/PXO 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 PXC/PXO 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

.
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 PXC/PXO declare the accessibility of the monitored PDU every 15 seconds (3 pings * 5 seconds) when that PDU is accessible, enter the following data.

Field	Data entered
Number of successful pings to enable feature	3

Field	Data entered
Wait time after successful ping	5

- To make the PXC/PXO 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 PXC/PXO stop pinging the target PDU for 60 seconds (1 minute) after the PDU inaccessibility is declared, enter the following data. After 60 seconds, the PXC/PXO 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 PXC/PXO react only when the target PDU becomes inaccessible.

5. Select the System SNMP Notification Action.

Raritan
A brand of legrand

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 302).*

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, Raritan 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 60).*

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 your PXC/PXO 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.
3. Click Save.

   You can turn on or off outlets/actuators by operating the front panel. See ***Power Control*** (on page 72) and ***Peripherals*** (on page 79).

Configuring the Serial Port

You can change the bit rate of the serial port labeled CONSOLE on the PXC/PXO. The default bit rate for console operation is 115200 bps.

The PXC/PXO 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 710)

You can set diverse bit-rate settings for console operations. Usually the PXC/PXO can detect the device type, and automatically apply the preset bit rate.

The PXC/PXO 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 PXC/PXO, 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 PXC/PXO to control its behaviors.

Raritan also provides some Lua scripts examples, which you can load as needed.

Note: Not all Raritan Lua script examples can apply to your PXC/PXO model. You should read each example's introduction before applying them.

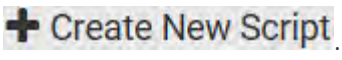
You must have the Administrator Privileges to manage Lua scripts.

Writing or Loading a Lua Script

You can enter or load up to 4 scripts to the PXC/PXO.

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 329).*

To write or load a Lua script:

1. Choose Device Settings > Lua Scripts > 

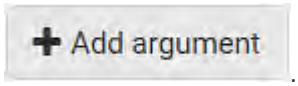
.
2. Type a name for this script. Its length ranges between 1 to 63 characters. The name must contain the following characters only.

- Alphanumeric characters
- Underscore (_)
- Minus (-)

Note: Spaces are NOT permitted.

3. Determine whether and when to automatically execute the loaded script.

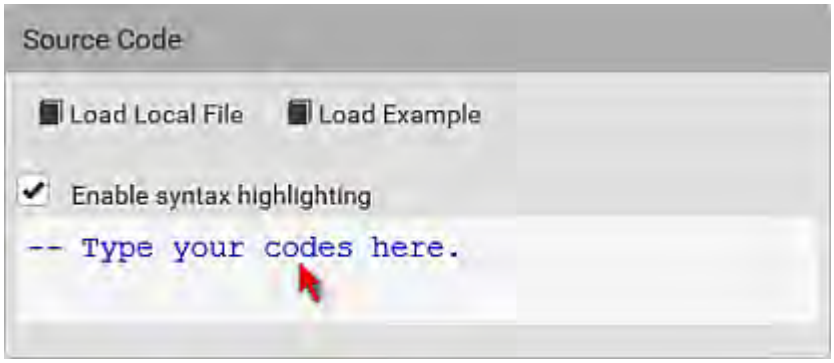
Checkbox	Behavior when selected
Start automatically at system boot	Whenever the PXC/PXO reboots, the script is automatically executed.
Restart after termination	The script is automatically executed each time after 10 seconds since the script execution finishes.

4. (Optional) Determine the arguments that will be executed by default.
   a. Click 

.
   b. Type the key and value.
   c. Repeat the same steps to enter more arguments as needed.
      - To remove any existing argument, click adjacent to it.

Note: 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 326) or* **Start or Stop a Lua Script** *(on page 288).*

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.



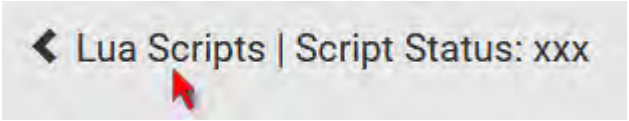
   - To load an existing Lua script file, click Load Local File.
   - To use one of Raritan's Lua script examples, click Load Example.

Warning: The newly-loaded script will overwrite all existing codes in the Source Code section. Therefore, do not load a new script if the current script meets your needs.

6. If you chose to load a script or Raritan's example in the previous step, its codes are then displayed in the Source Code section. Double check the codes. If needed, modify the codes to meet your needs.
7. Click Create.

Next steps:

- To execute the newly-added script immediately, click ▶ Start, or click ⋮ > Start With Arguments. See ***Manually Starting or Stopping a Script*** (on page 326).
- 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 103), and then repeat the above steps.



Manually Starting or Stopping a Script

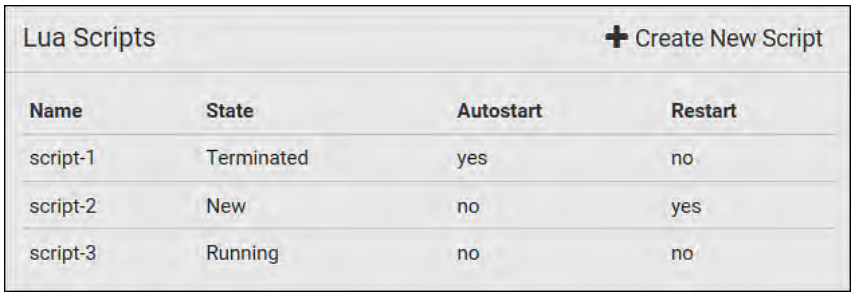
You can manually start or stop an existing Lua script at any time.

When starting a script, you can choose to start it either with its default arguments or with new arguments.

Tip: To have the PXC/PXO automatically start or stop a script in response to an event, create an event rule. See **Event Rules and Actions** *(on page 259) and* **Start or Stop a Lua Script** *(on page 288).*

To manually start a script:

1. Choose Device Settings > Lua Scripts. The Lua scripts list displays.



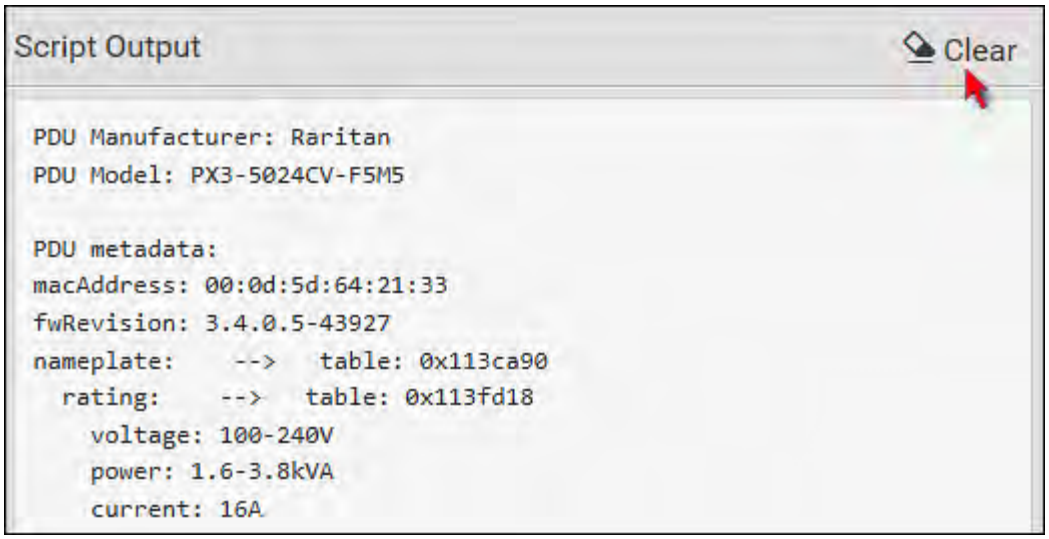
2. Click the desired script whose state is either 'Terminated' or 'New.' For details, see ***Checking Lua Scripts States*** (on page 328).
3. To start with default arguments, click ▶ Start.

Raritan
A brand of legrand

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.

5. Click Start.
6. The script output will be shown in the Script Output section.
   - If needed, click Clear to delete the existing output data.



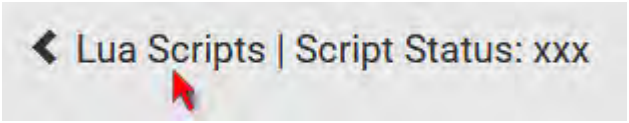
To manually stop a script:

1. Choose Device Settings > Lua Scripts.
2. Click the desired script whose state is either 'Running' or 'Restarting.' For details, see ***Checking Lua Scripts States*** (on page 328).

3. Click on the top-right corner.
4. Click Stop on the confirmation message.

To return to the scripts list:

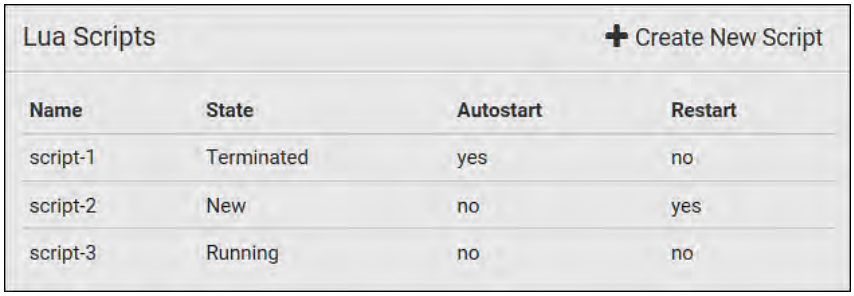
- Click "Lua Scripts" on the top of the page.



- Or click "Lua Scripts" in the ***Menu*** (on page 103).

Checking Lua Scripts States

Choose Device Settings > Lua Scripts to show the scripts list, which indicates the current state and settings of each script.



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 324).

Restart:

This column indicates whether the checkbox labeled "Restart after termination" is enabled. See ***Writing or Loading a Lua Script*** (on page 324).

Raritan
A brand of legrand

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 PXC/PXO.

To modify or replace a script:

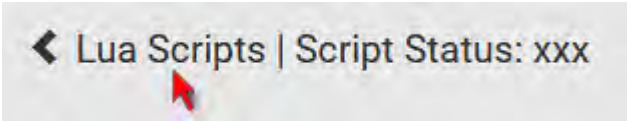
1. Choose Device Settings > Lua Scripts.
2. Click the desired one in the scripts list.
3. Click ⋮ > Edit Script.
4. Make changes to the information shown, except for the script's name, which cannot be revised.
   - To replace the current script, click Load Local File or Load Example to select a new script.

To delete a script:

1. Choose Device Settings > Lua Scripts.
2. Click the desired one in the scripts list.
3. Click ⋮ > Delete.
4. Click Delete on the confirmation message.

To return to the scripts list:

- Click "Lua Scripts" on the top of the page.



- Or click "Lua Scripts" in the ***Menu*** (on page 103).

Miscellaneous

If a Cisco® EnergyWise energy management architecture is implemented in your place, you can enable the Cisco EnergyWise endpoint implemented on the PXC/PXO so that this PXC/PXO becomes part of the Cisco EnergyWise domain.

In addition, if you have to prevent others from accessing your PXC/PXO via USB-A for security reasons, you can disable all of USB-A ports on the PXC/PXO. By default, USB-A ports are enabled.

Important: Disabling USB-A ports will disable all of 'USB-A' based features, such as wireless networking, USB cascading or pdView access using iOS mobile devices. Therefore, re-think about it before disabling USB-A.

To configure either feature, choose Device Settings > Miscellaneous.

To set the Cisco EnergyWise configuration:

1. Select the Enable EnergyWise checkbox.
2. Configure the following:

Field	Description
Domain name	Type the name of a Cisco EnergyWise domain where the PXC/PXO 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 PXC/PXO is queried in the Cisco EnergyWise domain. ▪ Range from 30 to 600 ms. ▪ Default is 180 ms.

3. Click Save in the *EnergyWise* section.

To disable the access to USB-A port(s):

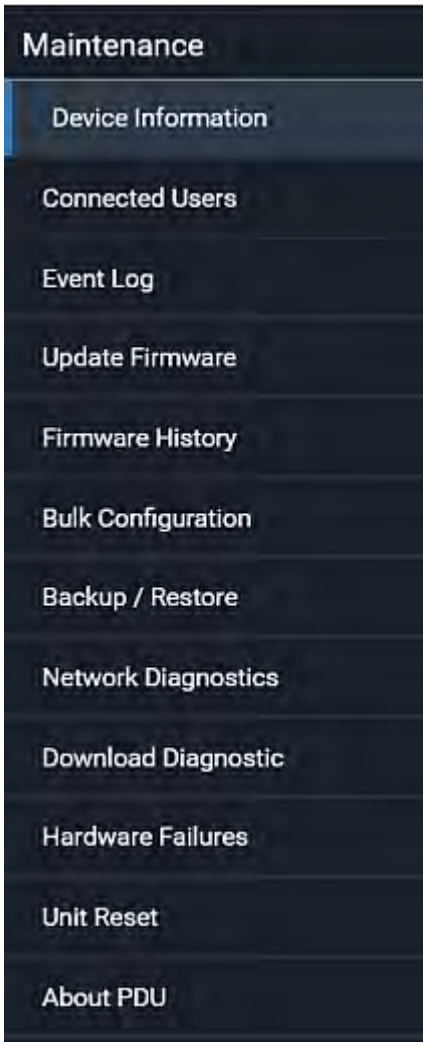
1. Deselect the Enable USB Host Ports checkbox.
2. Click Save in the USB Host Ports section.

Tip: After the Enable USB Host Ports checkbox is deselected, only the access to USB-A port(s) is prevented while the USB-B port works as normal. That is, users still can access the USB-B port, such as accessing CLI via USB-B. To disable the access to the USB-B port, you have to apply a mechanical method.

Raritan
A brand of legrand

Maintenance

Click 'Maintenance' in the ***Menu*** (on page 103), and the following submenu displays.



Submenu command	Refer to...
Device Information	***Device Information*** (on page 333)
Connected Users	***Viewing Connected Users*** (on page 338)
Event Log	***Viewing or Clearing the Local Event Log*** (on page 339)
Update Firmware	***Updating the PXC/PXO Firmware*** (on page 340)
Firmware History	***Viewing Firmware Update History*** (on page 342)

Submenu command	Refer to...
Bulk Configuration	***Bulk Configuration*** (on page 343)
Backup/Restore	***Backup and Restore of Device Settings*** (on page 349)
Network Diagnostic	***Network Diagnostics*** (on page 351)
Download Diagnostic	***Downloading Diagnostic Information*** (on page 352)
Hardware Failures	***Hardware Issue Detection*** (on page 352)
Unit Reset	▪ ***Rebooting the PXC/PXO*** (on page 354) ▪ ***Resetting All Settings to Factory Defaults*** (on page 354)
About PDU	***Retrieving Software Packages Information*** (on page 355)

Raritan
A brand of legrand

Device Information

Using the web interface, you can retrieve hardware and software information of components or peripheral devices connected to your PXC/PXO.

Tip: If the information shown on this page does not match the latest status, press F5 to reload it.

To display device information:

1. Choose Maintenance > Device Information.

2. Click the desired section's title bar to show that section's information. For example, click the Network section.

The number of available sections is model dependent.

Section title	Information shown
Information	General device information, such as model name, serial number, firmware version, hardware revision, MIB download link(s) and so

Section title	Information shown
	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 PXC/PXO is part of a cascading configuration. See ***Identifying Cascaded Devices*** (on page 334).
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 PXC/PXO devices, see ***Cascading Multiple PXC/PXO Devices for Sharing Ethernet Connectivity*** (on page 24).

This section explains how to identify a cascaded device on the Device Information page.

Note: For more information on cascading configurations and restrictions, refer to the Cascading Guide *on the Raritan* **Support page** *(***http://www.raritan.com/support/***).*

To identify the cascading status:

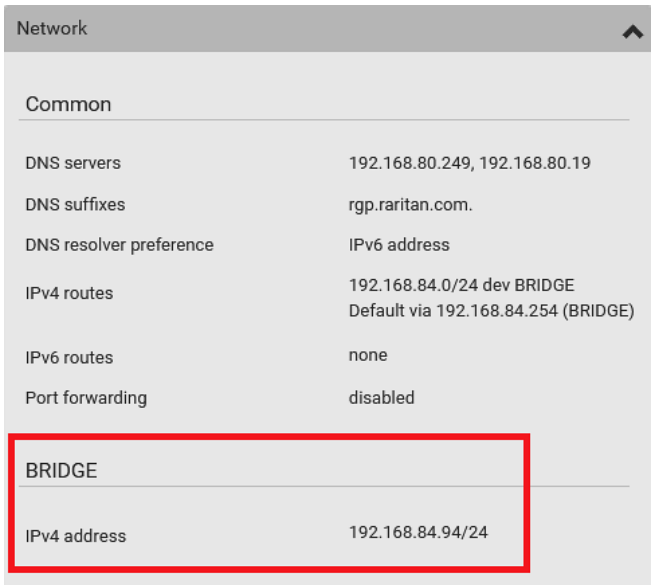
1. Choose Maintenance > Device Information.
2. Click the Network title bar.

- 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 207).
BRIDGE section	Indicates the device is in the Bridging mode and its IP address.



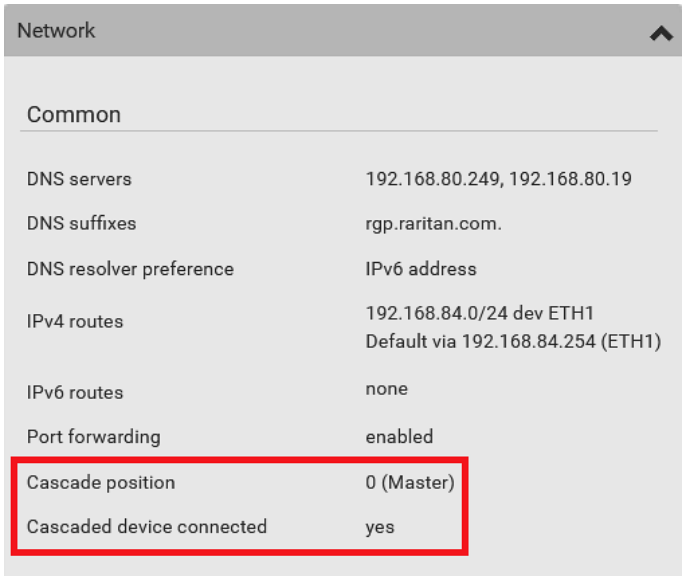
Cascading information in the Port Forwarding mode:

- The Common section contains three read-only fields for indicating the cascading status.

Fields	Description
Port forwarding	Indicates the Port Forwarding is enabled. See ***Setting the Cascading Mode*** (on page 207).

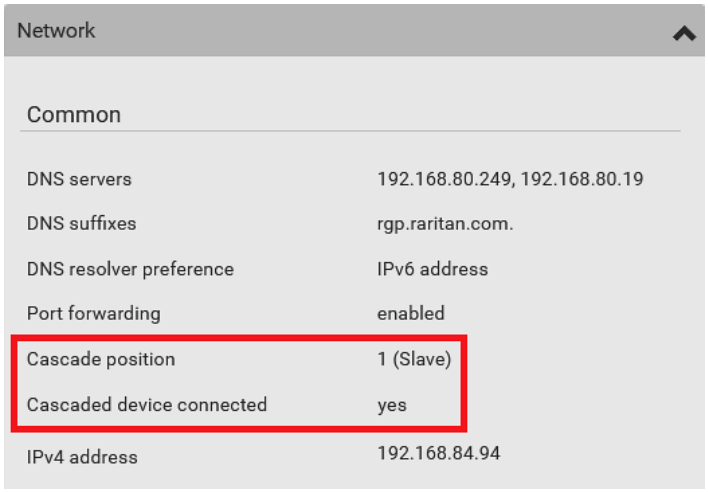
Fields	Description
Cascade position	Indicates the position of the PXC/PXO in the cascading chain. ▪ 0 (zero) represents the master device. ▪ A non-zero number represents a slave device. 1 is Slave 1, 2 is Slave 2, 3 is Slave 3 and so on.
Cascaded device connected	Indicates whether a slave device is detected 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.



- 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.



- The final slave device shows a non-zero number which indicates its position in the 'Cascade position' field and *no* in the 'Cascaded device connected' field.

  The following diagram shows 2, indicating it is the second slave device - Slave 2. The 'Cascaded device connected' field shows *no*, indicating that it is the final one in the chain.

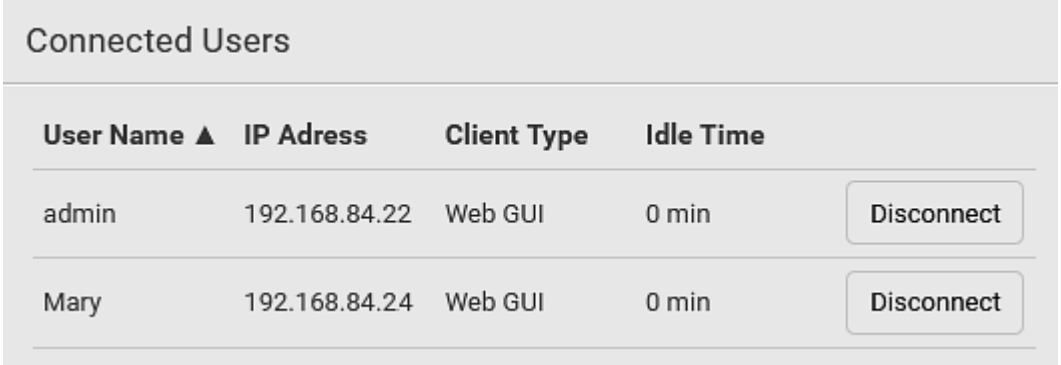
- For a list of port numbers required for accessing each cascaded device in the Port Forwarding mode, click the Port Forwarding title bar on the same page.

Viewing Connected Users

You can check which users have logged in to the PXC/PXO and their status. If you have administrator privileges, you can terminate any user's connection to the PXC/PXO.

To view and manage connected users:

1. Choose Maintenance > Connected Users. A list of logged-in users displays.



If wanted, you can resort the list by clicking the desired column header. See ***Sorting a List*** (on page 106).

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 PXC/PXO. ▪ 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.

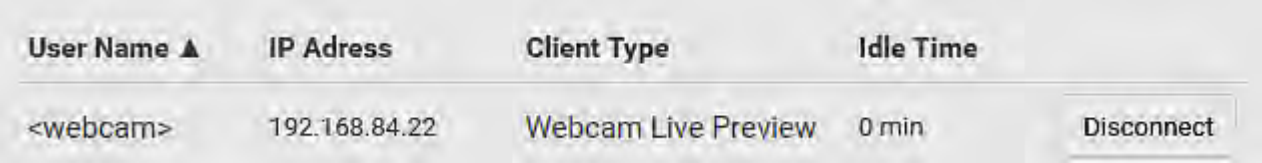
2. To disconnect any user, click the corresponding Disconnect.

Raritan
A brand of legrand

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.



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 356).

Viewing or Clearing the Local Event Log

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

You can view over 2000 historical events that occurred on the PXC/PXO 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.

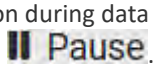
   Each event entry consists of:

   - ID number of the event
   - Date and time of the event

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

   - Event type
   - A description of the event

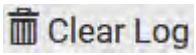
2. To view a specific type of events only, select the desired event type in the 'Filter event class' field.

3. The log is refreshed automatically at a regular interval of five seconds. To avoid any new events' interruption during data browsing, you can suspend the automatic update by clicking 

.
   - To restore automatic update, click

. Those new events that have not been listed yet due to suspension will be displayed in the log now.

To clear the local log:

1. Click 

on the top-right corner.
2. Click Clear Log on the confirmation message.

Updating the PXC/PXO Firmware

Firmware files are available on Raritan website's ***Support page*** (***http://www.raritan.com/support/***).

When performing the firmware upgrade, the PXC/PXO 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 PXC/PXO firmware.

Before starting the upgrade, read the release notes downloaded from Raritan website's ***Support page*** (***http://www.raritan.com/support/***). If you have any questions or concerns about the upgrade, contact Raritan Technical Support BEFORE upgrading.

Note that firmware upgrade via iOS mobile devices, such as iPad, requires the use of iCloud Drive or a file manager app.

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

To update the firmware:

1. Choose Maintenance > Update Firmware.
2. Click

to select an appropriate firmware file.
3. Click Upload. A progress bar appears to indicate the upload process.
4. Once complete, information of both installed and uploaded firmware versions as well as compatibility and signature-checking results are displayed.
   - If anything is incorrect, click Discard Upload.
5. To proceed with the update, click Update Firmware.

Warning: Do NOT power off the PXC/PXO 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 92).
   - No users can successfully log in to the PXC/PXO.
   - Other users' operation, if any, is forced to suspend.
7. When the update is complete, the PXC/PXO 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 PXC/PXO 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 378).**

Alternatives:

To use a different method to update the firmware, refer to:

- ***Firmware Update via SCP*** (on page 559)
- ***Bulk Configuration or Firmware Upgrade via DHCP/TFTP*** (on page 590)
- ***Firmware Upgrade via USB*** (on page 588)

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 PXC/PXO 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 PXC/PXO, disaster recovery can be performed via the USB connection only.

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

Contact Raritan Technical Support for the recovery utility, which works in Windows XP/Vista/7/10 and Linux. In addition, an appropriate PXC/PXO firmware file is required in the recovery procedure.

Viewing Firmware Update History

The firmware upgrade history is permanently stored on the PXC/PXO. 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 106).

Raritan
A brand of legrand

Bulk Configuration

The Bulk Configuration feature lets you save generic settings of a configured PXC/PXO device to your computer. You can use this configuration file to copy common settings to other PXC/PXO devices of the same model and firmware version. See ***Bulk Configuration Restrictions*** (on page 344).

A source device is the PXC/PXO device where the configuration file is downloaded/saved. A target device is the PXC/PXO 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 701).

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 349).*

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 345).
2. Perform the bulk configuration operation, which includes the following steps. For details, see ***Performing Bulk Configuration*** (on page 346).
   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, PXC/PXO 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 PXC/PXO, the last record similar to the following is displayed at the bottom of both the Bulk Configuration and Backup/Restore pages.

Last restore: 3/16/2019, 10:11:03 AM UTC+0800, status: OK

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

Alternatives:

To use a different bulk configuration method, refer to:

- ***Bulk Configuration via SCP*** (on page 560)
- ***Bulk Configuration or Firmware Upgrade via DHCP/TFTP*** (on page 590)
- ***Configuration or Firmware Upgrade with a USB Drive*** (on page 575)
- ***Raw Configuration Upload and Download*** (on page 613)

Tip: Both methods of uploading 'bulk configuration' file or 'raw configuration' file via SCP can serve the purpose of bulk configuration. The only difference is that you can configure device-specific *settings with the upload of raw configuration but not with the 'bulk configuration' file.*

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.

Raritan
A brand of legrand

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 PXC/PXO, whose settings you want to download.
2. Choose Maintenance > Bulk Configuration.
3. Click ✚ in the Bulk Profiles section.
4. In the 'Profile name' and 'Description' fields, enter information for identifying the new profile.
5. To make this new profile the default one for future bulk configuration operations, select the 'Select as default profile' checkbox.
   - After setting any profile as the default, the original default profile will no longer function as the default one.
6. Now decide which settings are wanted and which are not.
   a. Click ▼ of the setting which you want to configure.
   b. When the pop-up menu appears, select one of the options.

   Note that the two options 'Inherited' and 'Built-in' are mutually exclusive.

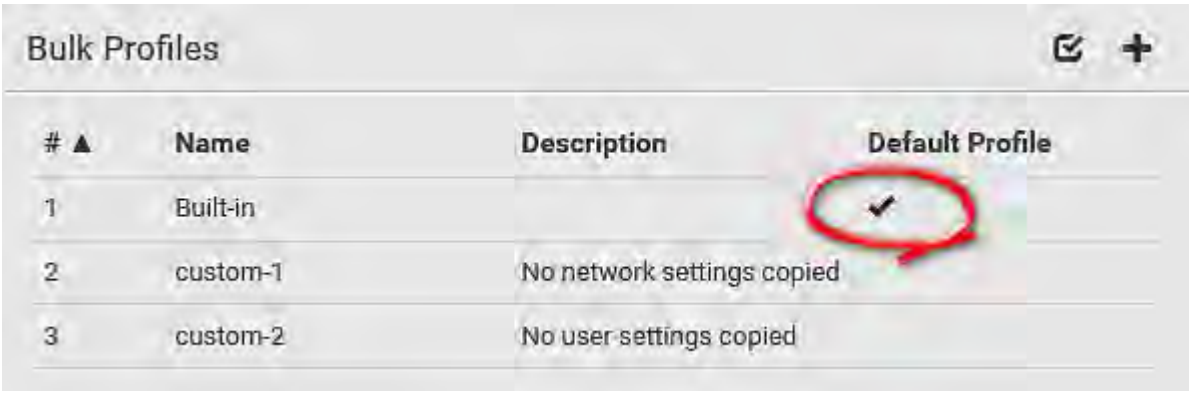
Option	Description
Excluded	The setting will *not* be downloaded.
Included	The setting will be downloaded.
Inherited	The setting will follow its parent setting (that is, the upper-level setting). ▪ If you select 'Excluded' for its upper-level setting, this setting will be also excluded. ▪ If you select 'Included' for its upper-level setting, this setting will be also included. The option inherited from its parent setting will be enclosed in parentheses.

Option	Description
Built-in	The setting will follow the same setting of Raritan's built-in profile. ▪ If 'Excluded' is selected in the built-in profile, this setting will be also excluded. ▪ If 'Included' is selected in the built-in profile, this setting will be also included. The option inherited from the built-in profile will be enclosed in parentheses. *Note: The option 'Built-in' is available in those settings whose corresponding settings in the built in profile have been set to a non-inherited option -- Excluded or Included.*

7. Click Save.
8. Repeat the same steps if you want to create more bulk profiles.

Performing Bulk Configuration

On the source device, make sure the wanted profile has been set as the default one. If not, start from step 1 below. If yes, go to step 2 directly.



Step 1: Select the desired bulk configuration profile (optional)

1. Log in to the source PXC/PXO, 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 PXC/PXO 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 PXC/PXO, which is of the same model and runs the same firmware as the source PXC/PXO.
2. Choose Maintenance > Bulk Configuration.
3. Click

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 PXC/PXO resets and the login page re-appears.

Alternatives:

To use a different bulk configuration method, refer to:

- ***Bulk Configuration via SCP*** (on page 560)
- ***Bulk Configuration or Firmware Upgrade via DHCP/TFTP*** (on page 590)
- ***Configuration or Firmware Upgrade with a USB Drive*** (on page 575)
- ***Raw Configuration Upload and Download*** (on page 613)

Tip: Both methods of uploading 'bulk configuration' file or 'raw configuration' file via SCP can serve the purpose of bulk configuration. The only difference is that you can configure device-specific *settings with the upload of raw configuration but not with the 'bulk configuration' file.*

Modifying or Removing Bulk Profiles

You can modify or remove any bulk profile except for the built-in one.

Note that a profile that has been set as the default cannot be removed, either. To remove it, you have to remove its default setting first.

Choose Maintenance > Bulk Configuration. A list of profiles displays and then do one of the following.

To modify an existing profile:

1. Click on the row of the wanted profile in the list.
2. Change the settings you want.
3. Click Save.

To remove a single profile:

1. Click on the row of the wanted profile.
2. Click on the top-right corner.
3. Click Delete on the confirmation message.

To remove one or multiple profiles:

1. Click to make checkboxes appear in front of profiles.
2. Select one or multiple profiles.

Raritan
A brand of legrand

- To select ALL profiles, select the topmost checkbox in the header row.

3. Click on the top-right corner.
4. Click Delete on the confirmation message.

Backup and Restore of Device Settings

Unlike the bulk configuration file, the backup file contains ALL device settings, including device-specific data like device names and all network settings. To back up or restore the settings of PXC/PXO, you should perform the Backup/Restore feature.

All PXC/PXO 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 PXC/PXO devices, use the Bulk Configuration feature instead. See **Bulk Configuration** *(on page 343).*

To download a backup PXC/PXO 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 PXC/PXO using a backup file:

You must have the Administrator Privileges to restore the device settings.

1. Choose Maintenance > Backup/Restore.
2. Click

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 PXC/PXO resets and the Login page re-appears, indicating that the restore is complete.

Note: On startup, PXC/PXO 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 PXC/PXO, the last record similar to the following is displayed at the bottom of both the Bulk Configuration and Backup/Restore pages.

Last restore: 3/16/2019, 10:11:03 AM UTC+0800, status: OK

Alternative:

To use a different method to perform backup/restore, refer to:

- ***Backup and Restore via SCP*** (on page 561)

Raritan
A brand of legrand

Network Diagnostics

PXC/PXO 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 554).*

Choose Maintenance > Network Diagnostics, and then perform any function below.

Ping:

1. Type values in the following fields.

Field	Description
Network host	The name or IP address of the host that you want to check.
Number of requests	A number up to 20. This determines how many packets are sent for pinging the host.

2. Click Run Ping to ping the host. The Ping results are then displayed.

Trace Route:

1. Type values in the following fields.

Field/setting	Description
Hostname	The IP address or name of the host whose route you want to check.
Timeout(s)	A timeout value in seconds to end the trace route operation.
Use ICMP packets	To use the Internet Control Message Protocol (ICMP) packets to perform the trace route command, select this checkbox.

2. Click Run. The Trace Route results are then displayed.

List TCP Connections:

1. Click the List TCP Connections title bar to show the list.

Downloading Diagnostic Information

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

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

This feature is accessible only by users with Administrative Privileges or Unrestricted View Privileges.

To retrieve a diagnostic file:

1. Choose Maintenance > Download Diagnostic >

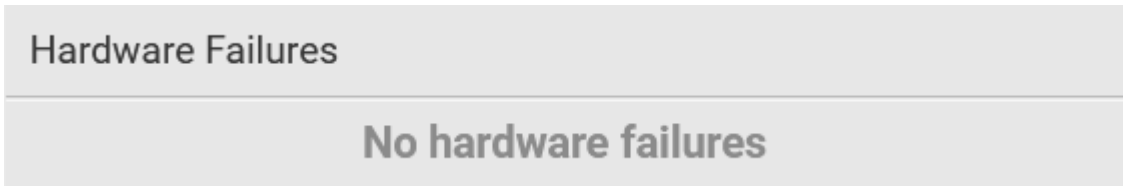
.
2. The system prompts you to save or open the file. Save the file then.
3. E-mail this file as instructed by Raritan Technical Support.

Hardware Issue Detection

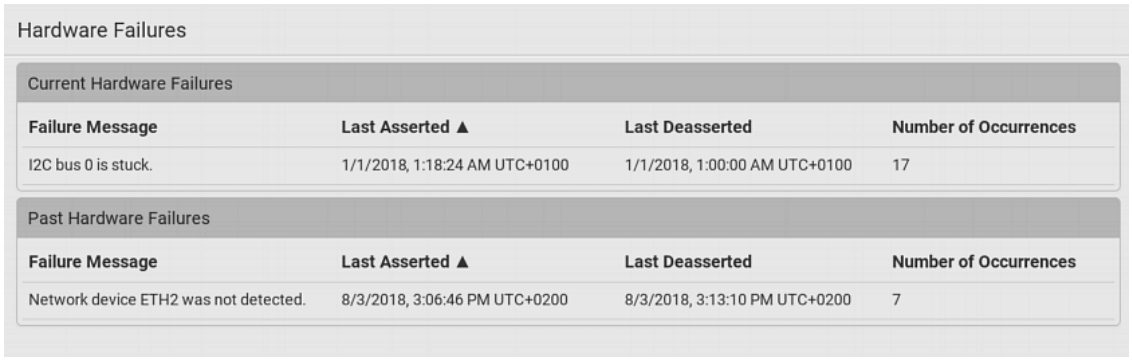
This page lists any internal hardware issues PXC/PXO has detected, including current events and historical records.

Choose Maintenance > Hardware Failures, and the page similar to either of the following diagrams opens.

NO hardware failures detected:



Hardware failure(s) detected:



Raritan
A brand of legrand

Hardware Failure alerts on the Dashboard page:

Note that *current* hardware failure events, if any, will also display on the ***Dashboard*** (on page 107).

Hardware failure types:

Hardware issues	Description
Network device not detected	A specific networking interface of PXC/PXO is NOT detected.
I2C Bus stuck	A specific I2C bus is stuck, which affects the communication with sensors.
Slave controller not reachable	Communication with a specific slave controller fails.
Slave controller malfunction	A specific slave controller does not work properly.
Outlet power state inconsistent	The physical power state of a specific outlet is different from the chosen power state set by the software.

Rebooting the PXC/PXO

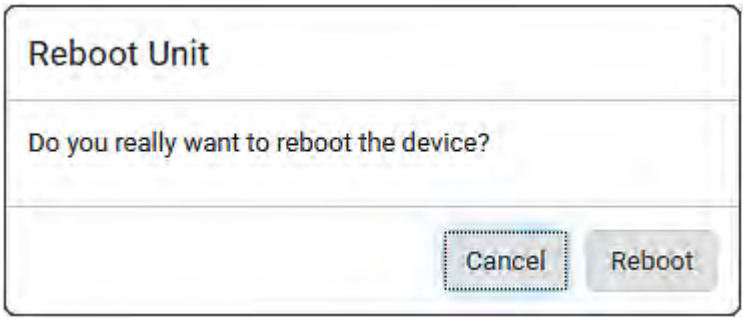
You can remotely reboot the PXC/PXO via the web interface.

Resetting the PXC/PXO 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 PXC/PXO deletes all webcam snapshots that are saved onto the PXC/PXO locally. If needed, download important snapshots before rebooting the device. See ***Viewing and Managing Locally-Saved Snapshots*** (on page 363).

To reboot the device:

1. Choose Maintenance > Unit Reset > Reboot Unit.



2. Click Reboot to restart the PXC/PXO.
3. A message appears, with a countdown timer showing the remaining time of the operation. It takes about one minute to complete.
4. When the restart is complete, the login page opens.

Tip: If you are not redirected to the login page after the restart is complete, click the text "this link" in the countdown message.

Note: Device reset will cause CLI communications over an "USB" connection to be lost. Therefore, re-connect the USB cable after the reset is complete.

Resetting All Settings to Factory Defaults

You must have the Administrator Privileges to reset all settings of the PXC/PXO to factory defaults.

Important: Exercise caution before resetting the PXC/PXO 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.

Raritan
A brand of legrand

To reset the device to factory defaults:

1. Choose Maintenance > Unit Reset > Reset to Factory Defaults.

2. Type your password and then click Factory Reset to reset the PXC/PXO to factory defaults.
3. A message appears, with a countdown timer showing the remaining time of the operation. It takes about two minutes to complete.
4. When the reset is complete, the login page opens.

Tip: If you are not redirected to the login page after the reset is complete, click the text "this link" in the countdown message.

Alternative:

There are two more methods to reset the device to factory defaults.

- Use the "mechanical" reset button
- Perform the CLI command

For details, see ***Resetting to Factory Defaults*** (on page 619).

Note: Device reset will cause CLI communications over an "USB" connection to be lost. Therefore, re-connect the USB cable after the reset is complete.

Retrieving Software Packages Information

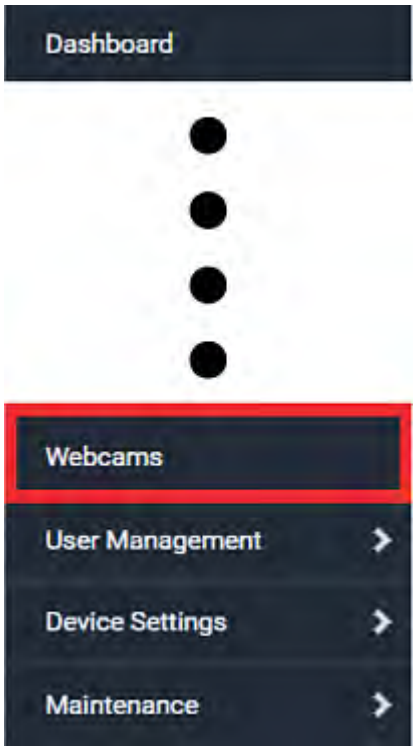
You can check the current firmware version and the information of all open source packages embedded in the PXC/PXO through the web interface.

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 PXC/PXO, or when there are snapshots saved onto the PXC/PXO already. See ***Connecting a Logitech Webcam*** (on page 54).



Raritan
A brand of legrand

With a Logitech® webcam connected to the PXC/PXO, you can visually monitor the environment around the PXC/PXO 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 PXC/PXO or a remote server	▪ ***Configuring Webcams and Viewing Live Images*** (on page 358) ▪ ***Changing Storage Settings*** (on page 365)
Send a snapshot or video session's link to other people via email or instant message	***Sending Links to Snapshots or Videos*** (on page 361)
Create event rules to trigger emails containing snapshots from a webcam	***Available Actions*** (on page 273)

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

Configuring Webcams and Viewing Live Images

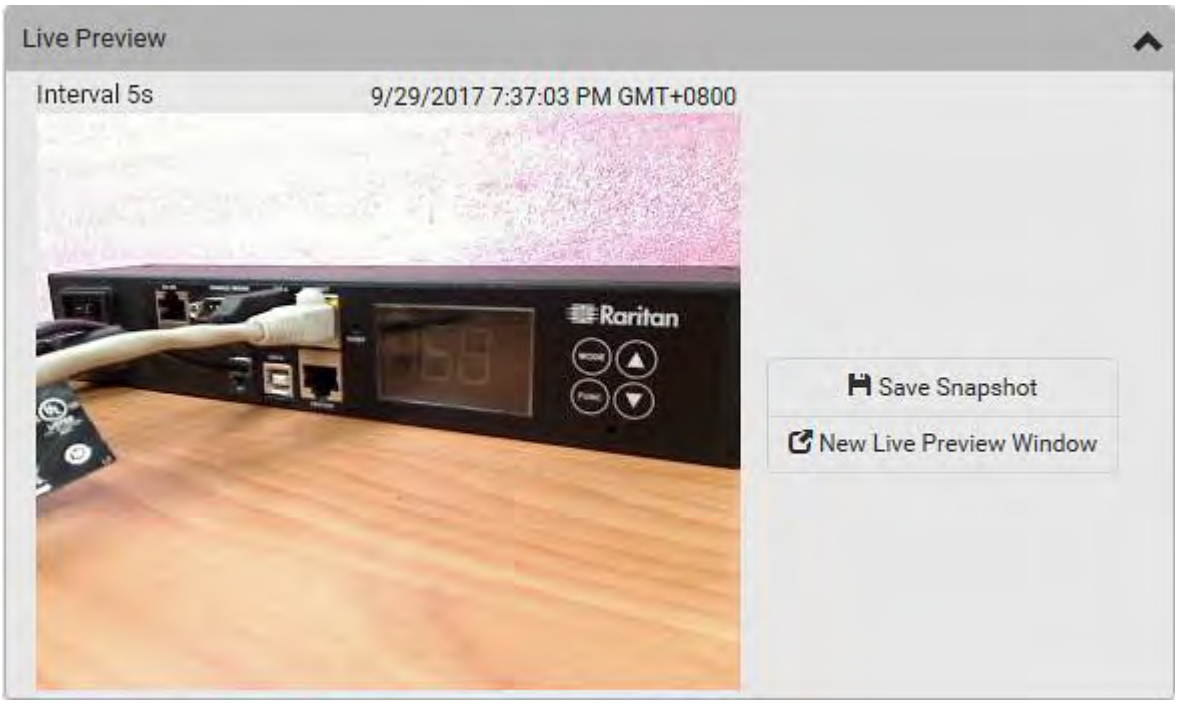
To configure a webcam or view live snapshot/video sessions, choose Webcams in the ***Menu*** (on page 103). Then click the desired webcam to open that webcam's page.

Note that default webcam names are determined by the detection order. The one that is detected first is named *Webcam*, and the other that is detected later is named *Webcam 2*.

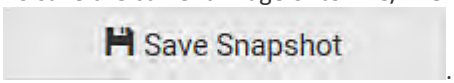
The Webcam page consists of three sections -- *Live Preview*, *Image Controls* and *Settings*.

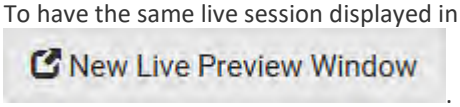
Live Preview:

1. By default the Live Preview section is opened, displaying the live snapshot/video session captured by the webcam.
   - The default is to show live snapshots. Interval time and capture date/time of the image are displayed on the top of the image.



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

2. To save the current image onto PXC/PXO or a remote server, click 

.
   - The default storage location for snapshots is the PXC/PXO device. To save them onto a remote server, see ***Changing Storage Settings*** (on page 365).
   - 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 

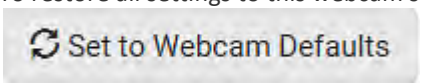
.
   - A separate window appears, which is called the Primary Standalone Live Preview window in this User Guide.
   - You can send out this window's URL to share the live image with others. See ***Sending Links to Snapshots or Videos*** (on page 361).

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 

.

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 365) and ***Identifying Snapshots Folders on Remote Servers*** (on page 367).
   - 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, PXC/PXO 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.

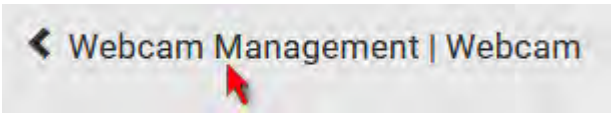
   Tip: If the webcam's location is important, you can customize the webcam's name based on its location when configuring PXC/PXO to save snapshots onto a remote server.
5. Select a resolution for the webcam.
   - If you connect two webcams to one USB-A port using a powered USB hub, set the resolution to 352x288 or lower for optimal performance.
6. Select the webcam mode.

Mode	Description
Video	The webcam enters the video mode. ▪ Set the 'Framerate' (frames per second) as needed.
Snapshot	The webcam shows static images captured by the webcam at a regular interval. ▪ To determine the interval, set the 'Time Between Snapshots' (seconds) as needed.

7. Click Save. The changes made to the settings are applied to the live session in the above *Live Preview* section immediately.

To return to the Webcam Management page:

- Click Webcam Management on the top of the page.



- Or click Webcams again in the ***Menu*** (on page 103).

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).

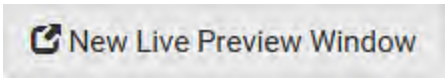
Tip: All Live Preview window sessions sharing the same URL, including one Primary Standalone Live Preview window and multiple Secondary Standalone Live Preview windows, are identified as one single "<webcam>" user in the Connected Users list. You can disconnect a "<webcam>" user to terminate all sessions sharing the same URL. See **Viewing Connected Users** *(on page 338).*

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 363).

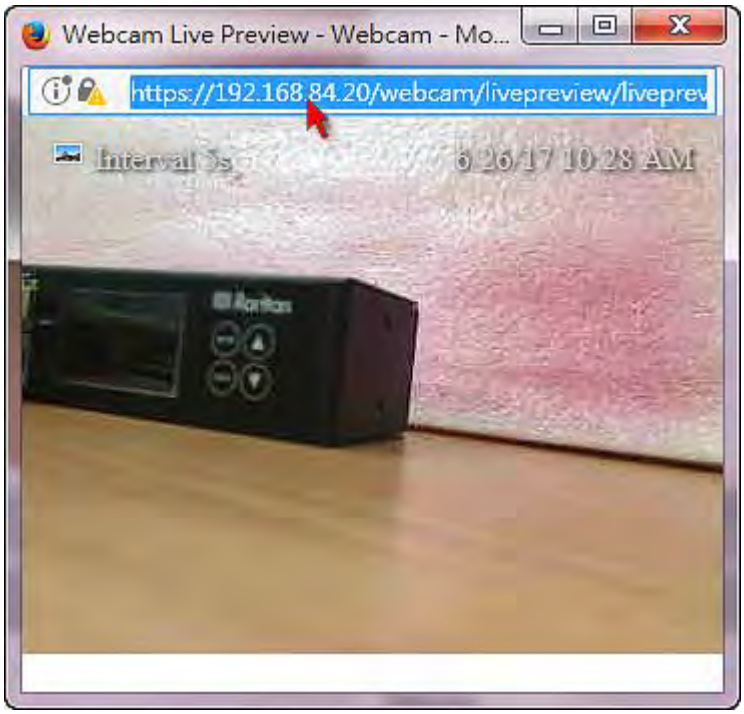
To send a snapshot or video link via email or instant message:

1. Choose Webcams in the ***Menu*** (on page 103).
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*.

3. Click 

in the Live Preview section. The live snapshot or video in a standalone window opens. See ***Configuring Webcams and Viewing Live Images*** (on page 358).
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 PXC/PXO 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 PXC/PXO 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 PXC/PXO device by default. For snapshot-saving operations, see ***Configuring Webcams and Viewing Live Images*** (on page 358).

Up to 10 snapshots can be stored onto the PXC/PXO. 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.

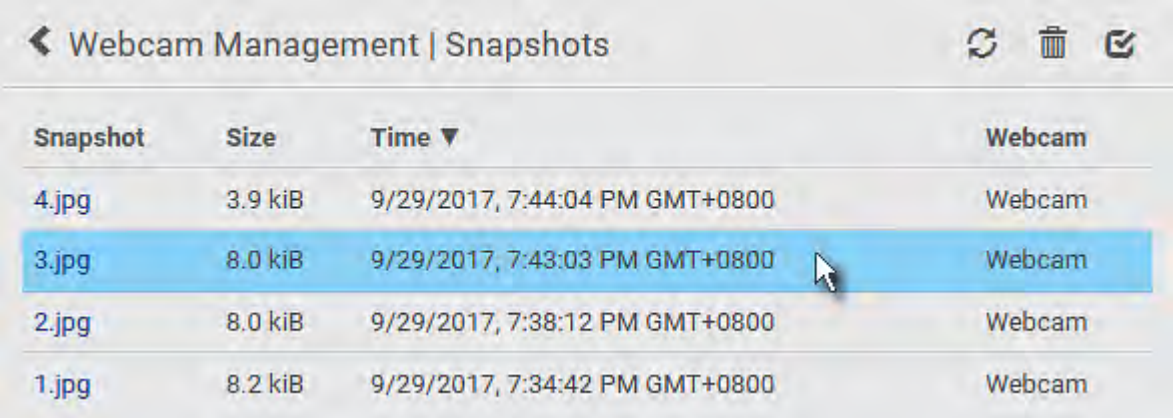
Tip: To save more than 10 snapshots, you must change the storage location from the PXC/PXO to an FTP or Common Internet File System (CIFS)/Samba server. See **Changing Storage Settings** *(on page 365).*

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 PXC/PXO deletes all webcam snapshots that are saved onto the PXC/PXO 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 PXC/PXO web interface are automatically converted to your computer's time zone. To avoid time confusion, it is suggested to apply the same time zone settings as those of PXC/PXO to your computer or mobile device.

3. The selected snapshot as well as its information, such as captured time and resolution, is displayed on the same page.
4. If the latest saved snapshot is not listed yet, click .

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.

Raritan
A brand of legrand

3. On the top of the list, click .
4. Click Delete on the confirmation message.

To download any image onto the computer:

- To download an image onto your computer, move your mouse to that image, right click on it, and choose Save Image As.

Changing Storage Settings

Important: The PXC/PXO web interface only lists the snapshots stored locally on the PXC/PXO 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.

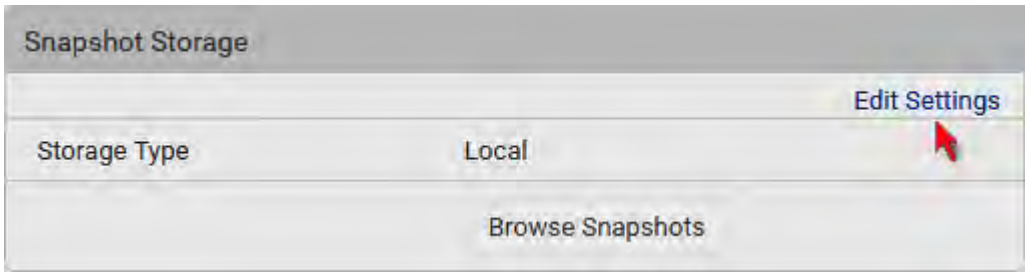
The default is to store snapshots onto the PXC/PXO device, which has a limitation of 10 snapshots. Note that any operation involving device reboot will remove the snapshots saved on the PXC/PXO, such as firmware upgrade.

If you have either or both needs below, you must save snapshots onto a remote server like FTP or CIFS/Samba, instead of the PXC/PXO.

- Total number of saved snapshots will exceed 10.
- Saved snapshots must be stored *permanently*, or at least should *not* be removed by the PXC/PXO 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 PXC/PXO. 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 PXC/PXO. See ***Viewing and Managing Locally-Saved Snapshots*** (on page 363). ▪ All snapshots are CLEARED when the PXC/PXO 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 PXC/PXO. ▪ 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 PXC/PXO. ▪ 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 367).

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 PXC/PXO web interface. If this issue occurs, first restore the connectivity of the remote server and then change the storage settings of the webcam snapshots.

Raritan
A brand of legrand

Tip for notifications showing the snapshots path on FTP:

If you are using SNMP to retrieve PXC/PXO data, you can make PXC/PXO automatically send a notification containing the full path or URL to the snapshots saved onto FTP with this SNMP code: `webcamStorageUploadStarted`.

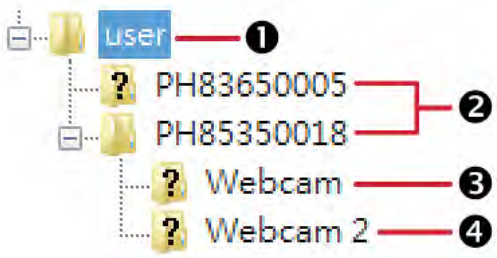
Identifying Snapshots Folders on Remote Servers

If saving snapshots onto a remote server, you can access those snapshots via an appropriate third-party application, such as an FTP client.

All snapshots are saved as JPEG and named according to the date and time when saving the snapshots. Note that the date and time of the filename are based on the time zone of the PXC/PXO rather than that of the computer or mobile device you are operating.

Tip: To check the time zone of your PXC/PXO, choose Device Settings > Date/Time. See **Setting the Date and Time** *(on page 251).*

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 PXC/PXO device where the webcam is connected. For example, *PH85350018*. ▪ To find your PXC/PXO serial number, see ***Device Information*** (on page 333).

Number	Folder name description
❸	The name of the webcam that your PXC/PXO 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 358). ▪ If the webcam's location is important, you can customize the webcam's name based on its location when configuring PXC/PXO to save snapshots onto a remote server.
❹	The name of the webcam that your PXC/PXO 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 PXC/PXO 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, PXC/PXO will create a new folder with the new webcam name while keeping the old folder with the old name.

Raritan
A brand of legrand

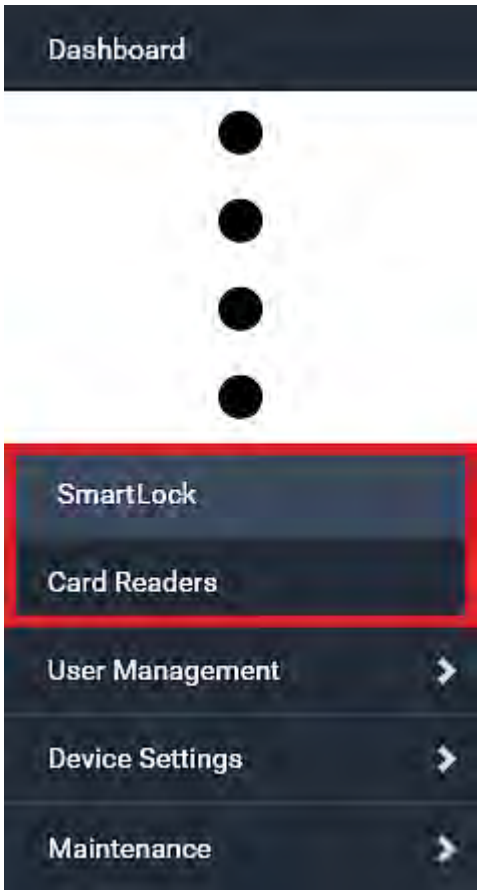
SmartLock and Card Reader

PXO does NOT support the SmartLock kit or DX2-DH2C2, but it supports external USB card reader. PXC supports both the SmartLock kit (that is, DX2-DH2C2) and external USB card readers.

Raritan's SmartLock kits provide several cabinet access control solutions.

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 and configuring properly DX2-DH2C2 and the door handles included in the kit.

Note: For more information on DX2-DH2C2, such as its hardware installation, refer to the SmartLock Quick Setup Guide accompanying the SmartLock kit or 'Environmental Sensors and Actuators Guide' (or its Online Help version) on the Raritan **Support page** *(***http://www.raritan.com/support/***).*



Note that "SmartLock" appears only when your door handles are connected to PXC/PXO via **DX2-DH2C2**, but "Card Readers" appears as long as PXC/PXO detects the presence of any card reader -- either a standalone USB card reader or a card reader integrated with the door handles.

"SmartLock" page:

- Shows the information of all door handle controllers (that is, DX2-DH2C2 modules) attached to PXC/PXO.
- Shows the status of the door handle-integrated card readers connected to DX2-DH2C2.

  Note: Data of "external" USB card readers is NOT shown on the SmartLock page. It is shown on the Card Readers page instead.

- You can control the door handles on this page. See ***SmartLock*** (on page 371).

"Card Readers" page:

- Shows the information of all card readers connected to PXC/PXO, including:
  - Door handle-integrated card readers connected to the DX2-DH2C2 module.
  - External USB card readers connected to the USB-A port of PXC/PXO.

See ***Card Readers*** (on page 376).

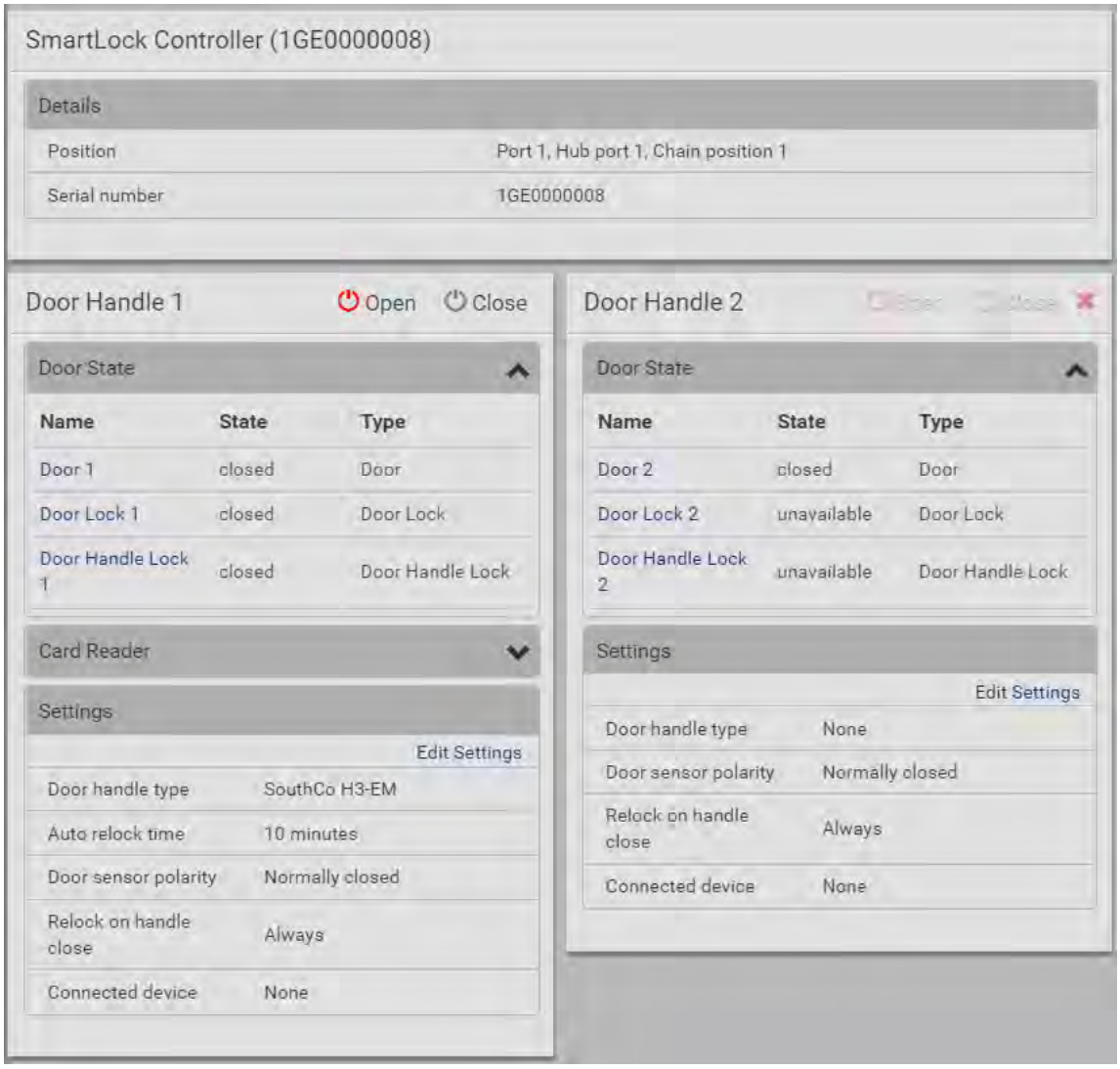
Raritan
A brand of legrand

SmartLock

Only PXC supports this feature while PXO does NOT.

To open the SmartLock page, choose SmartLock in the ***Menu*** (on page 103).

The page shows information of all DX2-DH2C2 modules attached to PXC, including its serial number, position and its door handle configuration. When master units and/or link units have SmartLock controllers connected, this page includes all door handle information for both master and link units.



On this page you can:

- View the status of the cabinet door and card reader.

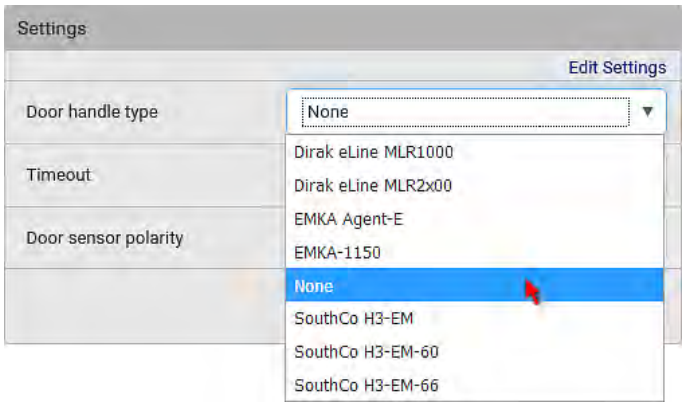
  Note: Data of "external" USB card readers is NOT shown on the SmartLock page. It is shown on the Card Readers page instead.

- Configure the door handles connected to DX2-DH2C2. You must set this because PXC cannot detect the types of connected door handles.
- Control the door handles connected to DX2-DH2C2.

To configure the door handles:

There are two door handle sections per DX2-DH2C2 because a DX2-DH2C2 has two door handle ports. Before you configure the connected door handle(s), a lock icon is displayed on each door handle section's top-right corner, and both the Door State and Card Reader sections are unavailable.

1. Click Edit Settings in the Settings section.
2. In the 'Door handle type' field, select the door handle type you are using.
   - If your specific Southco H3-EM model is listed, select it. For all other supported Southco H3-EM models, select "Southco H3-EM".



3. Make changes to the remaining fields as needed.

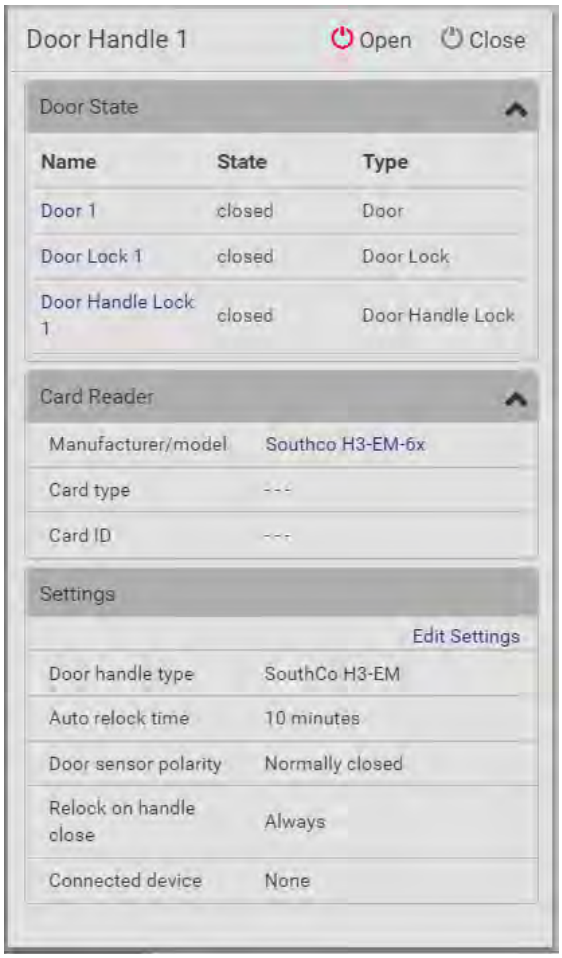
Raritan
A brand of legrand

Section	Description
Timeout	▪ Specify how long the **door handle lock** can remain open after someone opens the door handle via a smart card or via remote control using the software. When the timeout expires, the door handle lock will be automatically closed. Default is 600 seconds (that is, 10 minutes).
Door sensor polarity	▪ Choose the correct setting based on the type of contact closure sensors used to monitor the door: ▪ **Normally closed:** The contact is closed (conducting) when the door is closed and open (not conducting) when the door is open. Default. ▪ **Normally open:** The contact not conducting when the door is closed and conducting when the door is open. ▪ **Note:** For both normally closed and normally open sensors, the reported state is "open" when the door is open and "closed" when the door is closed.
Relock on Handle Close	▪ This setting controls auto-locking of door handles. Select "Only if door closed" to delay auto-locking of door handles until "Door State" and "Door Lock State" are both verified as "Closed". Select "Always" to relock door handles automatically.
Connected Device	▪ If your door handle has a connected device, such as a keypad, select it from the list.

4. Click Save.

Door Handle Status and Control

After configuring the door handle type properly, two more sections are shown for the configured door handle -- **Door State** and **Card Reader**.



Raritan
A brand of legrand

To view the status of the door and card reader:

Section	Description
Door State	Shows all sensor states detected by DX2-DH2C2, including: ▪ *Door*: States of contact closure sensors connected to DX2-DH2C2. Contact closure sensors detect whether the door is physically opened or closed. ▪ *Door Lock*: States of door locks integrated with the door handles. ▪ *Door Handle Lock*: States of the door handle locks. Door locks and door handle locks are interrelated so their states are changed one after another. The door handle lock is opened first and then the door lock. *Exception: If you manually open the door lock with the key shipped with your door handle, the Door Lock state will enter the open state while the Door Handle Lock state remains closed.*
Card Reader	Shows the data of the smart card scanned by the internal or external card reader accompanying each door handle connected to DX2-DH2C2. *Note: The internal card reader integrates with a third-party application, such as Power IQ, for access control. To configure door access rules as a fallback method of authentication when Power IQ is unavailable, see Refer to the user documentation of your third-party application for more information.*

Tip: All sensors of the connected door handles are also listed on the page of **Peripherals** *(on page 154).*

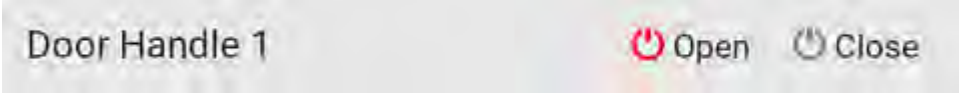
Note that the same Card Reader information is also available on the page of ***Card Readers*** (on page 376).

To control the door handles:

Per default, only one door handle can be opened at the same time so you must close one door handle before opening another door handle connected to the same PXC. To increase the upper limit of concurrently opened door handles, see ***Peripherals*** (on page 154).

1. Make sure you have configured the door handle type properly in the above procedure.

2. Go to the proper door handle section, and click Open or Close to open or close the door handle lock.



3. Confirm the operation when prompted.
4. Now you can physically open the cabinet door with the opened door handle.

DX2-DH2C2 LED information:

- For information on DX2-DH2C2 LED, refer to 'Environmental Sensors and Actuators Guide' (or its Online Help version) on the Raritan ***Support page*** (***http://www.raritan.com/support/***).

Card Readers

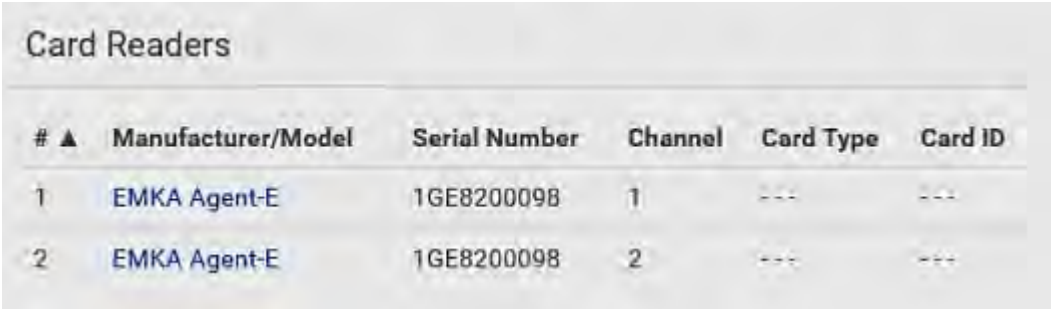
PXO supports "standalone" USB card readers only while PXC supports both standalone USB card readers and internal card readers integrated inside SmartLock kit's door handles.

To open the Card Readers page, choose Card Readers in the ***Menu*** (on page 103).

This page lists all card readers connected to PXC/PXO, including:

- Standalone USB card readers
- Card readers integrated with door handles

Note: To have card readers integrated with door handles display on this page, you must first configure the door handle properly on the page of **SmartLock** *(on page 371).*



When a user scans his/her smart card with the card reader, PXC/PXO 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 PXC/PXO to perform security features like cabinet access control. Refer to that application's user documentation for more information.

Listed card readers can be one or both of the following types.

Door handle-integrated card readers:

- This type of card reader is integrated in the door handle, which is any series below:
  - Emka Agent E
  - SouthCo H3-EM
  - Dirak eLine MLR 2x00

  Note: Not every SouthCo H3-EM door handle has a card reader integrated. For example, H3-EM-60-100 requires an external card reader.
- It is connected to PXC/PXO via the DX2-DH2C2 module.
- The Channel column indicates which door handle port (channel) it is connected to.
- Note that the serial number displayed for this card reader is the same as DX2-DH2C2's serial number.

  Each DX2-PD2C2 module can show two card readers because they have two ports for connecting two door handles with card readers integrated.

Standalone USB card readers:

- It is directly connected to the USB-A port of PXC/PXO.
- The Channel column does not show any data.

Chapter 7 Using SNMP

This SNMP section helps you set up the PXC/PXO for use with an SNMP manager. The PXC/PXO 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 378
Downloading SNMP MIB.....383
SNMP Gets and Sets 383

Enabling and Configuring SNMP

To communicate with an SNMP manager, you must enable SNMP protocols on the PXC/PXO. By default, SNMP is disabled.

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 PXC/PXO.

Important: You must download the SNMP MIB for your PXC/PXO to use with your SNMP manager. See *Downloading SNMP MIB* **(on page 383).**

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 219).

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 177).

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 379)
   - ***SNMPv3 Notifications*** (on page 380)

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 273).*

SNMPv2c Notifications

1. Choose Device Settings > Network Services > SNMP.
2. In the SNMP Agent, make sure the Enable SNMP v1/v2c checkbox is selected.
3. In the SNMP Notifications section, make sure the 'Enable SNMP notifications' checkbox is selected.

4. Select 'SNMPv2c trap' or 'SNMPv2c inform' as the notification type.
5. Type values in the following fields.

Field	Description
Timeout	The interval of time, in seconds, after which a new inform communication is resent if the first is not received. ▪ For example, resend a new inform communication

Field	Description
	once every 3 seconds.
Number of retries	The number of times you want to resend the inform communication if it fails. ▪ For example, inform communications are resent up to 5 times when the initial communication fails.
Host	The IP address of the device(s) you want to access. This is the address to which notifications are sent by the SNMP agent. You can specify up to 3 SNMP destinations.
Port	The port number used to access the device(s).
Community	The SNMP community string to access the device(s). The community is the group representing the PXC/PXO and all SNMP management stations.

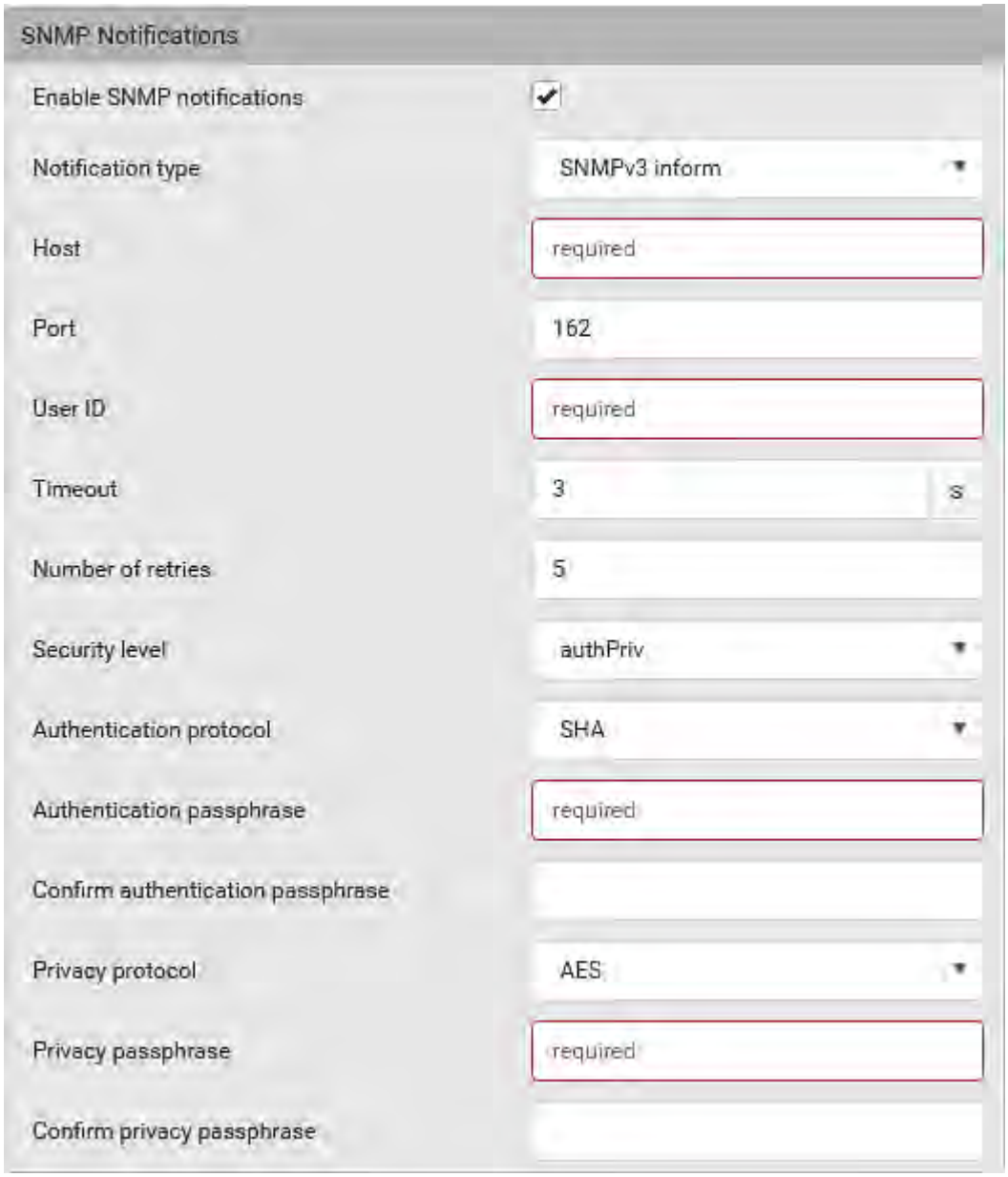
6. Click Save.

SNMPv3 Notifications

1. Choose Device Settings > Network Services > SNMP.
2. In the SNMP Agent, make sure the Enable SNMP v1/v2c checkbox is selected.

Raritan
A brand of legrand

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.

Field	Description
	This is the address to which notifications are sent by the SNMP agent.
Port	The port number used to access the device(s).
User ID	User name for accessing the device. ▪ Make sure the user has the SNMP v3 access permission.
Timeout	The interval of time, in seconds, after which a new inform communication is resent if the first is not received. ▪ For example, resend a new inform communication once every 3 seconds.
Number of retries	Specify the number of times you want to resend the inform communication if it fails. ▪ For example, inform communications are resent up to 5 times when the initial communication fails.
Security level	Three types are available. ▪ noAuthNoPriv - neither authentication nor privacy protocols are needed. ▪ authNoPriv - only authentication is required. ▪ authPriv - both authentication and privacy protocols are required.
Authentication protocol, Authentication passphrase, Confirm authentication passphrase	The three fields are available when the security level is set to AuthNoPriv or authPriv. ▪ Select the authentication protocol - MD5 or SHA ▪ Enter the authentication passphrase
Privacy protocol, Privacy passphrase, Confirm privacy passphrase	The three fields are available when the security level is set to authPriv. ▪ Select the Privacy Protocol - DES or AES ▪ Enter the privacy passphrase and then confirm the privacy passphrase

7. Click Save.

Raritan
A brand of legrand

Downloading SNMP MIB

You must download an appropriate SNMP MIB file for successful SNMP communications. Always use the latest SNMP MIB downloaded from the current firmware of your PXC/PXO.

You can download the MIBs from two different pages of the web interface.

MIB download via the SNMP page:

1. Choose Device Settings > Network Services > SNMP.
2. Click the Download MIBs title bar.

3. Select the desired MIB file to download.
   - PDU2-MIB: The SNMP MIB file for PXC/PXO management.
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
3. Click Save to save the file onto your computer.

SNMP Gets and Sets

In addition to sending notifications, the PXC/PXO is able to receive SNMP get and set requests from third-party SNMP managers.

- Get requests are used to retrieve information about the PXC/PXO, 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 PXC/PXO device name. When you change the SNMP system name, the device name shown in the web interface is also changed.

  The PXC/PXO 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 PXC/PXO MIB.

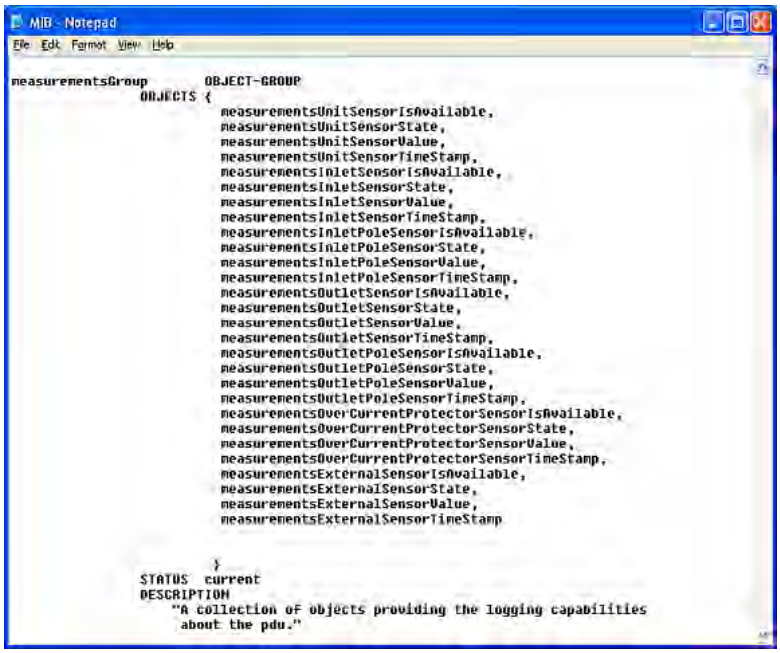
The PXC/PXO MIB

The SNMP MIB file is required for using your PXC/PXO with an SNMP manager. An SNMP MIB file describes the SNMP functions.

Layout

Opening the MIB reveals the custom objects that describe the PXC/PXO 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 PXC/PXO 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.

Raritan
A brand of legrand

SNMP Sets and Thresholds

Some objects can be configured from the SNMP manager using SNMP set commands. Objects that can be configured have a MAX-ACCESS level of "read-write" in the MIB.

These objects include threshold objects, which cause the PXC/PXO to generate a warning and send an SNMP notification when certain parameters are exceeded. See ***Sensor Threshold Settings*** (on page 676) 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 464). For the web interface, see* **Setting the Date and Time** *(on page 251).*

When using the SNMP SET command to specify or change NTP servers, it is required that both the NTP server's address type and address be set in the command line simultaneously.

For example, the SNMP command to change the primary NTP server's address from IPv4 (192.168.84.84) to host name looks similar to the following:

```
snmpset -v2c -c private 192.168.84.84
firstNTPServerAddressType = dns firstNTPServerAddress =
"angu.pep.com"
```

A Note about Enabling Thresholds

When enabling previously-disabled thresholds via SNMP, make sure you set a correct value for all thresholds that are supposed to be enabled prior to actually enabling them. Otherwise, you may get an error message.

Chapter 8 Using the Command Line Interface

This section explains how to use the command line interface (CLI) to administer the PXC/PXO.

Note that available CLI commands are model dependent.

CLI commands are case sensitive.

In This Chapter

About the Interface 386
Logging in to CLI 387
The ? Command for Showing Available Commands 389
Querying Available Parameters for a Command 390
Showing Information 391
Clearing Information 420
Configuring the PXC/PXO Device and Network 421
Load Shedding Configuration Commands 546
Power Control Operations 547
Actuator Control Operations 551
Unblocking a User 553
Resetting the PXC/PXO 553
Network Troubleshooting 554
Retrieving Previous Commands 557
Automatically Completing a Command 557
Logging out of CLI 558

About the Interface

The PXC/PXO 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 PXC/PXO
- Display the PXC/PXO and network information, such as the device name, firmware version, IP address, and so on
- Configure the PXC/PXO 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 223).*

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 PXC/PXO. 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 PDU name appears at the prompt. See ***Different CLI Modes and Prompts*** (on page 389) 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.

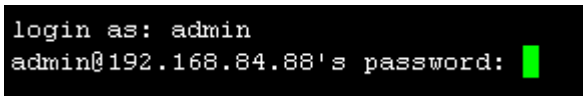
To log in using SSH or Telnet:

1. Ensure SSH or Telnet has been enabled. See ***Configuring Network Services*** (on page 216) in the User Guide.
2. Launch an SSH or Telnet client and open a console window. A login prompt appears.

3. Type a name and press Enter. The name is case sensitive.

Note: If using the SSH client, the name must NOT exceed 25 characters. Otherwise, the login fails.

Then you are prompted to enter a password.



4. Type a password and press Enter. The password is case sensitive.
5. After properly entering the password, the PDU name appears at the prompt. See ***Different CLI Modes and Prompts*** (on page 389) 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.

Raritan
A brand of legrand

Different CLI Modes and Prompts

Depending on the login name you use and the mode you enter, the system prompt in the CLI varies. The PDU name appears with the prompt.

- User Mode: When you log in as a normal user, who may not have full permissions to configure the PXC/PXO, the **>** prompt appears.
- Administrator Mode: When you log in as an administrator, who has full permissions to configure the PXC/PXO, 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 PXC/PXO device and network configurations. See ***Entering Configuration Mode*** (on page 421).
- 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 554).

Closing a Local Connection

Close the window or terminal emulation program when you finish accessing the PXC/PXO over the local connection.

When accessing or upgrading multiple PXC/PXO devices, do not transfer the local connection cable from one device to another without closing the local connection window first.

The ? Command for Showing Available Commands

When you are not familiar with CLI commands, you can press the ? key at anytime for one of the following purposes.

- Show a list of main CLI commands available in the current mode.
- Show a list of available commands or parameters for the command you type. See ***Querying Available Parameters for a Command*** (on page 390).

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 557). To re-execute one of the previous commands, see* **Retrieving Previous Commands** *(on page 557).*

Querying Available Parameters for a Command

If you are not sure what commands or parameters are available for a particular type of CLI command or its syntax, you can have the CLI show them by adding a space and the help command (?) or list command (ls) to the end of that command. A list of available parameters and their descriptions will be displayed.

The following shows a few query examples.

To query available parameters for the "show" command:

```
#           show ?
```

To query available parameters for the "show user" command:

```
#           show user ?
```

To query available role configuration parameters:

```
config:#    role ?
```

To query available parameters for the "role create" command:

```
config:#    role create ?
```

Tip: To automatically complete a command after typing part of the full command, see **Automatically Completing a Command** *(on page 557). To re-execute one of the previous commands, see* **Retrieving Previous Commands** *(on page 557).*

Raritan
A brand of legrand

Showing Information

You can use the show commands to view current settings or the status of the PXC/PXO 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 389).*

Network Configuration

This command shows all network configuration and all network interfaces' information, such as the IP address, MAC address, the Ethernet interfaces' duplex mode, and the wireless interface's status/settings.

```
#        show network
```

IP Configuration

This command shows the IP settings shared by all network interfaces, such as DNS and routes. Information shown will include both IPv4 and IPv6 configuration.

Tip: To show IPv4-only and IPv6-only configuration data, see **IPv4-Only or IPv6-Only Configuration** *(on page 393).*

```
#       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 PXC/PXO 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*.*

Raritan
A brand of legrand

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 392).*

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 PXC/PXO is set to the bridging mode.

  Note: In the bridging mode, only the IP parameters of the BRIDGE interface function. The IP parameters of ETH1/ETH2 and WIRELESS interfaces do NOT function.

Interface	Description
eth1	Show the IPv4 or IPv6 configuration of the ETH1 interface.
eth2	Show the IPv4 or IPv6 configuration of the ETH2 interface.
wireless	Show the IPv4 or IPv6 configuration of the WIRELESS interface.

Interface	Description
bridge	Show the IPv4 or IPv6 configuration of the BRIDGE interface.
all	Show the IPv4 or IPv6 configuration of all interfaces. *Tip: You can also type the command without adding this option "all" to get the same data. That is,* show network ipv4 interface.

Network Interface Settings

This command shows the specified network interface's information which is NOT related to IP configuration. For example, the Ethernet port's LAN interface speed and duplex mode, or the wireless interface's SSID parameter and authentication protocol.

```
#       show network interface <ETH>
```

Variables:

- <ETH> is one of the network interfaces: *ETH1/ETH2*, *WIRELESS*, or *BRIDGE*. Note that you must choose/configure the bridge interface if your PXC/PXO is set to the bridging mode.

  Note: In the bridging mode, only the IP parameters of the BRIDGE interface function. The IP parameters of ETH1/ETH2 and WIRELESS interfaces do NOT function.

Interface	Description
eth1	Show the ETH1 interface's non-IP settings.
eth2	Show the ETH2 interface's non-IP settings.
wireless	Show the WIRELESS interface's non-IP settings.
bridge	Show the BRIDGE interface's non-IP settings.
all	Show the non-IP settings of all interfaces. *Tip: You can also type the command without adding this option "all" to get the same data. That is,* show network interface.

Raritan
A brand of legrand

Network Service Settings

This command shows the network service settings only, including the Telnet setting, TCP ports for HTTP, HTTPS, SSH and Modbus/TCP services, and SNMP settings.

```
#        show network services <option>
```

Variables:

- <option> is one of the options: *all*, *http*, *https*, *telnet*, *ssh*, *snmp*, *modbus* and *zeroconfig*.

Option	Description
all	Displays the settings of all network services, including HTTP, HTTPS, Telnet, SSH and SNMP. *Tip: You can also type the command without adding this option "all" to get the same data.*
http	Only displays the TCP port for the HTTP service.
https	Only displays the TCP port for the HTTPS service.
telnet	Only displays the settings of the Telnet service.
ssh	Only displays the settings of the SSH service.
snmp	Only displays the SNMP settings.
modbus	Only displays the settings of the Modbus/TCP service.
zeroconfig	Only displays the settings of the zero configuration advertising.

PDU Configuration

This command shows the PDU configuration, such as the device name, firmware version, model type and upper limit of active powered dry contact actuators.

```
#        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.

Raritan
A brand of legrand

Outlet Group Information

This command syntax shows the outlet group information.

```
#       show outletgroups <n>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show outletgroups <n> details
```

Variables:

- <n> is one of the options: *all*, or a number.

Option	Description
all	Displays the information for all outlet groups. *Tip: You can also type the command without adding this option "all" to get the same data.*
A specific outlet group number	Displays the information for the specified outlet group only.

Displayed information:

- Without the parameter "details," only the group's name, the group's index number, member outlets and the group's power state (if it is a switched PDU) are displayed.
- With the parameter "details," more inlet information is displayed in addition to the above outlet group information, such as each member outlet's power state.

Tip: PXC/PXO allows you to assign the same name to diverse outlet groups. If this really occurs, you still can identify different groups through their unique index numbers.

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.

Raritan
A brand of legrand

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.*
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 PXC/PXO.

```
#        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 PXC/PXO web and CLI interfaces across all users, especially those users authenticated through remote authentication servers.

```
#        show user defaultPreferences
```

Note: If a user has set his/her own preferred measurement units or the administrator has changed any user's preferred units, the web and CLI interfaces show the preferred measurement units for that user instead of the default ones. See **Existing User Profiles** *(on page 413) for the preferred measurement units for a specific user.*

Raritan
A brand of legrand

Environmental Sensor Information

This command syntax shows the environmental sensor's information.

```
#        show externalsensors <n>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#        show externalsensors <n> details
```

```
# show externalsensors 2 details
External sensor 2 ('Temperature 2')
Sensor type: Temperature
Reading:     24.0 deg C (normal)

Serial number:            QMSemu0004
Description:              Not configured
Location:                X Not configured
                         Y Not configured
                         Z Not configured
Position:                 Port 1, Chain Position 4
Using default thresholds: yes
```

Variables:

- <n> is one of the options: *all*, or a number.

Option	Description
all	Displays the information of all environmental sensors. *Tip: You can also type the command without adding this option "all" to get the same data.*
A specific environmental sensor number*	Displays the information for the specified environmental sensor only.

* The environmental sensor number is the ID number assigned to the sensor, which can be found on the Peripherals page of the PXC/PXO web interface.

Displayed information:

- Without the parameter "details," only the sensor ID, sensor type and reading are displayed.

  Note: A state sensor displays the sensor state instead of the reading.

- With the parameter "details," more information is displayed in addition to the ID number and sensor reading, such as the serial number, sensor position, and X, Y, and Z coordinates.

Environmental Sensor Package Information

Different from the "`show externalsensors`" commands, which show the reading, status and configuration of an individual environmental sensor, the following command shows the information of all connected environmental sensor packages, each of which may contain more than one sensor or actuator.

```
#       show peripheralDevicePackages
```

Information similar to the following is displayed. Peripheral Device Package refers to an environmental sensor package.

```
Peripheral Device Package 1
Serial Number:    1GE7A00022
Package Type:           DX2-T1H1
Position:         Port 1, Chain Position 1
Package State:    operational
Firmware Version: 33.0

Peripheral Device Package 2
Serial Number:    1GE7A00021
Package Type:           DX2-T3H1
Position:         Port 1, Chain Position 2
Package State:    operational
Firmware Version: 33.0
```


Raritan
A brand of legrand

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 PXC/PXO 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

Raritan
A brand of legrand

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 PXC/PXOs:

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

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

Raritan
A brand of legrand

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 PXC/PXOs:

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.

Raritan
A brand of legrand

Environmental Sensor Threshold Information

This command syntax shows the specified environmental sensor's threshold-related information.

```
#        show sensor externalsensor <n>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#        show sensor externalsensor <n> details
```

```
External sensor 1 (Temperature):
Reading: 22.6 deg C
State:   normal

Active Thresholds: Default thresholds

Default Thresholds for Temperature sensors:
Lower critical threshold: 10.0 deg C
Lower warning threshold:  15.0 deg C
Upper warning threshold:  30.0 deg C
Upper critical threshold: 35.0 deg C
Deassertion hysteresis:   1.0 deg C
Assertion timeout:        0 samples

Sensor Specific Thresholds:
Lower critical threshold: 10.0 deg C
Lower warning threshold:  15.0 deg C
Upper warning threshold:  30.0 deg C
Upper critical threshold: 35.0 deg C
Deassertion hysteresis:   1.0 deg C
Assertion timeout:        0 samples
```

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 PXC/PXO web interface.

Displayed information:

- Without the parameter "details," only the reading, threshold, deassertion hysteresis and assertion timeout settings of the specified environmental sensor are displayed.
- With the parameter "details," more sensor information is displayed, including resolution and range.

Note: For a state sensor, the threshold-related and accuracy-related data is NOT available.

Environmental Sensor Default Thresholds

This command syntax shows a certain sensor type's default thresholds, which are the initial thresholds applying to the specified type of sensor.

```
#        show defaultThresholds <sensor type>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#        show defaultThresholds <sensor type> details
```

Variables:

- <sensor type> is one of the following numeric sensor types:

Sensor types	Description
absoluteHumidity	Absolute humidity sensors
relativeHumidity	Relative humidity sensors
temperature	Temperature sensors
airPressure	Air pressure sensors
airFlow	Air flow sensors
vibration	Vibration sensors

Sensor types	Description
all	All of the above numeric sensors *Tip: You can also type the command without adding this option "all" to get the same data.*

Displayed information:

- Without the parameter "details," only the default upper and lower thresholds, deassertion hysteresis and assertion timeout settings of the specified sensor type are displayed.
- With the parameter "details," the threshold range is displayed in addition to default thresholds settings.

Security Settings

This command shows the security settings of the PXC/PXO.

```
#        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 PXC/PXO, including both LDAP and Radius settings.

```
#       show authentication
```

One LDAP server's settings:

To show the configuration of a specific LDAP server, assign the desired LDAP server with its sequential number in the command. To get detailed information, add "details" to the end of the command.

```
#       show authentication ldapServer <server_num>
```

-- OR --

```
#       show authentication ldapServer <server_num>
```

One Radius server's settings:

To show the configuration of a specific Radius server, assign the desired Radius server with its sequential number in the command. To get detailed information, add "details" to the end of the command.

```
#       show authentication radiusServer <server_num>
```

-- OR--

```
#       show authentication radiusServer <server_num> details
```

Variables:

- <server_num> is the sequential number of the specified authentication server on the LDAP or Radius server list.

Displayed information:

- Without specifying any server, PXC/PXO 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.

Raritan
A brand of legrand

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.

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 426).*

Serial Port Settings

This command shows the baud rate setting of the serial port labeled CONSOLE on the PXC/PXO.

```
#        show serial
```


Raritan
A brand of legrand

EnergyWise Settings

This command shows the PXC/PXO 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.
An integer number	Displays the specified number of last entries in the event log. The number ranges between 1 to 10,000.

- <event_type> is one of the following event types.

Event type	Description
all	All events.
device	Device-related events, such as system starting or firmware upgrade event.

Event type	Description
userAdministration	User management events, such as a new user profile or a new role.
userActivity	User activities, such as login or logout.
pdu	Displays PDU-related events.
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: PXC/PXO does not support features regarding Schroff LHX, modem, Raritan asset management, and transfer switch so you can ignore these event types in the CLI.

Network Connections Diagnostic Log

This command shows the diagnostic log for both the EAP authentication and wireless LAN connection.

```
#        show network diagLog
```

Server Reachability Information

This command shows all server reachability information with a list of monitored servers and status.

```
#        show serverReachability
```

Server Reachability Information for a Specific Server

To show the server reachability information for a certain IT device only, use the following command.

```
#       show serverReachability server <n>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show serverReachability server <n> details
```

Variables:

- <n> is a number representing the sequence of the IT device in the monitored server list.

  You can find each IT device's sequence number using the CLI command of `show serverReachability` as illustrated below.

```
-------------------------------------------------------------
#  IP address       Enabled  Status
-------------------------------------------------------------
1  192.168.84.126   Yes      Waiting for reliable connection
2  www.raritan.com  Yes      Waiting for reliable connection
```

Displayed information:

- Without the parameter "details," only the specified device's IP address, monitoring enabled/disabled state and current status are displayed.
- With the parameter "details," more settings for the specified device are displayed, such as number of pings and wait time prior to the next ping.

Command History

This command shows the command history for current connection session.

```
#       show history
```

Displayed information:

- A list of commands that were previously entered in the current session is displayed.

Reliability Data

This command shows the reliability data.

```
#        show reliability data
```

Reliability Error Log

This command shows the reliability error log.

```
#        show reliability errorlog <n>
```

Variables:

- <n> is one of the options: *0* (zero) or any other integer number.

Option	Description
0	Displays all entries in the reliability error log. *Tip: You can also type the command without adding this option "0" to get all data.*
A specific integer number	Displays the specified number of last entries in the reliability error log.

Reliability Hardware Failures

This command shows a list of detected hardware failures.

```
#        show reliability hwfailures
```

For details, see ***Hardware Issue Detection*** (on page 352).

Examples

This section provides examples of the show command.

Raritan
A brand of legrand

Example 1 - Basic Security Information

The diagram shows the output of the *show security* command.

```
# show security
IPv4 access control: Disabled

IPv6 access control: Disabled

Role based access control for IPv4: Disabled

Role based access control for IPv6: Disabled

Password aging: Disabled

Prevent concurrent user login:   No

Strong passwords: Disabled

Restricted Service Agreement: disabled
```

Example 2 - In-Depth Security Information

More information is displayed when typing the *show security details* command.

```
# show security details
IPv4 access control: Disabled

IPv6 access control: Disabled

Role based access control for IPv4: Disabled

Role based access control for IPv6: Disabled

Password aging: Disabled

Prevent concurrent user login:   No
Maximum number of failed logins: 3
User block time:                 10 minutes

User idle timeout: 10 minutes

Strong passwords: Disabled

Restricted Service Agreement: disabled
Restricted Service Agreement Banner Content:
Unauthorized access prohibited; all access and activities not explicitl
y authorized by management are unauthorized. All activities are monitor
ed and logged. There is no privacy on this system. Unauthorized access
and activities or any criminal activity will be reported to appropriate
 authorities.

Front-Panel Permissions:
  Switch Outlet:              no
  Switch Peripheral Actuator: no
```

Clearing Information

You can use the clear commands to remove unnecessary data from the PXC/PXO.

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 389).*

Raritan
A brand of legrand

Clearing Event Log

This command removes all data from the event log.

```
#       clear eventlog
```

-- OR --

```
#       clear eventlog /y
```

If you entered the command without "/y," a message appears, prompting you to confirm the operation. Type y to clear the event log or n to abort the operation.

If you type y, a message "Event log was cleared successfully" is displayed after all data in the event log is deleted.

Clearing Diagnostic Log for Network Connections

This command removes all data from the diagnostic log for both the EAP authentication and WLAN connection.

```
#       clear networkDiagLog
```

-- OR --

```
#       clear networkDiagLog /y
```

If you entered the command without "/y," a message appears, prompting you to confirm the operation. Type y to clear the log or n to abort the operation.

Configuring the PXC/PXO Device and Network

To configure the PXC/PXO 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 389).*

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 422).**

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 389).

PDU Configuration Commands

One PDU configuration command begins with *pdu*. You can use the PDU configuration commands to change the settings that apply to the whole PXC/PXO device.

Configuration commands are case sensitive so ensure you capitalize them correctly.

Changing the PDU Name

This command changes the device name of PXC/PXO.

```
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 PXC/PXO 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 PXC/PXO powers up.
on	Switches ON all outlets when the PXC/PXO powers up.
lastKnownState	Restores all outlets to the previous status before powering down the PXC/PXO when the PDU powers up again.

Raritan
A brand of legrand

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 117) 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 130).

```
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 310).

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 310).

Specifying the Device Altitude

This command specifies the altitude of your PXC/PXO above sea level (in meters). You must specify the altitude of PXC/PXO above sea level if a Raritan's differential air pressure sensor is attached. This is because the device's altitude is associated with the altitude correction factor. See ***Altitude Correction Factors*** (on page 686).

```
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 523).*

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 167)..

Raritan
A brand of legrand

Setting the Maximum Number of Active Powered Dry Contact Actuators

This command determines the upper limit of "active" powered dry contact actuators on one PXC/PXO device. You need either 'Change Peripheral Device Configuration' privilege or 'Administrator Privileges' to change its upper limit.

```
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, or, if with a door handle connected, is OPENED.

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 PXC/PXO.

```
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 PXC/PXO 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).

Raritan
A brand of legrand

- <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 PXC/PXO is set to the bridging mode.

  Note: In the bridging mode, only the IP parameters of the BRIDGE interface function. The IP parameters of ETH1/ETH2 and WIRELESS interfaces do NOT function.

Interface	Description
eth1	Determine the IPv4 preferred host name of the ETH1 interface (that is, wired networking).
eth2	Determine the IPv4 preferred host name of the ETH2 interface (that is, wired networking).
wireless	Determine the IPv4 preferred host name of the WIRELESS interface (that is, wireless networking).
bridge	Determine the IPv4 preferred host name of the BRIDGE interface (that is, bridging mode).

- <name> is a host name which:
  - Consists of alphanumeric characters and/or hyphens
  - Cannot begin or end with a hyphen
  - Cannot contain more than 63 characters
  - Cannot contain punctuation marks, spaces, and other symbols

Setting the IPv4 Address

After selecting the static IP configuration mode, you can use this command to assign a permanent IP address to the PXC/PXO.

```
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 PXC/PXO 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 PXC/PXO. 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.

Raritan
A brand of legrand

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 PXC/PXO 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 203).

- **Method 1: add a static route when the other network is NOT directly reachable:**

```
config:#   network ipv4 staticRoutes add <dest-1> nextHop <hop>
```

- **Method 2: add a static route when the other network is directly reachable:**

```
config:#   network ipv4 staticRoutes add <dest-1> interface <ETH>
```

- **Delete an existing static route:**

```
config:#   network ipv4 staticRoutes delete <route_ID>
```

- **Modify an existing static route:**

```
config:#   network ipv4 staticRoutes modify <route_ID> dest <dest-2> nextHop <hop>
```

-- OR --

```
config:#    network ipv4 staticRoutes modify <route_ID> dest <dest-2> interface
            <ETH>
```

Variables:

- <dest-1> is a combination of the IP address and subnet mask of the other subnet. The format is *IP address/subnet mask*.
- <hop> is the IP address of the next hop router.
- <ETH> is one of the interfaces: *ETH1/ETH2*, *WIRELESS* and *BRIDGE*. Type "bridge" only when your PXC/PXO 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 PXC/PXO 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).

Raritan
A brand of legrand

Interface	Description
bridge	Determine the IPv6 configuration mode of the BRIDGE interface (that is, bridging mode).

- <mode> is one of the modes: *automatic* or *static*.

Mode	Description
automatic	The IPv6 configuration mode is set to automatic.
static	The IPv6 configuration mode is set to static IP address.

Setting the IPv6 Preferred Host Name

After selecting DHCP as the IPv6 configuration mode, you can specify the preferred host name, which is optional. The following is the command:

```
config:#   network ipv6 interface <ETH> preferredHostName <name>
```

Variables:

- <ETH> is one of the network interfaces: *ETH1/ETH2*, *WIRELESS*, or *BRIDGE*. Note that you must choose/configure the bridge interface if your PXC/PXO is set to the bridging mode.

  Note: In the bridging mode, only the IP parameters of the BRIDGE interface function. The IP parameters of ETH1/ETH2 and WIRELESS interfaces do NOT function.

Interface	Description
eth1	Determine the IPv6 preferred host name of the ETH1 interface (wired networking).
eth2	Determine the IPv6 preferred host name of the ETH2 interface (wired networking).
wireless	Determine the IPv6 preferred host name of the WIRELESS interface (that is, wireless networking).
bridge	Determine the IPv6 preferred host name of the BRIDGE interface (that is, bridging mode).

- <name> is a host name which:
  - Consists of alphanumeric characters and/or hyphens
  - Cannot begin or end with a hyphen
  - Cannot contain more than 63 characters

- 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 PXC/PXO.

```
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 PXC/PXO 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 PXC/PXO. 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.

Raritan
A brand of legrand

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 PXC/PXO 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 203).

▶ **Method 1: add a static route when the other network is NOT directly reachable:**

```
config:#   network ipv6 staticRoutes add <dest-1> nextHop <hop>
```

▶ **Method 2: add a static route when the other network is directly reachable:**

```
config:#   network ipv6 staticRoutes add <dest-1> interface <ETH>
```

▶ **Delete an existing static route:**

```
config:#   network ipv6 staticRoutes delete <route_ID>
```

▶ **Modify an existing static route:**

```
config:#   network ipv6 staticRoutes modify <route_ID> dest <dest-2>
           nextHop <hop>
```

-- OR --

```
config:#    network ipv6 staticRoutes modify <route_ID> dest <dest-2> interface
            <ETH>
```

Variables:

- <dest-1> is the IP address and prefix length of the subnet where the PXC/PXO 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 PXC/PXO 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 --

Raritan
A brand of legrand

```
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 PXC/PXO. 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.

Raritan
A brand of legrand

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 PXC/PXO selects the optimum transmission mode through auto-negotiation.
half	Half duplex: Data is transmitted in one direction (to or from the PXC/PXO) at a time.
full	Full duplex: Data is transmitted in both directions simultaneously.

Setting the LAN MTU

This command sets the MTU for the ethernet interface.

config:# *network ethernet <ETH> mtu <mtu>*

Variables:

- <ETH> is one of the options -- eth1 or eth2.
- <mtu> is the Maximum Transfer Unit. Enter a value from 1280-1500.

Setting the Ethernet Authentication Method

This command sets the authentication method for the selected Ethernet interface to either none or Extensible Authentication Protocol (EAP).

```
config:#   network ethernet <ETH> authMethod <method>
```

Variables:

- <ETH> is one of the options -- *eth1 or eth2*.

Option	Description
eth1	ETH1 port
eth2	ETH2 port

- <method> is one of the authentication methods: *NONE* or *EAP*.

Method	Description
NONE	The authentication method is set to NONE.
EAP	The authentication method is set to EAP.

Setting Ethernet EAP Parameters

When the selected Ethernet interface's authentication method is set to EAP, you must configure EAP authentication parameters, including outer authentication, inner authentication, EAP identity, client certificate, client private key, password, CA certificate, and RADIUS authentication server. For more information, see ***Ethernet Interface Settings*** (on page 194).

Determine the outer authentication protocol:

```
config:#   network ethernet <ETH> eapOuterAuthentication <outer_auth>
```

Determine the inner authentication protocol for authentication set to "EAP + PEAP":

Raritan
A brand of legrand

```
config:#    network ethernet <ETH> eapInnerAuthentication <inner_auth>
```

- **Set the EAP identity:**

  ```
  config:#    network ethernet <ETH> eapIdentity <identity>
  ```

- **Set the EAP password:**

  ```
  config:#    network ethernet <ETH> eapPassword
  ```

  After performing the above command, the PXC/PXO prompts you to enter the password. Then type the password and press Enter.

- **Provide a client certificate for authentication set to "EAP + TLS" or "EAP + PEAP + TLS":**

  ```
  config:#    network ethernet <ETH> eapClientCertificate
  ```

  After performing any certificate or private key commands, including commands for the client certificate, client private key, and CA certificate, the system prompts you to enter the contents of the wanted certificate or key. For an example with detailed procedure, see ***EAP CA Certificate Example*** (on page 445).

- **Provide a client private key for authentication set to "EAP + TLS" or "EAP + PEAP + TLS":**

  ```
  config:#    network ethernet <ETH> eapClientPrivateKey
  ```

- **Provide a CA TLS certificate for EAP:**

  ```
  config:#    network ethernet <ETH> eapCACertificate
  ```

- **Eable or disable verification of the TLS certificate chain:**

```
config:#    network ethernet <ETH> enableCertVerification <option1>
```

- **Allow expired and not yet valid TLS certificates:**

```
config:#    network ethernet <ETH> allowOffTimeRangeCerts <option2>
```

- **Allow network connection with incorrect system time:**

```
config:#    network ethernet <ETH> allowConnectionWithIncorrectClock
            <option3>
```

Set the RADIUS authentication server for EAP:

```
config:#    network ethernet <ETH> eapAuthServerName <FQDN>
```

Variables:

- <ETH> is one of the options -- *eth1 or eth2*.

Option	Description
eth1	ETH1 port
eth2	ETH2 port

- <outer_auth> is one of the options: *PEAP* or *TLS*.

Option	Description
PEAP	Outer authentication is set to Protected Extensible Authentication Protocol (PEAP).
TLS	Outer authentication is set to TLS.

- <inner_auth> is one of the options: *MS-CHAPv2* or *TLS*.

Option	Description
MSCHAPv2	Inner authentication is set to Microsoft's Challenge Authentication Protocol Version 2 (MS-CHAPv2).
TLS	Inner authentication is set to TLS.

- <identity> is your user name for the EAP authentication.
- <option1> is one of the options: *true* or *false*.

Option	Description
true	Enables the verification of the TLS certificate chain.
false	Disables the verification of the TLS certificate chain.

Raritan
A brand of legrand

- <option2> is one of the options: *true* or *false*.

Option	Description
true	Always make the network connection successful even though the TLS certificate chain contains any certificate which is outdated or not valid yet.
false	The network connection is NOT successfully established when the TLS certificate chain contains any certificate which is outdated or not valid yet.

- <option3> is one of the options: *true* or *false*.

Option	Description
true	Make the network connection successful when the PXC/PXO system time is earlier than the firmware build before synchronizing with the NTP server, causing the TLS certificate to become invalid.
false	The network connection is NOT successfully established when the PXC/PXO finds that the TLS certificate is not valid due to incorrect system time.

- <FQDN> is the name of the RADIUS server if it is present in the TLS certificate. The name must match the fully qualified domain name (FQDN) of the host shown in the certificate.

EAP CA Certificate Example

This section provides a CA certificate example for the Ethernet interface "ETH1". Your CA certificate contents should be different from the contents displayed in this example.

In addition, the procedure of uploading the client certificate and client private key in CLI is similar to the following example, except for the CLI command.

To provide a CA certificate:

1. Make sure you have entered the configuration mode. See ***Entering Configuration Mode*** (on page 421).
2. Type the following command for ETH1 and press Enter.

```
config:#   network ethernet eth1 eapCACertificate
```

3. The system prompts you to enter the contents of the CA certificate.

4. Open a CA certificate using a text editor. You should see certificate contents similar to the following.

```
--- BEGIN CERTIFICATE ---
MIICjTCCAfigAwIBAgIEMaYgRzALBgkqhkiG9w0BAQQwRTELMAkGA1UEBhMCVVMx
NjA0BgNVBAoTLU5hdGlvbmFsIEFlcm9uYXV0aWNzIGFuZCBTcGFjZSBBZG1pbmlz
dHJhdGlvbjAmFxE5NjA1MjgxMzQ5MDUrMDgwMBcROTgwNTI4MTM0OTA1KzA4MDAw
ZzELMAkGA1UEBhMCVVMxNjA0BgNVBAoTLU5hdGlvbmFsIEFlcm9uYXV0aWNzIGFu
ZCBTcGFjZSBBZG1pbmlzdHJhdGlvbjEgMAkGA1UEBRMCMTYwEwYDVQQDEwxTdGV2
ZSBTY2hvY2gwWDALBgkqhkiG9w0BAQEDSQAwRgJBALrAwyYdgxmzNP/ts0Uyf6Bp
miJYktU/w4NG67ULaN4B5CnEz7k57s9o3YY3LecETgQ5iQHmkwlYDTL2fTgVfw0C
AQOjgaswgagwZAYDVR0ZAQH/BFowWDBWMFQxCzAJBgNVBAYTAlVTMTYwNAYDVQQK
Ey1OYXRpb25hbCBBZXJvbmF1dGljcyBhbmQgU3BhY2UgQWRtaW5pc3RyYXRpb24x
DTALBgNVBAMTBENSTDEwFwYDVR0BAQH/BA0wC4AJODMyOTcwODEwMBgGA1UdAgQR
MA8ECTgzMjk3MDgyM4ACBSAwDQYDVR0KBAYwBAMCBkAwCwYJKoZIhvcNAQEEA4GB
AH2y1VCEw/A4zaXzSYZJTTUi3uawbbFiS2yxHvgf28+8Js0OHXk1H1w2d6qOHH21
X82tZXd/0JtG0g1T9usFFBDvYK8O0ebgz/P5ELJnBL2+atObEuJy1ZZ0pBDWINR3
WkDNLCGiTkCKp0F5EWIrVDwh54NNevkCQRZita+z4IBO
--- END CERTIFICATE ---
```

5. Select and copy the contents as illustrated below, including the starting line containing "BEGIN CERTIFICATE" and the ending line containing "END CERTIFICATE."
6. Paste the contents in the terminal.
7. Press Enter.
8. Verify whether the system shows the following command prompt, indicating the provided CA certificate is valid.

   ```
   config:#
   ```

Removing the Uploaded Certificate or Private Key

The procedures of removing an existing client certificate, client private key or CA certificate in CLI are similar.

This section illustrates such a procedure for the Ethernet interface "ETH1."

To remove a certificate or private key for ETH1:

1. Make sure you have entered the configuration mode. See ***Entering Configuration Mode*** (on page 421).
2. Type the appropriate command, depending on which file you want to remove, and press Enter.
   - *Client certificate:*

     ```
     config:#   network ethernet eth1 eapClientCertificate
     ```

   - *Client private key:*

     ```
     config:#   network ethernet eth1 eapClientPrivateKey
     ```

- *CA certificate:*

  ```
  config:#   network ethernet eth1 eapCACertificate
  ```

3. The system prompts you to enter the contents of the chosen certificate or private key.
4. Press Enter without typing any data.
5. Verify whether the system shows the following command prompt, indicating the existing certificate or private key has been removed.

   ```
   config:#
   ```

Setting Wireless Parameters

You must configure wireless parameters, including Service Set Identifier (SSID), authentication method, Pre-Shared Key (PSK), and Basic Service Set Identifier (BSSID) after the wireless networking mode is enabled.

A wireless configuration command begins with *network wireless*.

Note: If wireless networking mode is not enabled, the SSID, PSK and BSSID values are not applied until the wireless networking mode is enabled. In addition, a message appears, indicating that the active network interface is not wireless.

Setting the SSID

This command specifies the SSID string.

```
config:#   network wireless SSID <ssid>
```

Variables:

- <ssid> is the name of the wireless access point, which consists of:
  - Up to 32 ASCII characters
  - No spaces
  - ASCII codes 0x20 ~ 0x7E

Enabling or Disabling 802.11n High Throughput

This command enables or disables the 802.11n high throughput protocol.

```
config:#   network wireless enableHT <option>
```

Variables:

- <option> is one of the options: *true or false*.

Option	Description
true	802.11n is enabled.
false	802.11n is disabled.

Setting the Wireless Authentication Method

This command sets the wireless authentication method to either PSK or Extensible Authentication Protocol (EAP).

```
config:#   network wireless authMethod <method>
```

Variables:

- <method> is one of the authentication methods: *PSK* or *EAP*.

Method	Description
PSK	The authentication method is set to PSK.
EAP	The authentication method is set to EAP.

Setting the PSK

If the Pre-Shared Key (PSK) authentication method is selected, you must assign a PSK passphrase by using this command.

```
config:#   network wireless PSK <psk>
```

Variables:

- <psk> is a string or passphrase that consists of:
  - 8 to 63 characters
  - No spaces
  - ASCII codes 0x20 ~ 0x7E

Raritan
A brand of legrand

Setting Wireless EAP Parameters

When the wireless authentication method is set to EAP, you must configure EAP authentication parameters, including outer authentication, inner authentication, EAP identity, client certificate, client private key, password, CA certificate, and RADIUS authentication server. For more information, see ***Wireless Network Settings*** (on page 197).

- **Determine the outer authentication protocol:**

```
config:#   network wireless eapOuterAuthentication <outer_auth>
```

- **Determine the inner authentication protocol for authentication set to "EAP + PEAP":**

```
config:#   network wireless eapInnerAuthentication <inner_auth>
```

- **Set the EAP identity:**

```
config:#   network wireless eapIdentity <identity>
```

- **Set the EAP password:**

```
config:#   network wireless eapPassword
```

After performing the above command, the PXC/PXO prompts you to enter the password. Then type the password and press Enter.

- **Provide a Client Certificate for authentication set to "EAP + TLS" or "EAP + PEAP + TLS":**

```
config:#   network wireless eapClientCertificate
```

After performing any certificate or private key commands, including commands for the client certificate, client private key, and CA certificate, the system prompts you to enter the contents of the wanted certificate or key. For an example with detailed procedure, see ***EAP CA Certificate Example*** (on page 445).

- **Provide a Client Private Key for authentication set to "EAP + TLS" or "EAP + PEAP + TLS":**

```
config:#   network wireless eapClientPrivateKey
```

- **Provide a CA TLS certificate for EAP:**

```
config:#   network wireless eapCACertificate
```

- **Eable or disable verification of the TLS certificate chain:**

```
config:#   network wireless enableCertVerification <option1>
```

- **Allow expired and not yet valid TLS certificates:**

```
config:#   network wireless allowOffTimeRangeCerts <option2>
```

- **Allow wireless network connection with incorrect system time:**

```
config:#   network wireless allowConnectionWithIncorrectClock <option3>
```

- **Set the RADIUS authentication server for EAP:**

```
config:#   network wireless eapAuthServerName <FQDN>
```

Variables:

- <outer_auth> is one of the options: *PEAP* or *TLS*.

Option	Description
PEAP	Outer authentication is set to Protected Extensible Authentication Protocol (PEAP).
TLS	Outer authentication is set to TLS.

- <inner_auth> is one of the options: *MS-CHAPv2* or *TLS*.

Option	Description
MSCHAPv2	Inner authentication is set to Microsoft's Challenge Authentication Protocol Version 2 (MS-CHAPv2).
TLS	Inner authentication is set to TLS.

- <identity> is your user name for the EAP authentication.
- <option1> is one of the options: *true* or *false*.

Option	Description
true	Enables the verification of the TLS certificate chain.
false	Disables the verification of the TLS certificate chain.

- <option2> is one of the options: *true* or *false*.

Option	Description
true	Always make the network connection successful even though the TLS certificate chain contains any certificate which is outdated or not valid yet.

Raritan
A brand of legrand

Option	Description
false	The network connection is NOT successfully established when the TLS certificate chain contains any certificate which is outdated or not valid yet.

- <option3> is one of the options: *true* or *false*.

Option	Description
true	Make the network connection successful when the PXC/PXO system time is earlier than the firmware build before synchronizing with the NTP server, causing the TLS certificate to become invalid.
false	The network connection is NOT successfully established when the PXC/PXO finds that the TLS certificate is not valid due to incorrect system time.

- <FQDN> is the name of the RADIUS server if it is present in the TLS certificate. The name must match the fully qualified domain name (FQDN) of the host shown in the certificate.

Setting the BSSID

This command specifies the BSSID.

```
config:#   network wireless BSSID <bssid>
```

Variables:

- <bssid> is either the MAC address of the wireless access point or *none* for automatic selection.

Setting the Wireless MTU

This command sets the MTU for the wireless interface.

config:# network wireless mtu<mtu>

Variables:

- <mtu> is the Maximum Transfer Unit. Enter a value from 1280-1500.

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.

Raritan
A brand of legrand

If Port Forwarding mode is enabled, you must configure two more settings to finish the configuration:

On ALL cascaded devices, you must configure the 'role' setting one by one.

```
config:#   network portForwarding role <option2>
```

On the master device, you must configure the 'downstream interface' setting.

```
config:#   network portForwarding
           masterDownstreamInterface <option3>
```

Variables:

- <option2> is one of the following cascading roles:

Role	Description
master	The device is a master device.
slave	The device is a slave device.

- <option3> is one of the following options:

Option	Description
ETH1/ETH2	ETH1/ETH2 port is the port where the 1st slave device is connected.
Usb	USB port is the port where the 1st slave device is connected.

Setting Network Service Parameters

A network service command begins with *network services*.

Setting the HTTP Port

The commands used to configure the HTTP port settings begin with *network services http*.

Change the HTTP port:

```
config:#   network services http port <n>
```

Enable or disable the HTTP port:

```
config:#   network services http enabled <option>
```

Enforce redirection from HTTP to HTTPS:

```
config:#   network services http enforceHttps <option>
```

Variables:

- <n> is a TCP port number between 1 and 65535. The default HTTP port is 80.
- <option> is one of the options: *true* or *false*.

Option	Description
true	▪ The HTTP port is enabled. - OR - ▪ HTTP redirection to HTTPS is enabled.
false	▪ The HTTP port is disabled. - OR - ▪ HTTP redirection to HTTPS is disabled.

Raritan
A brand of legrand

Setting the HTTPS Port

The commands used to configure the HTTPS port settings begin with *network services https*.

Change the HTTPS port:

```
config:#   network services https port <n>
```

Enable or disable the HTTPS access:

```
config:#   network services https enabled <option>
```

Variables:

- <n> is a TCP port number between 1 and 65535. The default HTTPS port is 443.
- <option> is one of the options: *true* or *false*.

Option	Description
true	Forces any access to the PXC/PXO via HTTP to be redirected to HTTPS.
false	No HTTP access is redirected to HTTPS.

Changing the Telnet Configuration

You can enable or disable the Telnet service, or change its TCP port using the CLI commands.

A Telnet command begins with *network services telnet*.

Enabling or Disabling Telnet

This command enables or disables the Telnet service.

```
config:#   network services telnet enabled <option>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	The Telnet service is enabled.

Option	Description
false	The Telnet service is disabled.

Changing the Telnet Port

This command changes the Telnet port.

```
config:#   network services telnet port <n>
```

Variables:

- <n> is a TCP port number between 1 and 65535. The default Telnet port is 23.

Changing the SSH Configuration

You can enable or disable the SSH service, or change its TCP port using the CLI commands.

An SSH command begins with *network services ssh*.

Enabling or Disabling SSH

This command enables or disables the SSH service.

```
config:#   network services ssh enabled <option>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	The SSH service is enabled.
false	The SSH service is disabled.

Changing the SSH Port

This command changes the SSH port.

```
config:#   network services ssh port <n>
```

Variables:

- <n> is a TCP port number between 1 and 65535. The default SSH port is 22.

Raritan
A brand of legrand

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 501).

Setting the SNMP Configuration

You can enable or disable the SNMP v1/v2c or v3 agent, configure the read and write community strings, or set the MIB-II parameters, such as sysContact, using the CLI commands.

An SNMP command begins with *network services snmp*.

Enabling or Disabling SNMP v1/v2c

This command enables or disables the SNMP v1/v2c protocol.

```
config:#   network services snmp v1/v2c <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	The SNMP v1/v2c protocol is enabled.
disable	The SNMP v1/v2c protocol is disabled.

Enabling or Disabling SNMP v3

This command enables or disables the SNMP v3 protocol.

```
config:#   network services snmp v3 <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	The SNMP v3 protocol is enabled.
disable	The SNMP v3 protocol is disabled.

Setting the SNMP Read Community

This command sets the SNMP read-only community string.

```
config:#   network services snmp readCommunity <string>
```

Variables:

- <string> is a string comprising 4 to 64 ASCII printable characters.
- The string CANNOT include spaces.

Setting the SNMP Write Community

This command sets the SNMP read/write community string.

```
config:#   network services snmp writeCommunity <string>
```

Variables:

- <string> is a string comprising 4 to 64 ASCII printable characters.
- The string CANNOT include spaces.

Setting the sysContact Value

This command sets the SNMP MIB-II sysContact value.

```
config:#   network services snmp sysContact <value>
```

Variables:

- <value> is a string comprising 0 to 255 alphanumeric characters.

Raritan
A brand of legrand

Setting the sysName Value

This command sets the SNMP MIB-II sysName value.

```
config:#   network services snmp sysName <value>
```

Variables:

- <value> is a string comprising 0 to 255 alphanumeric characters.

Setting the sysLocation Value

This command sets the SNMP MIB-II sysLocation value.

```
config:#   network services snmp sysLocation <value>
```

Variables:

<value> is a string comprising 0 to 255 alphanumeric characters.

Changing the Modbus Configuration

You can enable or disable the Modbus agent, configure its read-only capability, or change its TCP port.

A Modbus command begins with *network services modbus*.

Enabling or Disabling Modbus

This command enables or disables the Modbus protocol.

```
config:#   network services modbus enabled <option>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	The Modbus agent is enabled.
false	The Modbus agent is disabled.

Enabling or Disabling the Read-Only Mode

This command enables or disables the read-only mode for the Modbus agent.

```
config:#   network services modbus readonly <option>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	The read-only mode is enabled.
false	The read-only mode is disabled.

Changing the Modbus Port

This command changes the Modbus port.

```
config:#   network services modbus port <n>
```

Variables:

- <n> is a TCP port number between 1 and 65535. The default Modbus port is 502.

Enabling or Disabling Service Advertising

This command enables or disables the zero configuration protocol, which enables advertising or auto discovery of network services. See ***Enabling Service Advertising*** (on page 226) for details.

```
config:#   network services zeroconfig <method> <option>
```

Variables:

- <method> is one of the options: *mdns* or *llmnr.*

Option	Description
mdns	Service advertisement via MDNS is enabled or disabled.
llmnr	Service advertisement via LLMNR is enabled or disabled.

Raritan
A brand of legrand

- <option> is one of the options: *enable* or *disable.*

Option	Description
enable	Service advertisement via the selected method (MDNS or LLMNR) is enabled.
disable	Service advertisement via the selected method (MDNS or LLMNR) is disabled.

Examples

This section illustrates several network configuration examples.

Example 1 - Wireless Networking Mode

The following command enables the wireless networking mode.

```
config:#   network wireless enabled true
```

Example 2 - Enabling IPv6 Protocol on the Ethernet Interface

The following command enables the IPv6 protocol on the ETH1 interface.

```
config:#   network ipv6 interface eth1 enabled true
```

Example 3 - Wireless Authentication Method

The following command sets the wireless authentication method to PSK.

```
config:#   network wireless authMethod PSK
```

Example 4 - Static IPv4 Configuration

The following command enables the Static IPv4 configuration mode on the ETH1 interface.

```
config:#   network ipv4 interface eth1 configMethod static
```

Time Configuration Commands

A time configuration command begins with *time*.

Determining the Time Setup Method

This command determines the method to configure the system date and time.

```
config:#   time method <method>
```

Variables:

- <method> is one of the time setup options: *manual* or *ntp*.

Mode	Description
manual	The date and time settings are customized.
ntp	The date and time settings synchronize with a specified NTP server.

Raritan
A brand of legrand

Setting NTP Parameters

A time configuration command for NTP-related parameters begins with *time ntp*.

- **Specify the primary time server:**

```
config:#   time ntp firstServer <first_server>
```

- **Specify the secondary time server:**

```
config:#   time ntp secondServer <second_server>
```

- **To delete the primary time server:**

```
config:#   time ntp firstServer ""
```

- **To delete the secondary time server:**

```
config:#   time ntp secondServer ""
```

Variables:

- The <first_server> is the IP address or host name of the primary NTP server.
- The <second_server> is the IP address or host name of the secondary NTP server.

Customizing the Date and Time

To manually configure the date and time, use the following CLI commands to specify them.

Note: You shall set the time configuration method to "manual" prior to customizing the date and time. See **Determining the Time Setup Method** *(on page 462).*

▶ **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 PXC/PXO.

```
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.

Raritan
A brand of legrand

3. Type `apply` for the selected time zone to take effect.

Setting the Automatic Daylight Savings Time

This command determines whether the daylight saving time is applied to the time settings.

```
config:#   time autoDST <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Mode	Description
enable	Daylight savings time is enabled.
disable	Daylight savings time is disabled.

Examples

This section illustrates several time configuration examples.

Example 1 - Time Setup Method

The following command sets the date and time settings by using the NTP servers.

```
config:#   time method ntp
```

Example 2 - Primary NTP Server

The following command sets the primary time server to 192.168.80.66.

```
config:#   time ntp firstServer 192.168.80.66
```

Checking the Accessibility of NTP Servers

This command verifies the accessibility of NTP servers specified manually on your PXC/PXO and then shows the result. For instructions on specifying NTP servers via CLI, see ***Setting NTP Parameters*** (on page 463).

To perform this command successfully, you must:

- Own the "Change Date/Time Settings" permission.
- Customize NTP servers. See ***Setting NTP Parameters*** (on page 463).

This command is available either in the administrator/user mode or in the configuration mode. See ***Different CLI Modes and Prompts*** (on page 389).

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 PXC/PXO from a specific or a range of IP addresses.

- An IPv4 firewall configuration command begins with *security ipAccessControl ipv4*.
- An IPv6 firewall configuration command begins with *security ipAccessControl ipv6*.

Modifying Firewall Control Parameters

There are different commands for modifying firewall control parameters.

- *IPv4 commands*

Enable or disable the IPv4 firewall control feature:

```
config:#   security ipAccessControl ipv4 enabled <option>
```

Determine the default IPv4 firewall control policy for inbound traffic:

```
config:#    security ipAccessControl ipv4 defaultPolicyIn <policy>
```

Determine the default IPv4 firewall control policy for outbound traffic:

```
config:#    security ipAccessControl ipv4 defaultPolicyOut <policy>
```

- *IPv6 commands*

Enable or disable the IPv6 firewall control feature:

```
config:#    security ipAccessControl ipv6 enabled <option>
```

Determine the default IPv6 firewall control policy for inbound traffic:

```
config:#    security ipAccessControl ipv6 defaultPolicyIn <policy>
```

Determine the default IPv6 firewall control policy for outbound traffic:

```
config:#    security ipAccessControl ipv6 defaultPolicyOut <policy>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	Enables the IP access control feature.
false	Disables the IP access control feature.

- <policy> is one of the options: *accept, drop* or *reject*.

Option	Description
accept	Accepts traffic from all IP addresses.
drop	Discards traffic from all IP addresses, without sending any failure notification to the source host.
reject	Discards traffic from all IP addresses, and an ICMP message is sent to the source host for failure notification.

Tip: You can combine both commands to modify all firewall control parameters at a time. See **Multi-Command Syntax** *(on page 544).*

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.

Raritan
A brand of legrand

Direction	Description
out	Outbound traffic.

- <rule_number> is the number of the existing rule that you want to modify.
- <ip_mask> is the combination of the IP address and subnet mask values (or prefix length), which are separated with a slash. For example, an IPv4 combination looks like this: *192.168.94.222/24*.
- <policy> is one of the options: *accept, drop* or *reject*.

Option	Description
accept	Accepts traffic from/to the specified IP address(es).
drop	Discards traffic from/to the specified IP address(es), without sending any failure notification to the source or destination host.
reject	Discards traffic from/to the specified IP address(es), and an ICMP message is sent to the source or destination host for failure notification.

Deleting a Firewall Rule

The following commands remove a specific IPv4 or IPv6 rule from the list.

▶ IPv4 commands

```
config:#   security ipAccessControl ipv4 rule delete <direction> <rule_number>
```

▶ IPv6 commands

```
config:#   security ipAccessControl ipv6 rule delete <direction> <rule_number>
```

Variables:

- <direction> is one of the options: *in* or *out*.

Direction	Description
in	Inbound traffic.
out	Outbound traffic.

- <rule_number> is the number of the existing rule that you want to remove.

Restricted Service Agreement

The CLI command used to set the Restricted Service Agreement feature begins with `security restrictedServiceAgreement`,

Enabling or Disabling the Restricted Service Agreement

This command activates or deactivates the Restricted Service Agreement.

```
config:#   security restrictedServiceAgreement enabled <option>
```

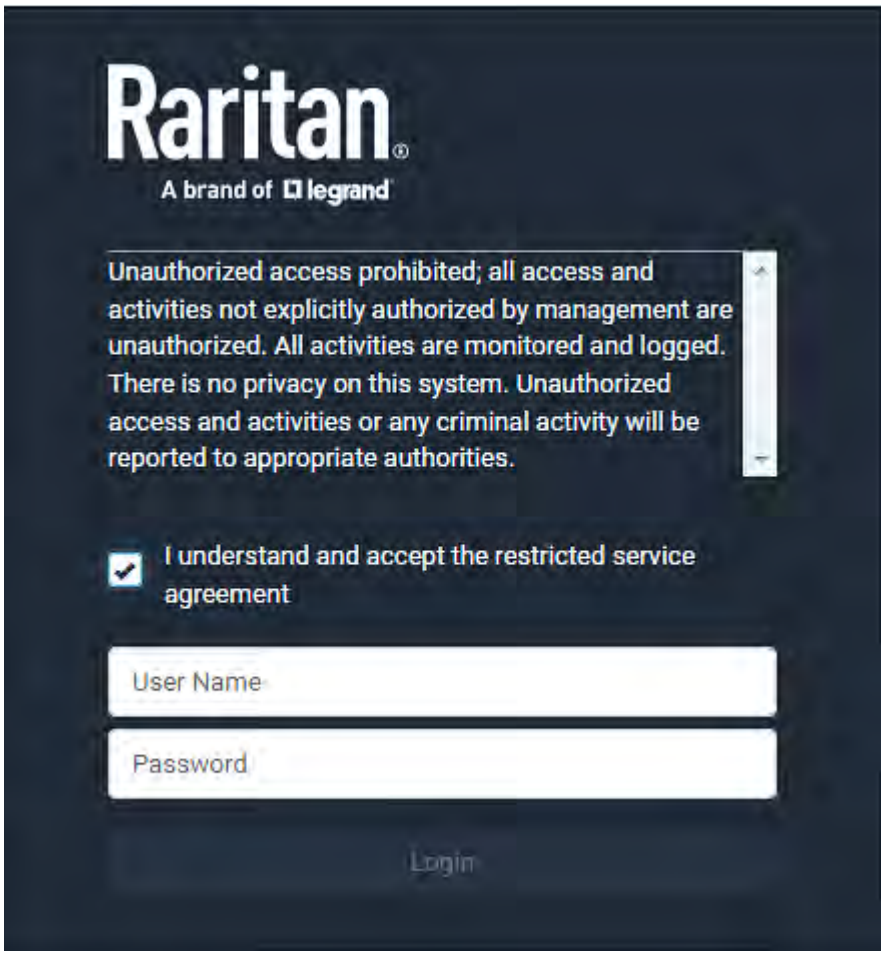
Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	Enables the Restricted Service Agreement feature.
false	Disables the Restricted Service Agreement feature.

Raritan
A brand of legrand

After the Restricted Service Agreement feature is enabled, the agreement's content is displayed on the login screen.



Do either of the following, or the login fails:

- In the web interface, select the checkbox labeled "I understand and accept the restricted service agreement."

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

- In the CLI, type y when the confirmation message "I understand and accept the restricted service agreement" is displayed.

Specifying the Agreement Contents

This command allows you to create or modify contents of the Restricted Service Agreement.

```
config:#   security restrictedServiceAgreement bannerContent
```

After performing the above command, do the following:

1. Type the text comprising up to 10,000 ASCII characters when the CLI prompts you to enter the content.
2. To end the content:
   a. Press Enter.
   b. Type `--END--` to indicate the end of the content.
   c. Press Enter again.

If the content is successfully entered, the CLI displays this message "Successfully entered Restricted Service Agreement" followed by the total number of entered characters in parentheses.

Note: The new content of Restricted Service Agreement is saved only after typing the `apply` command. See **Quitting Configuration Mode** *(on page 422).*

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 the PXC/PXO. If you are
   not the system administrator, do NOT operate it or change
   any settings 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.

Raritan
A brand of legrand

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 544).

Single Login Limitation

This command enables or disables the single login feature, which controls whether multiple logins using the same login name simultaneously is permitted.

```
config:#   security loginLimits singleLogin <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	Enables the single login feature.
disable	Disables the single login feature.

Password Aging

This command enables or disables the password aging feature, which controls whether the password should be changed at a regular interval:

```
config:#   security loginLimits passwordAging <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	Enables the password aging feature.
disable	Disables the password aging feature.

Password Aging Interval

This command determines how often the password should be changed.

```
config:#   security loginLimits passwordAgingInterval <value>
```

Variables:

- <value> is a numeric value in days set for the password aging interval. The interval ranges from 7 to 365 days.

Idle Timeout

This command determines how long a user can remain idle before that user is forced to log out of the PXC/PXO 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 544).

▶ **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.

Raritan
A brand of legrand

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 544).

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.

Raritan
A brand of legrand

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 544).*

Raritan
A brand of legrand

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:**

Raritan
A brand of legrand

```
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.

Raritan
A brand of legrand

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
```

Tip: If your PXC/PXO 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
```

Enabling or Disabling Front Panel Actuator Control

The following CLI commands control whether you can turn on or off connected actuator(s) by operating the front panel LCD display.

To enable the front panel actuator control feature:

```
config:#   security frontPanelPermissions add switchActuator
```

To disable the front panel actuator control feature:

```
config:#   security frontPanelPermissions remove switchActuator
```

Tip: If your PXC/PXO 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 in 192.168.84.123/24 accept
           insertAbove 5
```

Results:

- A new IPv4 firewall control rule is added to accept all packets sent from the IPv4 address 192.168.84.123.
- The newly-added rule is inserted above the 5th rule. That is, the new rule becomes the 5th rule, and the original 5th rule becomes the 6th rule.

Example 3 - User Blocking

The following command sets up two user blocking parameters.

```
config:#   security userBlocking maximumNumberOfFailedLogins 5 blockTime 30
```

Results:

- The maximum number of failed logins is set to 5.
- The user blocking time is set to 30 minutes.

Raritan
A brand of legrand

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 PXC/PXO 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 424).*

Raritan
A brand of legrand

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 425).*

Example - Outlet Naming

The following command assigns the name "Win XP" to outlet 8.

```
config:#   outlet 8 name "Win XP"
```

Outlet Group Configuration Commands

An outlet group configuration command begins with *outletgroup*. Such a command allows you to configure or operate an outlet group.

Creating an Outlet Group

This command creates a new outlet group.

```
config:#   outletgroup add "<name>" <members>
```

Variables:

- <name> is a string comprising up to 64 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.

  Tip: PXC/PXO allows you to assign the same name to diverse outlet groups. If this really occurs, you still can identify different groups through their unique index numbers.

- <members> is one or multiple member outlets' index numbers separated with commas. If the member outlets are consecutive outlets, you can type a hyphen between the initial and the final index number instead of using commas.

  For example, to assign outlets 3, 4, 5, 8 and 10 to the outlet group named "servers", you have two choices -- either use a hyphen for consecutive outlets 3 to 5, or use commas for all of member outlets:

  - `outletgroup add servers 3-5,8,10`

    -- OR --

  - `outletgroup add servers 3,4,5,8,10`

Managing an Outlet Group

You can modify an outlet group's name and member outlets, or simply remove any existing outlet group.

You can modify both the name and members of an outlet group at a time by combining multiple commands. See ***Multi-Command Syntax*** (on page 544).

Modify an outlet group's name:

```
config:#   outletgroup modify <ID> name "<name>"
```

Modify an outlet group's member outlets:

```
config:#   outletgroup modify <ID> members <members>
```

Delete an outlet group:

```
config:#   outletgroup delete <ID>
```

Variables:

- <ID> is an outlet group's index number.
- <name> is a string comprising up to 64 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.
- <members> is one or multiple member outlets' index numbers separated with commas. If the member outlets are consecutive outlets, you can type a hyphen between the initial and the final index number instead of using commas.

  For example, to assign outlets 3, 4, 5, 8 and 10 to the outlet group named "servers", you have two choices -- either use a hyphen for consecutive outlets 3 to 5, or use commas for all of member outlets:

  In the following examples, it is assumed that the "servers" outlet group's index number is 2.

Raritan
A brand of legrand

- `outletgroup modify 2 members 3-5,8,10`

  -- OR --
- `outletgroup modify 2 members 3,4,5,8,10`

Powering On/Off/Cycle Outlet Groups

This section applies to outlet-switching capable models only.

You must perform this operation in the *administrator mode*. See ***Different CLI Modes and Prompts*** (on page 389).

Power on one outlet group:

```
#       power outletgroup <ID> on
```

Power off one outlet group:

```
#       power outletgroup <ID> off
```

Power cycle one outlet group:

```
#       power outletgroup <ID> cycle
```

To quicken the operation, you can add the parameter "/y" to the end of the command, which confirms the operation.

For example:

```
#       power outletgroup <ID> off /y
```

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

Variables:

- <ID> is an outlet group's index number.

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 PXC/PXO contains multiple inlets, this command names the 1st inlet.

```
config:#   inlet 1 name "AC source"
```


Raritan
A brand of legrand

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 PXC/PXO.

```
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"
```

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 PXC/PXO 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 544).*

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, PXC/PXO 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 421).

Raritan
A brand of legrand

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 544).

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 PXC/PXO 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 544).

Enable or disable the SNMP v3 access to PXC/PXO for the specified user:

Raritan
A brand of legrand

```
config:#    user modify <name> snmpV3Access <option1>
```

- **Determine the security level:**

```
config:#    user modify <name> securityLevel <option2>
```

- **Determine whether the authentication passphrase is identical to the password:**

```
config:#    user modify <name> userPasswordAsAuthenticationPassphrase <option3>
```

- **Determine the authentication passphrase:**

```
config:#    user modify <name> authenticationPassPhrase
```

After performing the above command, PXC/PXO prompts you to enter the authentication passphrase.

- **Determine whether the privacy passphrase is identical to the authentication passphrase:**

```
config:#    user modify <name> useAuthenticationPassPhraseAsPrivacyPassPhrase <option4>
```

- **Determine the privacy passphrase:**

```
config:#    user modify <name> privacyPassPhrase
```

After performing the above command, PXC/PXO prompts you to enter the privacy passphrase.

- **Determine the authentication protocol:**

```
config:#    user modify <name> authenticationProtocol <option5>
```

- **Determine the privacy protocol:**

```
config:#   user modify <name> privacyProtocol <option6>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option1> is one of the options: *enable* or *disable*.

Option	Description
enable	Enables the SNMP v3 access permission for the specified user.
disable	Disables the SNMP v3 access permission for the specified user.

- <option2> is one of the options: *noAuthNoPriv*, *authNoPriv* or *authPriv*.

Option	Description
noAuthNoPriv	No authentication and no privacy.
authNoPriv	Authentication and no privacy.
authPriv	Authentication and privacy.

- <option3> is one of the options: *true* or *false*.

Option	Description
true	Authentication passphrase is identical to the password.
false	Authentication passphrase is different from the password.

- <option4> is one of the options: *true* or *false*.

Option	Description
true	Privacy passphrase is identical to the authentication passphrase.
false	Privacy passphrase is different from the authentication passphrase.

- <option5> is one of the options: *MD5* or *SHA-1*.

Option	Description
MD5	MD5 authentication protocol is applied.

Raritan
A brand of legrand

Option	Description
SHA-1	SHA-1 authentication protocol is applied.

- <option6> is one of the options: *DES* or *AES-128*.

Option	Description
DES	DES privacy protocol is applied.
AES-128	AES-128 privacy protocol is applied.

- An authentication or privacy passphrase is a string comprising 8 to 32 ASCII printable characters.

Changing the Role(s)

This command changes the role(s) of a specific user.

```
config:#   user modify <name> roles <roles>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <roles> is a role or a list of comma-separated roles assigned to the specified user profile. See ***All Privileges*** (on page 505).

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 544).

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 PXC/PXO user interfaces for all users via CLI, see **Setting Default Measurement Units** *(on page 502).*

Set the preferred temperature unit:

```
config:#   user modify <name> preferredTemperatureUnit <option1>
```

Set the preferred length unit:

```
config:#   user modify <name> preferredLengthUnit <option2>
```

Set the preferred pressure unit:

```
config:#   user modify <name> preferredPressureUnit <option3>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option1> is one of the options: *C* or *F*.

Option	Description
C	This option displays the temperature in Celsius.
F	This option displays the temperature in Fahrenheit.

- <option2> is one of the options: *meter* or *feet*.

Option	Description
meter	This option displays the length or height in meters.
feet	This option displays the length or height in feet.

- <option3> is one of the options: *pascal* or *psi*.

Option	Description
pascal	This option displays the pressure value in Pascals (Pa).
psi	This option displays the pressure value in psi.

Specifying the SSH Public Key

If the SSH key-based authentication is enabled, specify the SSH public key for each user profile using the following procedure.

To specify or change the SSH public key for a specific user:

1. Type the SSH public key command as shown below and press Enter.

   ```
   config:#   user modify <name> sshPublicKey
   ```

2. The system prompts you to enter the contents of the SSH public key. Do the following to input the contents:
   a. Open your SSH public key with a text editor.
   b. Copy all contents in the text editor.
   c. Paste the contents into the terminal.
   d. Press Enter.

To remove an existing SSH public key:

1. Type the same command as shown above.
2. When the system prompts you to input the contents, press Enter without typing or pasting anything.

Example

The following procedure illustrates how to change the SSH public key for the user "assistant."

1. Verify that you have entered the configuration mode. See ***Entering Configuration Mode*** (on page 421).
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 PXC/PXO 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 421).
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 PXC/PXO 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 544).

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

Raritan
A brand of legrand

Tip: To change the preferred measurement units displayed in the PXC/PXO user interfaces for a specific user via CLI, see **Changing Measurement Units** *(on page 499).*

▶ **Set the default temperature unit:**

```
config:#   user defaultpreferences preferredTemperatureUnit <option1>
```

▶ **Set the default length unit:**

```
config:#   user defaultpreferences preferredLengthUnit <option2>
```

▶ **Set the default pressure unit:**

```
config:#   user defaultpreferences preferredPressureUnit <option3>
```

Variables:

- <option1> is one of the options: *C* or *F*.

Option	Description
C	This option displays the temperature in Celsius.
F	This option displays the temperature in Fahrenheit.

- <option2> is one of the options: *meter* or *feet*.

Option	Description
meter	This option displays the length or height in meters.
feet	This option displays the length or height in feet.

- <option3> is one of the options: *pascal* or *psi*.

Option	Description
pascal	This option displays the pressure value in Pascals (Pa).
psi	This option displays the pressure value in psi.

Examples

This section illustrates several user configuration examples.

Example 1 - Creating a User Profile

The following command creates a new user profile and sets two parameters for the new user.

```
config:#   user create Mary enable admin
```

Results:

- A new user profile "Mary" is created.
- The new user profile is enabled.
- The **admin** role is assigned to the new user profile.

Example 2 - Modifying a User's Roles

The following command assigns two roles to the user "May."

```
config:#   user modify Mary roles admin,tester
```

Results:

- The user Mary has the union of all privileges of "admin" and "tester."

Example 3 - Default Measurement Units

The following command sets all default measurement units at a time.

```
config:#   user defaultpreferences preferredTemperatureUnit F preferredLengthUnit feet
           preferredPressureUnit psi
```

Results:

- The default temperature unit is set to Fahrenheit.
- The default length unit is set to feet.
- The default pressure unit is set to psi.

Raritan
A brand of legrand

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 505).
- <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
changeDataTimeSettings	Change Date/Time Settings

Privilege	Description
changeExternalSensorsConfiguration	Change Peripheral Device Configuration
changeLhxConfiguration	Change LHX/SHX Configuration
changeModemConfiguration	Change Modem Configuration
changeNetworkSettings	Change Network Settings
changePassword	Change Own Password
changePduConfiguration	Change 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
switchOutletGroup***	Switch Outlet Group
viewAuthSettings	View Authentication Settings
viewEventSetup	View Event Settings
viewEverything	Unrestricted View Privileges
viewLog	View Local Event Log
viewSecuritySettings	View Security Settings
viewSnmpSettings	View SNMP Settings
viewUserSettings	View Local User Management
viewWebcamSettings	View Webcam Snapshots and Configuration

* The "switchActuator" privilege requires an argument that is separated with a colon. The argument could be:

- All actuators, that is,
  `switchActuator:all`
- An actuator's ID number. For example:
  `switchActuator:1`
  `switchActuator:2`
  `switchActuator:3`
- A list of comma-separated ID numbers of different actuators. For example:
  `switchActuator:1,3,6`

Note: The ID number of each actuator is shown in the PXC/PXO web interface. It is an integer.

** 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`

*** The "switchOutletGroup" privilege requires an argument that is separated with a colon. The argument could be:

- All outlet groups, that is,
  `switchOutletGroup:all`
- An outlet group number. For example:
  `switchOutletGroup:1`
  `switchOutletGroup:2`
  `switchOutletGroup:3`
- A list of comma-separated outlet groups. For example:
  `switchOutletGroup: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>"
```

- **Add more privileges to a specific role:**

```
config:#    role modify <name> addPrivileges
            <privilege1>;<privilege2>;<privilege3>...
```

If a specific privilege contains any arguments, add a colon and the argument(s) after that privilege.

```
config:#    role modify <name> addPrivileges
            <privilege1>:<argument1>,<argument2>...;
            <privilege2>:<argument1>,<argument2>...;
            <privilege3>:<argument1>,<argument2>...;
            ...
```

- **Remove specific privileges from a role:**

```
config:#    role modify <name> removePrivileges
            <privilege1>;<privilege2>;<privilege3>...
```

If a specific privilege contains any arguments, add a colon and the argument(s) after that privilege.

```
config:#   role modify <name> removePrivileges
           <privilege1>:<argument1>,<argument2>...;
           <privilege2>:<argument1>,<argument2>...;
           <privilege3>:<argument1>,<argument2>...;
           ...
```

Note: When removing privileges from a role, make sure the specified privileges and arguments (if any) exactly match those assigned to the role. Otherwise, the command fails to remove specified privileges that are not available.

Variables:

- <name> is a string comprising up to 32 ASCII printable characters.
- <description> is a description comprising alphanumeric characters. The <description> variable must be enclosed in quotes when it contains spaces.
- <privilege1>, <privilege2>, <privilege3> and the like are names of the privileges assigned to the role. Separate each privilege with a semi-colon. See ***All Privileges*** (on page 505).
- <argument1>, <argument2> and the like are arguments set for a particular privilege. Separate a privilege and its argument(s) with a colon, and separate arguments with a comma if there are more than one argument for a privilege. For arguments syntax, see ***All Privileges*** (on page 505).

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.

Raritan
A brand of legrand

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 515).*

▶ **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 512). 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 412).*

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:*

Raritan
A brand of legrand

```
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 514).
`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 514).
`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: Select and copy the content including the starting line containing "BEGIN CERTIFICATE" and the ending 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 PXC/PXO. See ***Authentication Settings*** (on page 412).

Modifying an Existing LDAP Server

You can modify one or multiple parameters of an existing LDAP server, such as its IP address, TCP port number, Base DN and so on. Besides, you can also change the priority or sequence of existing LDAP servers in the server list.

Command syntax:

A command to modify an existing LDAP server's settings looks like the following:

```
config:#   authentication ldap modify <server_num> "parameters"
```

Variables:

- <server_num> is the sequential number of the specified server in the LDAP server list.
- Replace **"parameters"** with one or multiple commands in the following table, depending on which parameter(s) you want to modify.

A list of "parameters":

Parameters	Description
host <host>	Change the IP address or host name. ▪ <host> is the new IP address or host name.
port <port>	Change the TCP port number. ▪ <port> is the new TCP port number.
serverType <ldap_type>	Change the server type. ▪ <ldap_type> is the new type of the LDAP server. ▪ <ldap_type> values include: `openldap` and `activeDirectory`.
securityType <security>	Change the security type. ▪ <security> is the new security type. ▪ <security> values include: `none`, `startTls`, and `ssl`
bindType <bind_type>	Change the bind type. ▪ <bind_type> is the new bind type. ▪ <bind_type> values include: `anonymousBind` and `authenticatedBind`.
searchBaseDN <base_DN>	Change the base DN for search. ▪ <base_DN> is the new base DN for search.
loginNameAttribute <login_name_att>	Change the login name attribute. ▪ <login_name_att> is the new login name attribute.
userEntryObjectClass <user_entry_class>	Change the user entry object class. ▪ <user_entry_class> is the new user entry class.
userSearchSubfilter <user_search_filter>	Change the user search subfilter. ▪ <user_search_filter> is the new user search subfilter.
adDomain <AD_domain>	Change the Active Directory Domain name. ▪ <AD_domain> is the new domain name of the Active Directory.
verifyServerCertificate <verify_cert>	Enable or disable the certificate verification. ▪ <verify_cert> enables or disables the certificate verification feature. ▪ Available values include: `true`, `false`

Raritan
A brand of legrand

Parameters	Description
certificate	Re-upload a different certificate. a. First add the "certificate" parameter to the command, and press Enter. b. The system prompts you for the input of the certificate. c. Type or copy the content of the certificate in the CLI and press Enter.
allowExpiredCertificate <allow_exp_cert>	Determine whether to accept a certificate which is expired or not valid yet. ▪ <allow_exp_cert> determines whether to accept an expired or not valid yet certificate ▪ <allow_exp_cert> values include: `true`, and `false`
bindDN <bind_DN>	Change the bind DN. ▪ <bind_DN> is the new bind DN.
bindPassword	Change the bind DN password. a. First add the "bindPassword" parameter to the command, and press Enter. b. The system prompts you for the input of the password. c. Type the password and press Enter.
sortPosition <position>	Change the priority of the server (that is, resorting). ▪ <position> is the new sequential number of the server in the LDAP server list.

Note: For details of the above variables' values, see **Adding an LDAP Server** *(on page 511).*

Examples:

- **Change the IP address of the 1st LDAP server**

```
config:#    authentication ldap modify 1 host 192.168.3.3
```

- **Change both the IP address and TCP port of the 1st LDAP server**

```
config:#    authentication ldap modify 1 host 192.168.3.3 port 633
```

- **Change the IP address, TCP port and the type of the L1st DAP server**

```
config:#    authentication ldap modify 1 host 192.168.3.3 port 633
            serverType activeDirectory
```

Removing an Existing LDAP Server

This command removes an existing LDAP server from the server list.

```
config:#   authentication ldap delete <server_num>
```

Variables:

- <server_num> is the sequential number of the specified server in the LDAP server list.

Radius Settings

All Radius-related commands begin with *authentication radius*.

If you enable Radius authentication, you must add at least one Radius server. Later you can modify or delete any existing Radius server as needed.

Adding a Radius Server

You can repeat the following commands to add Radius servers one by one.

Command syntax:

```
config:#   authentication radius add <host> <rds_type> <auth_port> <acct_port> <timeout>
           <retries>
```

Variables:

- <host> is the IP address or host name of the Radius server.
- <rds_type> is one of the Radius authentication types: *pap, chap, msChapV2*.

Type	Description
chap	CHAP
pap	PAP
msChapV2	MSCHAP v2

- <auth_port> is the authentication port number.
- <acct_port> is the accounting port number.
- <timeout> is the timeout value in seconds. It ranges between 1 to 10 seconds.
- <retries> is the number of retries. It ranges between 0 to 5.

To enter the shared secret:

1. After executing the above Radius command, the system automatically prompts you to enter the shared secret.
2. Type the secret and press Enter.
3. Re-type the same secret and press Enter.

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.

Raritan
A brand of legrand

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 537).*

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 PXC/PXO web interface or using the command "`show externalsensors <n>`" in the CLI. It is an integer starting at 1.
- <name> is a string comprising up to 64 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.

Note: To name an actuator, see **Actuator Configuration Commands** *(on page 537).*

Specifying the CC Sensor Type

Raritan's contact closure sensor supports the connection of diverse third-party. You must specify the type of connected detector/switch for proper operation. Use this command when you need to specify the sensor type.

```
config:#   externalsensor <n> sensorSubType <sensor_type>
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is available in the PXC/PXO web interface or using the command "`show externalsensors <n>`" in the CLI. It is an integer starting at 1.
- <sensor_type> is one of these types: *contact*, *smokeDetection*, *waterDetection* or *vibration*.

Type	Description
contact	The connected detector/switch is for detection of door lock or door closed/open status.

Type	Description
smokeDetection	The connected detector/switch is for detection of the smoke presence.
waterDetection	The connected detector/switch is for detection of the water presence.
vibration	The connected detector/switch is for detection of the vibration.

Setting the X Coordinate

This command specifies the X coordinate of an environmental sensor.

```
config:#   externalsensor <n> xlabel "<coordinate>"
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is available in the PXC/PXO web interface or using the command "`show externalsensors <n>`" in the CLI. It is an integer starting at 1.
- <coordinate> is a string comprising up to 24 ASCII printable characters, and it must be enclosed in quotes.

Setting the Y Coordinate

This command specifies the Y coordinate of an environmental sensor.

```
config:#   externalsensor <n> ylabel "<coordinate>"
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is available in the PXC/PXO web interface or using the command "`show externalsensors <n>`" in the CLI. It is an integer starting at 1.
- <coordinate> is a string comprising up to 24 ASCII printable characters, and it must be enclosed in quotes.

Raritan
A brand of legrand

Setting the Z Coordinate

This command specifies the Z coordinate of an environmental sensor.

```
config:#   externalsensor <n> zlabel "<coordinate>"
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is available in the PXC/PXO web interface or using the command "`show externalsensors <n>`" in the CLI. It is an integer starting at 1.
- Depending on the Z coordinate format you set, there are two types of values for the <coordinate> variable:

Type	Description
Free form	<coordinate> is a string comprising up to 24 ASCII printable characters, and it must be enclosed in quotes.
Rack units	<coordinate> is an integer number in rack units.

Note: To specify the Z coordinate using the rack units, see **Setting the Z Coordinate Format for Environmental Sensors** *(on page 428).*

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 PXC/PXO web interface or using the command "`show externalsensors <n>`" in the CLI. It is an integer starting at 1.
- <description> is a string comprising up to 64 ASCII printable characters, and it must be enclosed in quotes when it contains spaces.

Using Default Thresholds

This command determines whether default thresholds, including the deassertion hysteresis and assertion timeout, are applied to a specific environmental sensor.

```
config:#   externalsensor <n> useDefaultThresholds <option>
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is available in the PXC/PXO web interface or using the command "`show externalsensors <n>`" in the CLI. It is an integer starting at 1.
- <option> is one of the options: *true* or *false*.

Option	Description
true	Default thresholds are selected as the threshold option for the specified sensor.
false	Sensor-specific thresholds are selected as the threshold option for the specified sensor.

Setting the Alarmed to Normal Delay for DX-PIR

This command determines the value of the Alarmed to Normal Delay setting for a Raritan presence detector.

```
config:#   externalsensor <n> alarmedToNormalDelay <time>
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is available in the PXC/PXO web interface or using the command "`show externalsensors <n>`" in the CLI. It is an integer starting at 1.
- <time> is an integer number in seconds, ranging between 0 and 300.

Examples

This section illustrates several environmental sensor configuration examples.

Raritan
A brand of legrand

Example 1 - Environmental Sensor Naming

The following command assigns the name "Cabinet humidity" to the environmental sensor with the ID number 4.

```
config:#   externalsensor 4 name "Cabinet humidity"
```

Example 2 - Sensor Threshold Selection

The following command sets the environmental sensor #1 to use the default thresholds, including the deassertion hysteresis and assertion timeout, as its threshold settings.

```
config:#   externalsensor 1 useDefaultThresholds true
```

Configuring Environmental Sensors' Default Thresholds

You can set the default values of upper and lower thresholds, deassertion hysteresis and assertion timeout on a sensor type basis, including temperature, humidity, air pressure and air flow sensors. The default thresholds automatically apply to all environmental sensors that are newly detected or added.

A default threshold configuration command begins with *defaultThresholds*.

You can configure various default threshold settings for the same sensor type at a time by combining multiple commands. See ***Multi-Command Syntax*** (on page 544).

- **Set the Default Upper Critical Threshold for a specific sensor type:**

```
config:#   defaultThresholds <sensor type> upperCritical <value>
```

- **Set the Default Upper Warning Threshold for a specific sensor type:**

```
config:#   defaultThresholds <sensor type> upperWarning <value>
```

- **Set the Default Lower Critical Threshold for a specific sensor type:**

```
config:#   defaultThresholds <sensor type> lowerCritical <value>
```

- **Set the Default Lower Warning Threshold for a specific sensor type:**

```
config:#   defaultThresholds <sensor type> lowerWarning <value>
```

- **Set the Default Deassertion Hysteresis for a specific sensor type:**

```
config:#   defaultThresholds <sensor type> hysteresis <hy_value>
```

Set the Default Assertion Timeout for a specific sensor type:

```
config:#   defaultThresholds <sensor type> assertionTimeout <as_value>
```

Variables:

- <sensor type> is one of the following numeric sensor types:

Sensor types	Description
absoluteHumidity	Absolute humidity sensors
relativeHumidity	Relative humidity sensors
temperature	Temperature sensors
airPressure	Air pressure sensors
airFlow	Air flow sensors
vibration	Vibration sensors

- <value> is the value for the specified threshold of the specified sensor type. Note that diverse sensor types use different measurement units.

Sensor types	Measurement units
absoluteHumidity	g/m^3 (that is, g/m³)
relativeHumidity	%
temperature	Degrees Celsius (°C) or Fahrenheit (°F), depending on your measurement unit settings.
airPressure	Pascal (Pa) or psi, depending on your measurement unit settings.
airFlow	m/s
vibration	g

- <hy_value> is the deassertion hysteresis value applied to the specified sensor type.
- <as_value> is the assertion timeout value applied to the specified sensor type. It ranges from 0 to 100 (samples).

Raritan
A brand of legrand

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 544).

▶ **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.

Raritan
A brand of legrand

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 681).
- <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 679).

Additional sensors supported:

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 544).

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.

Raritan
A brand of legrand

- <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 681).
- <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 679).

Additional sensors supported:

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 544).

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.

Option	Description
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 681).
- <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 679).

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 544).

▶ **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 PXC/PXO web interface or using the command "`show externalsensors <n>`" in the CLI. It is an integer starting at 1.
- <sensor type> is one of the following numeric sensor types:

Sensor types	Description
absoluteHumidity	Absolute humidity sensors
relativeHumidity	Relative humidity sensors
temperature	Temperature sensors
airPressure	Air pressure sensors
airFlow	Air flow sensors
vibration	Vibration sensors

Note: If the specified sensor type does not match the type of the specified environmental sensor, this error message appears: "Specified sensor type 'XXX' does not match the sensor's type (<sensortype>)," where XXX is the specified sensor type, and <sensortype> is the correct sensor type.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the specified threshold for a specific environmental sensor.
disable	Disables the specified threshold for a specific environmental sensor.
A numeric value	Sets a value for the specified threshold of a specific environmental sensor and enables this threshold at the same time.

Raritan
A brand of legrand

- <hy_value> is a numeric value that is assigned to the hysteresis for the specified environmental sensor. See ***"To De-assert" and Deassertion Hysteresis*** (on page 681).
- <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 679).

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 544).

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 PXC/PXO 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 428).*

- <description> is a string comprising up to 64 ASCII printable characters, and it must be enclosed in quotes when it contains spaces.

Example - Actuator Naming

The following command assigns the name "Door lock of cabinet 3" to the actuator whose ID number is 9.

```
config:#   actuator 9 name "Door lock of cabinet 3"
```

Server Reachability Configuration Commands

You can use the CLI to add or delete an IT device, such as a server, from the server reachability list, or modify the settings for a monitored IT device. A server reachability configuration command begins with *serverReachability*.

Adding a Monitored Device

This command adds a new IT device to the server reachability list.

```
config:#   serverReachability add <IP_host> <enable> <succ_ping>
           <fail_ping> <succ_wait> <fail_wait> <resume> <disable_count>
```

Variables:

- <IP_host> is the IP address or host name of the IT device that you want to add.
- <enable> is one of the options: *true* or *false*.

Option	Description
true	Enables the ping monitoring feature for the newly added device.
false	Disables the ping monitoring feature for the newly added device.

Raritan
A brand of legrand

- <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 PXC/PXO 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 PXC/PXO 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 544).

▶ **Modify a device's IP address or host name:**

```
config:#   serverReachability modify <n> ipAddress <IP_host>
```

▶ **Enable or disable the ping monitoring feature for the device:**

```
config:#    serverReachability modify <n> pingMonitoringEnabled <option>
```

Modify the number of successful pings for declaring "Reachable":

```
config:#    serverReachability modify <n> numberOfSuccessfulPingsToEnable
<succ_number>
```

Modify the number of unsuccessful pings for declaring "Unreachable":

```
config:#    serverReachability modify <n> numberOfUnsuccessfulPingsForFailure
<fail_number>
```

Modify the wait time after a successful ping:

```
config:#    serverReachability modify <n> waitTimeAfterSuccessfulPing
<succ_wait>
```

Modify the wait time after a unsuccessful ping:

```
config:#    serverReachability modify <n> waitTimeAfterUnsuccessfulPing
<fail_wait>
```

Modify the wait time before resuming pinging after declaring "Unreachable":

```
config:#    serverReachability modify <n> waitTimeBeforeResumingPinging
<resume>
```

Modify the number of consecutive "Unreachable" declarations before disabling the ping monitoring feature:

```
config:#    serverReachability modify <n> numberOfFailuresToDisable
<disable_count>
```

Variables:

- <n> is a number representing the sequence of the IT device in the server monitoring list.
- <IP_host> is the IP address or host name of the IT device whose settings you want to modify.
- <option> is one of the options: *true* or *false*.

Option	Description
true	Enables the ping monitoring feature for the monitored device.
false	Disables the ping monitoring feature for the monitored device.

- <succ_number> is the number of successful pings for declaring the monitored device "Reachable." Valid range is 0 to 200.
- <fail_number> is the number of consecutive unsuccessful pings for declaring the monitored device "Unreachable." Valid range is 1 to 100.
- <succ_wait> is the wait time to send the next ping after a successful ping. Valid range is 5 to 600 (seconds).
- <fail_wait> is the wait time to send the next ping after a unsuccessful ping. Valid range is 3 to 600 (seconds).
- <resume> is the wait time before the PXC/PXO 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 PXC/PXO 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 PXC/PXO 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.

Option	Description
false	The Cisco EnergyWise feature is disabled.

Specifying the EnergyWise Domain

This command syntax specifies to which Cisco® EnergyWise domain the PXC/PXO 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.

Raritan
A brand of legrand

Setting the Polling Interval

This command syntax determines the polling interval at which the Cisco® EnergyWise domain queries the PXC/PXO.

```
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 PXC/PXO 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 PXC/PXO 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 PXC/PXO 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 PXC/PXO device's serial port to 9600 bps.

```
config:#   serial consoleBaudRate 9600
```

Multi-Command Syntax

To shorten the configuration time, you can combine various configuration commands in one command to perform all of them at a time. All combined commands must belong to the same configuration type, such as commands prefixed with *network*, *user modify*, *sensor externalsensor* and so on.

A multi-command syntax looks like this:

```
<configuration type> <setting 1> <value 1> <setting 2>
<value 2> <setting 3> <value 3> ...
```

Example 1 - Combination of ETH1's Activation, Configuration Method and IP

The following multi-command syntax configures IPv4 address, configuration method and activation status for ETH1's network connectivity simultaneously.

```
config:#   network ipv4 interface eth1 enabled true configMethod static
           address 192.168.84.225/24
```

Results:

- The ETH1 interface is enabled.
- ETH1's configuration method is set to static IP address.
- ETH1's IPv4 address is set to 192.168.84.225/24.

Example 2 - Combination of 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.

Raritan
A brand of legrand

```
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 389).

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, PXC/PXO 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 PXC/PXO enter the load shedding mode.

```
config:#    loadshedding start
```


Raritan
A brand of legrand

Power Control Operations

This section applies to outlet-switching capable models only.

Outlets on the PXC/PXO can be turned on or off, or power cycled through the CLI.

Besides, you can cancel the power-on process while the PXC/PXO is powering on ALL outlets.

You must perform this operation in the *administrator mode*. See ***Different CLI Modes and Prompts*** (on page 389).

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`.

Option	Description
A range of outlets with a hyphen 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

If you have configured outlet switching sequence and/or delay, PXC/PXO will prompt you with one more question:

`Should outlet sequence order and delays be used during switching?`

- Type `y` to apply the current outlet sequence and delay settings when switching on outlets. See ***Setting Outlet Power-On Sequence and Delay*** (on page 128).
- Type `n` to apply the default sequence and delays.

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.

Raritan
A brand of legrand

Option	Description
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 a hyphen 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.

Option	Description
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 a hyphen 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

If you have configured outlet switching sequence and/or delay, PXC/PXO will prompt you with one more question:

`Should outlet sequence order and delays be used during switching?`

- Type `y` to apply the current outlet sequence and delay settings when switching on outlets. See ***Setting Outlet Power-On Sequence and Delay*** (on page 128).
- Type `n` to apply the default sequence and delays.

Raritan
A brand of legrand

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 Raritan sensor package, can control a mechanism or system. You can switch on or off that mechanism or system through the actuator control command in the CLI.

Perform these commands in the administrator or user mode. See ***Different CLI Modes and Prompts*** (on page 389).

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 PXC/PXO web interface or using the show command in the CLI. It is an integer starting at 1.

If you entered the command without "/y", a message appears, prompting you to confirm the operation. Then:

- Type y to confirm the operation, OR
- Type n to abort the operation

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 PXC/PXO web interface or using the show command in the CLI. It is an integer starting at 1.

If you entered the command without "/y", a message appears, prompting you to confirm the operation. Then:

- Type y to confirm the operation, OR

- Type n to abort the operation

Example - Turning On a Specific Actuator

The following command turns on the actuator whose ID number is 8.

```
#     control actuator 8 on
```

Unblocking a User

If any user is blocked from accessing the PXC/PXO, you can unblock them at the local console.

To unblock a user:

1. Access the CLI interface using any terminal program via a local connection. See ***With HyperTerminal*** (on page 387).
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 PXC/PXO

You can reset the PXC/PXO to factory defaults or simply restart it using the CLI commands.

Restarting the PDU

This command restarts the PXC/PXO. It is not a factory default reset.

To restart the PXC/PXO:

1. Ensure you have entered administrator mode and the # prompt is displayed.
2. Type either of the following commands to restart the PXC/PXO.

```
#     reset unit
```

-- OR --

```
#     reset unit /y
```

3. If you entered the command without "/y" in Step 2, a message appears prompting you to confirm the operation. Type y to confirm the reset.
4. Wait until the reset is complete.

Note: Device reset will cause CLI communications over an "USB" connection to be lost. Therefore, re-connect the USB cable after the reset is complete.

Resetting to Factory Defaults

The following commands restore all settings of the PXC/PXO to factory defaults.

To reset PXC/PXO settings after login, use either command:

```
#     reset factorydefaults
```

-- OR --

```
#     reset factorydefaults /y
```

To reset PXC/PXO settings before login:

```
Username:   factorydefaults
```

See ***Using the CLI Command*** (on page 620) for details.

Note: Device reset will cause CLI communications over an "USB" connection to be lost. Therefore, re-connect the USB cable after the reset is complete.

Network Troubleshooting

The PXC/PXO 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.

Raritan
A brand of legrand

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 389).

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>
```


Raritan
A brand of legrand

Tracing the Route

This command syntax traces the network route between your PXC/PXO and a network host.

```
diag>       traceroute <host> <useICMP>
```

Variables:

- <host> is the name or IP address of the host you want to trace.
- <useICMP> is optional. It has only one value -- `useICMP`. Type `useICMP` in the end of this command only when you want to use ICMP packets rather than UDP packets.

Example - Ping Command

The following command checks the network connectivity of the host 192.168.84.222 by sending the ICMP ECHO_REQUEST message to the host for 5 times.

```
diag>       ping 192.168.84.222 count 5
```

Retrieving Previous Commands

If you would like to retrieve any command that was previously typed in the same connection session, press the Up arrow (↑) on the keyboard several times until the desired command is displayed.

Automatically Completing a Command

A CLI command always consists of several words. You can easily enter a command by typing first word(s) or letter(s) and then pressing Tab or Ctrl+i instead of typing the whole command word by word.

To have a command completed automatically:

1. Type initial letters or words of the desired command. Make sure the letters or words you typed are unique so that the CLI can identify the command you want.
2. Press Tab or Ctrl+i until the complete command appears.
3. If there are more than one possible commands, a list of these commands is displayed. Then type the full command.

Examples:

- **Example 1 (only one possible command):**
  a. Type the first word and the first letter of the second word of the "`reset factorydefaults`" command -- that is, `reset f`.
  b. Then press Tab or Ctrl+i to complete the second word.
- **Example 2 (only one possible command):**
  a. Type the first word and initial letters of the second word of the "`security strongPasswords`" command -- that is, `security str`.
  b. Then press Tab or Ctrl+i to complete the second word.
- **Example 3 (more than one possible commands):**
  a. Type only the first two words of the "`network ipv4 gateway xxx.xxx.xxx.xxx`" command -- that is, `network ipv4.`
  b. Then press Tab or Ctrl+i one or two times, a list of possible commands displays as shown below.

```
gateway              interface          staticRoutes
```

  c. Type the full command "`network ipv4 gateway xxx.xxx.xxx.xxx`", according to the onscreen command list.

Logging out of CLI

After completing your tasks using the CLI, always log out of the CLI to prevent others from accessing the CLI.

To log out of the CLI:

1. Ensure you have entered administrator mode and the # prompt is displayed.
2. Type `exit` and press Enter.

Raritan
A brand of legrand

Chapter 9 Using SCP Commands

You can perform a Secure Copy (SCP) command to update the PXC/PXO firmware, do bulk configuration, or back up and restore the configuration.

Note: SCP cannot be used until you have changed the default admin password.

In This Chapter

Firmware Update via SCP 559
Bulk Configuration via SCP 560
Backup and Restore via SCP 561
Downloading Diagnostic Data via SCP 562
Uploading or Downloading Raw Configuration Data 564

Firmware Update via SCP

Same as any PXC/PXO firmware update, all user management operations are suspended and all login attempts fail during the SCP firmware update. For details, see ***Updating the PXC/PXO Firmware*** (on page 340).

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 PXC/PXO firmware's filename. If the firmware file is not in the current directory, you must include the path in the filename.
   - *<user name>* is the "admin" or any user profile with the Firmware Update permission.
   - <device ip> is the IP address or hostname of the PXC/PXO where you want to upload the specified file.
2. Type the password when prompted, and press Enter.
3. The system transmits the specified firmware file to the PXC/PXO, and shows the transmission speed and percentage.
4. When the transmission is complete, it shows the following message, indicating that the PXC/PXO 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 PXC/PXO.

b. Copy the configuration file to one or multiple destination PXC/PXO.

For detailed information on the bulk configuration requirements, see ***Bulk Configuration*** (on page 343).

To save the configuration via SCP:

1. Type the following SCP command and press Enter.

   ```
   scp <user name>@<device ip>:/bulk_config.txt <filename>
   ```

   - *<user name>* is the "admin" or any user profile with Administrator Privileges.
   - *<device ip>* is the IP address or hostname of the PXC/PXO whose configuration you want to save.
   - *<filename>* is the custom filename you assign to the "bulk_config.txt" of the source PXC/PXO.
2. Type the user password when prompted.
3. The system saves the configuration from the PXC/PXO to a file named "bulk_config.txt."

To copy the configuration via SCP:

1. Type the following SCP command and press Enter.

   ```
   scp bulk_config.txt <user name>@<device ip>:/bulk_restore
   ```

   - *<user name>* is the "admin" or any user profile with Administrator Privileges
   - *<device ip>* is the IP address of the PXC/PXO whose configuration you want to copy.
2. Type the user password when prompted.

Raritan
A brand of legrand

3. The system copies the configuration included in the file "bulk_config.txt" to another PXC/PXO, and displays the following message.

```
Starting restore operation. The connection will be
closed now.
```

SCP examples:

- Save operation:

```
scp admin@192.168.87.50:/bulk_config.txt today_config.txt
```

- Copy operation:

```
scp today_config.txt admin@192.168.87.47:/bulk_restore
```

Windows PSCP commands:

PSCP in Windows works in a similar way to the SCP.

- Save operation:

```
pscp <user name>@<device ip>:/bulk_config.txt today_config.txt
```

- Copy operation:

```
pscp today_config.txt <user name>@<device ip>:/bulk_restore
```

Alternative of bulk configuration via SCP:

Both methods of uploading 'bulk configuration' file or 'raw configuration' file via SCP can serve the purpose of bulk configuration. The only difference is that you can configure *device-specific* settings with the upload of raw configuration but not with the 'bulk configuration' file.

- ***Uploading or Downloading Raw Configuration Data*** (on page 564)

Backup and Restore via SCP

To back up ALL settings of a PXC/PXO, including device-specific settings, you should perform the backup operation instead of the bulk configuration.

You can restore all settings to previous ones after a backup file is available.

To back up the settings via SCP:

1. Type the following SCP command and press Enter.

```
scp <user name>@<device ip>:/backup_settings.txt
```

   - *<user name>* is the "admin" or any user profile with Administrator Privileges

- *<device ip>* is the IP address or hostname of the PXC/PXO whose settings you want to back up.

2. Type the user password when prompted.
3. The system saves the settings from the PXC/PXO to a file named "backup_settings.txt."

To restore the settings via SCP:

1. Type the following SCP command and press Enter.

```
scp backup_settings.txt <user name>@<device ip>:/settings_restore
```

   - *<user name>* is the "admin" or any user profile with Administrator Privileges
   - *<device ip>* is the IP address or hostname of the PXC/PXO 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 PXC/PXO, 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.

Raritan
A brand of legrand

Scenario 1: Use the default SCP port and default filename

- SSH/SCP port is the default (22), and the accessed PXC/PXO 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 PXC/PXO 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 PXC/PXO is a standalone device.
- Renaming the diagnostic file is wanted.

```
scp <user name>@<device ip>:/diag-data.zip <filename>
```

Scenario 4: Specify a different SCP port and a new filename

- SSH/SCP port is NOT the default (22), or the accessed PXC/PXO is a Port-Forwarding slave device.
- Renaming the diagnostic file is wanted.

```
scp -P <port> <user name>@<device ip>:/diag-data.zip <filename>
```

- *<user name>* is the "admin" or any user profile with Administrator Privileges or "Unrestricted View Privileges" privileges.
- *<device ip>* is the IP address or hostname of the PXC/PXO whose data you want to download.
- <port> is the current SSH/SCP port number, or the port number of a specific slave device in the Port-Forwarding chain.
- *<filename>* is the new filename of the downloaded file.

2. Type the password when prompted.
3. The system downloads the specified data from the PXC/PXO onto your computer.
   - If you do NOT specify a new filename in the command, such as Scenarios 1 or 2, the downloaded file's default name is "diag-data.zip."

- If you specify a new filename in the command, such as Scenarios 3 or 4, the downloaded file is renamed accordingly.

SCP example:

```
scp  admin@192.168.87.50:/diag-data.zip .
```

Windows PSCP command:

PSCP in Windows works in a similar way to the SCP.

- `pscp -P <port> <user name>@<device ip>:/diag-data.zip <filename>`

Uploading or Downloading Raw Configuration Data

You can download the raw configuration data of a specific PXC/PXO for review, backup or modification.

After modifying or creating any raw configuration data, you can upload it to a specific PXC/PXO for changing its configuration. The uploaded raw configuration file can contain only partial configuration keys that you want to modify. Other settings that are not contained in the uploaded file will remain unchanged.

Syntax of the raw configuration data is completely the same as the syntax in the config.txt file. See ***config.txt*** (on page 582).

Warning: Some configuration keys in the downloaded raw configuration are commented out, and those must NOT be part of the configuration that will be uploaded to any PXC/PXO. See *Keys that Cannot Be Uploaded* **(on page 567).**

To download raw configuration data:

1. Type one of the following SCP commands and press Enter.

Scenario 1: Use the default SCP port and default filename

- SSH/SCP port is the default (22), and the accessed PXC/PXO is a standalone device.
- The raw configuration file's default filename "raw_config.txt" is wanted. Then add a dot (.) in the end of the SCP command as shown below.

```
scp <user name>@<device ip>:/raw_config.txt .
```

Scenario 2: Specify a different SCP port but use the default filename

- SSH/SCP port is NOT the default (22), or the accessed PXC/PXO is a Port-Forwarding slave device.
- The raw configuration file's default filename "raw_config.txt" is wanted. Then add a dot in the end of the SCP command as shown below.

```
scp -P <port> <user name>@<device ip>:/raw_config.txt .
```


Raritan
A brand of legrand

Scenario 3: Specify a new filename but use the default SCP port

- SSH/SCP port is the default (22), and the accessed PXC/PXO is a standalone device.
- Renaming the raw configuration file is wanted.

```
scp <user name>@<device ip>:/raw_config.txt <filename>
```

Scenario 4: Specify a different SCP port and a new filename

- SSH/SCP port is NOT the default (22), or the accessed PXC/PXO is a Port-Forwarding slave device.
- Renaming the raw configuration file is wanted.

```
scp -P <port> <user name>@<device ip>:/raw_config.txt <filename>
```

- *<user name>* is the "admin" or any user profile with Administrator Privileges.
- *<device ip>* is the IP address or hostname of the PXC/PXO whose data you want to download.
- <port> is the current SSH/SCP port number, or the port number of a specific slave device in the Port-Forwarding chain.
- *<filename>* is the new filename of the downloaded file.

2. Type the password when prompted.
3. The system downloads the specified data from the PXC/PXO onto your computer.
   - If you do NOT specify a new filename in the command, such as Scenarios 1 or 2, the downloaded file's default name is "raw_config.txt."
   - If you specify a new filename in the command, such as Scenarios 3 or 4, the downloaded file is renamed accordingly.

To upload raw configuration data:

1. Type one of the following SCP commands and press Enter.

Scenario 1: Only one PXC/PXO to configure, with the default SCP port

- SSH/SCP port is the default (22), and the accessed PXC/PXO is a standalone device.
- There is only one device to configure so a CSV file for device-specific settings is NOT needed.

```
scp <config file> <user name>@<device ip>:/raw_config_update
```

Scenario 2: Only one PXC/PXO to configure, with a non-default SCP port

- SSH/SCP port is NOT the default (22), or the accessed PXC/PXO is a Port-Forwarding slave device.
- There is only one device to configure so a CSV file for device-specific settings is NOT needed.

```
scp -P <port> <config file> <user name>@<device ip>:/raw_config_update
```

Scenario 3: Multiple PXC/PXO to configure, with the default SCP port

- SSH/SCP port is the default (22), and the accessed PXC/PXO is a standalone device.
- There are multiple devices to configure so a CSV file for device-specific settings is needed during the upload.

```
scp <dev_list file> <config file> <user name>@<device
ip>:/raw_config_update /match=<col>
```

Scenario 4: Multiple PXC/PXO to configure, with a non-default SCP port

- SSH/SCP port is NOT the default (22), or the accessed PXC/PXO is a Port-Forwarding slave device.
- There are multiple devices to configure so a CSV file for device-specific settings is needed during the upload.

```
scp -P <port> <dev_list file> <config file> <user name>@<device
ip>:/raw_config_update /match=<dev_col>
```

- `<config file>` is the filename of the custom raw configuration that you want to upload.
- *<user name>* is the "admin" or any user profile with Administrator Privileges.
- <device ip> is the IP address or hostname of the PXC/PXO where you want to upload the specified file.
- <port> is the current SSH/SCP port number, or the port number of a specific slave device in the Port-Forwarding chain.
- `<dev_list file>` is the name of the CSV file for configuring multiple PXC/PXO with device-specific settings. For this file's format, see ***devices.csv*** (on page 585).
  - For device-specific settings in the `<config file>`, refer each device-specific configuration key to a specific column in the `<dev_list file>`. See ***config.txt*** (on page 582).
- `<dev_col>` comprises "serial:" or "mac:" and the number of the column where the serial number or MAC address of each PXC/PXO is in the uploaded CSV file. This is the data based on which each device finds its device-specific settings.

  For example:

Raritan
A brand of legrand

- If the second column contains each device's serial number, the parameter is then `serial:2`.
- If the seventh column contains each device's MAC address, the parameter is then `mac:7`.

SCP examples:

- Raw configuration download example --

```
scp  admin@192.168.87.50:/raw_config.txt config.txt
```

- Raw configuration upload example with the configuration file only --

```
scp  config.txt
admin@192.168.87.50:/raw_config_update
```

- Raw configuration upload example with both configuration and device list files --

```
scp  devices.csv config.txt
admin@192.168.87.50:/raw_config_update
/match=serial:2
```

Windows PSCP commands:

PSCP in Windows works in a similar way to the SCP.

- `pscp -P <port> <user name>@<device ip>:/raw_config.txt <filename>`
- `pscp -P <port> <CSV file> <config file> <user name>@<device ip>:/raw_config_update /match=<col>`

Alternative of bulk configuration via SCP:

Both methods of uploading 'bulk configuration' file or 'raw configuration' file via SCP can serve the purpose of bulk configuration. The only difference is that you can configure *device-specific* settings with the upload of raw configuration but not with the 'bulk configuration' file.

- ***Bulk Configuration via SCP*** (on page 560)

Keys that Cannot Be Uploaded

The raw configuration downloaded from any PXC/PXO contains a few configuration keys that are commented out with either syntax below.

Comment syntax	Description
#INTERNAL#	These keys are internal ones. They are NOT user configurable settings.
#OLD/INVALID#	These keys are old or invalid ones.

Note that these configuration keys cannot be part of the configuration that you will upload to any PXC/PXO. That is, they should be either not available or they remain to be commented out in the configuration file you will upload.

Raritan
A brand of legrand

Appendix A Specifications

In This Chapter

Maximum Ambient Operating Temperature 569
Serial RS-232 "RJ-45" Port Pinouts 569
Sensor RJ-45 Port Pinouts 569

Maximum Ambient Operating Temperature

The maximum ambient operating temperature (TMA) for PXC/PXO is 60 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.

Appendix B Equipment Setup Worksheet

PXC/PXO Series Model _____

PXC/PXO 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

Raritan
A brand of legrand

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

_____

Raritan
A brand of legrand

Appendix C 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 PXC/PXO.

- Configuration changes
- Firmware upgrade
- Diagnostic data download

Tip: You can also accomplish the same tasks via the TFTP server in a DHCP network. See **Bulk Configuration or Firmware Upgrade via DHCP/TFTP** *(on page 590).*

In This Chapter

Device Configuration/Upgrade Procedure 575
System and USB Requirements 576
Configuration Files 577
Firmware Upgrade via USB 588

Device Configuration/Upgrade Procedure

Any firmware **downgrade** using "fwupdate.cfg" is NOT supported by default. Only firmware upgrade is permitted with "fwupdate.cfg". A special parameter is required to permit firmware downgrade via "fwupdate.cfg". See ***fwupdate.cfg*** (on page 578).

Therefore, **firmware downgrade via USB** is disallowed by default.

You can use one USB drive to configure or upgrade multiple PXC/PXO devices one by one as long as it contains valid configuration files.

To use a USB drive to configure the PXC/PXO or upgrade firmware:

1. Verify that both the USB drive and your PXC/PXO meet the requirements. See ***System and USB Requirements*** (on page 576).
2. Prepare required configuration files. See ***Configuration Files*** (on page 577).
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 PXC/PXO.
5. The initial message shown on the front panel display depends on the first task performed by the PXC/PXO.

- If no firmware upgrade task will be performed, a happy smiley is displayed after around 30 seconds.

  The happy smiley looks like the following diagram and its background color will turn green.

- If the USB drive contains the firmware upgrade data, the PXC/PXO:

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 588).

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 PXC/PXO device for performing the same task(s) once the happy smiley or the firmware upgrade message displays.

7. Wait for several seconds until the PXC/PXO 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.

PXC/PXO system requirements:

- There is at least one USB-A port available on your Raritan device.
- Your PXC/PXO must run firmware version 3.6.0 or later.

  Note that the PXC/PXO 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 578).

Raritan
A brand of legrand

Configuration Files

There are three types of configuration files.

- **fwupdate.cfg:**

  This file MUST be always present for performing configuration or firmware upgrade tasks. See ***fwupdate.cfg*** (on page 578).

- **config.txt:**

  This file is used for configuring device settings. See ***config.txt*** (on page 582).

- **devices.csv:**

  This file is required only when there are device-specific settings to configure for multiple PXC/PXO devices. See ***devices.csv*** (on page 585).

Raritan provides a Mass Deployment Utility, which helps you quickly generate all configuration files for your PXC/PXO. See ***Creating Configuration Files via Mass Deployment Utility*** (on page 586).

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
set_password=newpassword
logfile=log.txt
config=config.txt
device_list=devices.csv
```

This section explains common options in the file.

Note: To make sure all of the following options work fine, you must update your PXC/PXO to the latest firmware version.

user

- A required option.
- Specify the name of a user account with Administrator Privileges.
- For PXC/PXO with factory default configuration, set this option to `admin`.

password

- A required option.
- Specify the password of the specified admin user.
- For PXC/PXO with factory default configuration, set this option to `raritan`.

Tip: You can add multiple user credentials to fwupdate.cfg. Each 'user' line must be immediately followed by its 'password' line. PXC/PXO will authenticate listed user credentials one by one until one of them succeeds, or until all user credentials fail.

Raritan
A brand of legrand

set_password

- **You are required to change the default password for all units. Access to units with factory default password settings will be denied unless this option is used.**
- Changes the password of the given user before executing any commands.

logfile

- Specify the name of a text file where the PXC/PXO will append the log messages when interpreting the USB drive contents.
- If the specified file does not exist in the USB drive, it will be automatically created.
- If this option is not set, no log messages are recorded. The disadvantage is that no feedback is available if the PXC/PXO detects a problem with the USB drive contents.

firmware

- Specify the name of a firmware binary file used to upgrade your PXC/PXO.
- The specified firmware file must be compatible with your PXC/PXO and have an official Raritan signature.
- If the specified firmware file is the same as the current firmware version of your PXC/PXO, no firmware upgrade is performed.
- The default is to NOT permit any firmware **downgrade** via USB drive on Raritan power products with "USB-A" port(s). To do this, the parameter "allow_downgrade" must be present and properly set in the *fwupdate.cfg* file.

config

- Specify the name of the configuration file containing device settings.
- The suggested filename is *config.txt*. See ***config.txt*** (on page 582).

device_list

- Specify the name of the configuration file listing all PXC/PXO devices to configure and their device-specific settings.
- This file is required if any macros are used in the device configuration file "config.txt."
- The suggested filename is *devices.csv*. See ***devices.csv*** (on page 585).

match

- Specify a match condition for identifying a line or one PXC/PXO 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 PXC/PXO to search for the MAC address in the 7th column of the "devices.csv" file.
- The default value is `serial:1`, making the PXC/PXO 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 PXC/PXO 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 PXC/PXO.

  Note: See **Bulk Configuration** *(on page 343) 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 PXC/PXO.

  Note: See **Backup and Restore of Device Settings** *(on page 349) 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 PXC/PXO is transmitted to the USB drive.
- The filename of the diagnostic data written into the USB drive is:

  diag_<unit-serial>.zip

Raritan
A brand of legrand

- The PXC/PXO device beeps after it finishes writing the diagnostic data to the USB drive.

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 PXC/PXO.
- 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 PXC/PXO.
- This option should be used with **tls_cert_file** listed above.
- *This option is NOT supported by bulk configuration or backup/restore via DHCP/TFTP.*

execute_lua_script

- Specify a Lua script file. For example:
  `execute_lua_script=my_script.lua`

- Script output will be recorded to a log file -- <BASENAME_OF_SCRIPT>.<SERIAL_NUMBER>.log. Note this log file's size is limited on DHCP/TFTP.
- A DHCP/TFTP-located script has a timeout of 60 seconds. After that duration the script will be removed.
- This feature can be used to manage LuaService, such as upload, start, get output, and so on.
- If you unplug the USB drive while the Lua script is still running, the script will be removed.
- An exit handler can be used but the execution time is limited to three seconds. Note that this is not implemented on DHCP/TFTP yet.

allow_downgrade

- This parameter is required for any firmware **downgrade** via *USB drive*, or the firmware upgrade via USB drive will fail.
- Add this parameter to this configuration file and set its value to *yes*.

Tip: Only firmware downgrade via USB is disabled by default. To downgrade firmware using other methods is still feasible by default, such as firmware downgrade via web interface.

config.txt

To perform device configuration using a USB drive, you must:

- Copy the device configuration file "config.txt" to the root directory of the USB drive.
- Reference the "config.txt" file in the *config* option of the "fwupdate.cfg" file. See ***fwupdate.cfg*** (on page 578).

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 PXC/PXO model.

You can use Raritan's Mass Deployment Utility to create this file by yourself, or contact Raritan to get a device configuration file specific to your PXC/PXO 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 587).*

Regular configuration key syntax:

- Each configuration key and value pair is in a single line as shown below:

```
key=value
```


Raritan
A brand of legrand

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 USB drive. See ***devices.csv*** (on page 585)
2. In the "config.txt" file, refer each device-specific configuration key to a specific column in the "devices.csv" file. The syntax is: `${column}`, where "column" is a column number.

   Examples:

```
net.interfaces[eth0].ipv4.static.addr_cidr.addr=${4
}
pdu.name=${16}
```

To rename the admin user:

You can rename the admin user by adding the following configuration key:

```
users[0].name=new admin name
```

Example:

```
users[0].name=May
```

To encrypt any settings:

You can encrypt the value of any setting in the config.txt. See ***Data Encryption in 'config.txt'*** (on page 587).

To restore a specific setting to factory default:

Add "delete:" to the beginning of the key whose setting you want to remove. The custom setting will be removed and then reset to factory default.

Example:

```
delete:net.port_forwarding
```

Tip:

You can also download "config.txt" from a specific PXC/PXO or upload it to a specific PXC/PXO from anywhere in the world via Internet. See ***Raw Configuration Upload and Download*** (on page 613).

Raritan
A brand of legrand

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 PXC/PXO device.

This file must be:

- A CSV (comma-separated values) format file exported from a spreadsheet application like Excel.
- Copied to the root directory of USB drive.
- Referenced in the *device_list* option of the "fwupdate.cfg" file. See ***fwupdate.cfg*** (on page 578).

Every PXC/PXO identifies its entry in the "devices.csv" file by comparing its serial number or MAC address to one of the columns in the file.

Determine the column to identify PXC/PXO devices:

- By default, the PXC/PXO searches for its serial number in the 1st column of "devices.csv".
- To override the default, set the *match* option in the "fwupdate.cfg" file to a different column.

Syntax:

- Values containing commas, line breaks or double quotes are all supported.
- The commas and line breaks to be included in the values must be enclosed in double quotes.
- Every double quote to be included in the value must be escaped with another double quote.

  For example:

```
Value-1,"Value-2,with,three,commas",Value-3

Value-1,"Value-2,""with""three""double-quotes",Valu
e-3

Value-1,"Value-2
with a line break", Value-3
```

Creating Configuration Files via Mass Deployment Utility

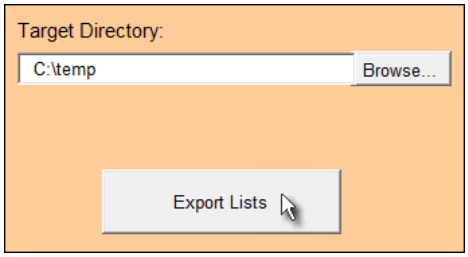
The Mass Deployment Utility is an Excel file that lets you fill in basic information required for the three configuration files, such as the admin account and password.

After entering required information, you can generate all configuration files with only one click, including *fwupdate.cfg*, *config.txt* and *devices.csv*.

To use the Mass Deployment Utility:

1. Download the Mass Deployment Utility from the Raritan website.
   - The utility is named *mass_deployment-xxx* (where xxx is the firmware version number).
   - It is available on the PXC/PXO product section of Raritan website's ***Support page*** (***http://www.raritan.com/support/***).
2. Launch Excel to open this utility.

   Note: Other office suites, such as OpenOffice and LibreOffice, are not supported.
3. Read the instructions in the 1st worksheet of the utility, and make sure Microsoft Excel's security level has been set to Medium or the equivalent for executing unsigned macros of this utility.
4. Enter information in the 2nd and 3rd worksheets.
   - The 2nd worksheet contains information required for *fwupdate.cfg* and *config.txt*.
   - The 3rd worksheet contains device-specific information for *devices.csv*.
5. Return to the 2nd worksheet to execute the export macro.
   a. In the Target Directory field, specify the folder where to generate the configuration files. For example, you can specify the root directory of a connected USB drive.
   b. Click Export Lists to generate configuration files.



Verify that at least 3 configuration files are created - *fwupdate.cfg*, *config.txt* and *devices.csv*. You are ready to configure or upgrade any PXC/PXO with these files.

See ***Configuration or Firmware Upgrade with a USB Drive*** (on page 575).

Raritan
A brand of legrand

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 PXC/PXO running firmware version 3.6.0 or later.

Data encryption procedure:

1. Open the "config.txt" file to determine which setting(s) to encrypt.
   - If an appropriate "config.txt" is not created yet, see ***Creating Configuration Files via Mass Deployment Utility*** (on page 586).
2. Launch a terminal to log in to the CLI of any PXC/PXO running version 3.6.0 or later. See ***Logging in to CLI*** (on page 387).
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 --

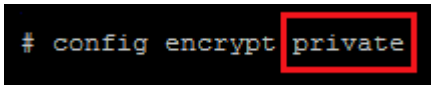
   ```
   # config encrypt "<value with spaces>"
   ```
4. Press Enter. The CLI generates and displays the encrypted form of the typed value.
5. Go to the "config.txt" file and replace the chosen value with the encrypted one by typing or copying the encrypted value from the CLI.
6. Add the text "encrypted:" 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 PXC/PXO running version 3.6.0 or later. See ***Configuration or Firmware Upgrade with a USB Drive*** (on page 575).

Illustration:

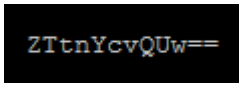
In this example, we will encrypt the word "private", which is the value of the SNMP write community in the "config.txt" file.

```
snmp.write_community=private
```

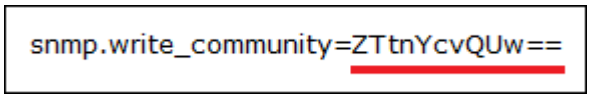
1. In the CLI, type the following command to encrypt "private."



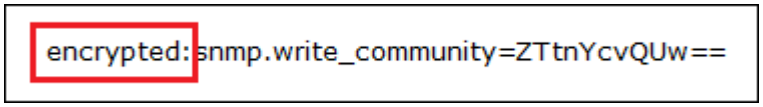
2. The CLI generates and shows the encrypted form of "private."



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.



   b. Add "encrypted:" to the beginning of that setting.



Firmware Upgrade via USB

Firmware files are available on Raritan website's ***Support page*** (***http://www.raritan.com/support/***).

Note that if the firmware file used for firmware upgrade is the same as the firmware version running on the PXC/PXO, 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 578).

To use a USB drive to upgrade the PXC/PXO:

1. Copy the configuration file "fwupdate.cfg" and an appropriate firmware file to the root directory of the USB drive.
2. Reference the firmware file in the *firmware* option of the "fwupdate.cfg" file.
3. Plug the USB drive into the USB-A port on the PXC/PXO.
4. The PXC/PXO 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 PXC/PXO 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.

Raritan
A brand of legrand

- **Sad smiley**: Failed. Check the log file in the USB drive or contact Raritan Technical Support to look into the failure cause.

Appendix D 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 PXC/PXO devices in the same network.

- Initial deployment
- Configuration changes
- Firmware upgrade
- Downloading diagnostic data

This feature is useful if you have hundreds or even thousands of PXC/PXO devices to configure or upgrade.

Warning: The feature of bulk configuration or firmware upgrade via DHCP/TFTP only works on standalone PXC/PXO devices directly connected to the network. This feature does NOT work for slave devices in the cascading configuration.

Tip: For the other alternatives, see **Configuration or Firmware Upgrade with a USB Drive** *(on page 575) or* **Raw Configuration Upload and Download** *(on page 613).*

In This Chapter

Bulk Configuration/Upgrade Procedure 591
TFTP Requirements.....592
DHCP IPv4 Configuration in Windows 592
DHCP IPv6 Configuration in Windows 602
DHCP IPv4 Configuration in Linux.....609
DHCP IPv6 Configuration in Linux.....611

Bulk Configuration/Upgrade Procedure

Any firmware **downgrade** using "fwupdate.cfg" is NOT supported by default. Only firmware upgrade is permitted with "fwupdate.cfg". A special parameter is required to permit firmware downgrade via "fwupdate.cfg". See ***fwupdate.cfg*** (on page 578).

Therefore, firmware "downgrade" via DHCP/TFTP is disallowed by default.

Steps of using DHCP/TFTP for bulk configuration/upgrade:

1. Create configuration files specific to your PXC/PXO models and firmware versions. See ***Configuration Files*** (on page 577) or contact Raritan Technical Support to properly prepare some or all of the following files:
   - *fwupdate.cfg (always required)*
   - *config.txt*
   - *devices.csv*

   Note: Supported syntax of "fwupdate.cfg" and "config.txt" may vary based on different firmware versions. If you have existing configuration files, it is suggested to double check with Raritan Technical Support for the correctness of these files prior to using this feature.
2. Configure your TFTP server properly. See ***TFTP Requirements*** (on page 592).
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 PXC/PXO.

   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 592)
   - ***DHCP IPv6 Configuration in Windows*** (on page 602)
   - ***DHCP IPv4 Configuration in Linux*** (on page 609)
   - ***DHCP IPv6 Configuration in Linux*** (on page 611)
5. Make sure all of the desired PXC/PXO devices use DHCP as the IP configuration method and have been *directly* connected to the network.
6. Re-boot these PXC/PXO devices. The DHCP server will execute the commands in the "fwupdate.cfg" file on the TFTP server to configure or upgrade those PXC/PXO devices supporting DHCP in the same network.

   DHCP will execute the "fwupdate.cfg" commands once for IPv4 and once for IPv6 respectively if both IPv4 and IPv6 settings are configured properly in DHCP.

TFTP Requirements

To perform bulk configuration or firmware upgrade successfully, your TFTP server must meet the following requirements:

- The server is able to work with both IPv4 and IPv6.

  In Linux, remove any IPv4 or IPv6 flags from */etc/xinetd.d/tftp*.

  Note: DHCP will execute the "fwupdate.cfg" commands once for IPv4 and once for IPv6 respectively if both IPv4 and IPv6 settings are configured properly in DHCP.

- All required configuration files are available in the TFTP root directory. See ***Bulk Configuration/Upgrade Procedure*** (on page 591).

If you are going to upload any PXC/PXO 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

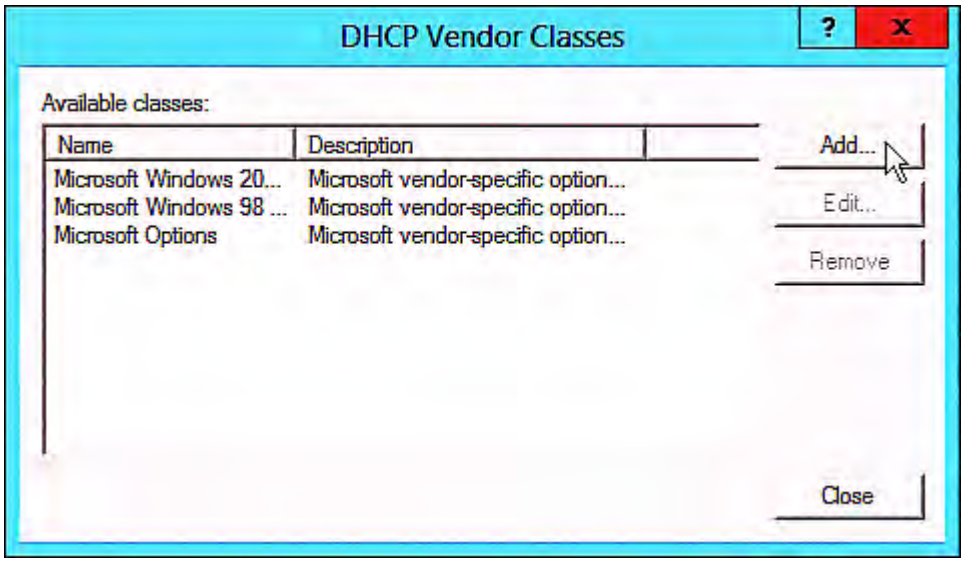
For those PXC/PXO devices using IPv4 addresses, follow this procedure to configure your DHCP server. The following illustration is based on Microsoft® Windows Server 2012 system.

Required Windows IPv4 settings in DHCP:

1. Add a new vendor class for PXC/PXO under IPv4.
   a. Right-click the IPv4 node in DHCP to select Define Vendor Classes.

Raritan
A brand of legrand

b. Click Add to add a new vendor class.



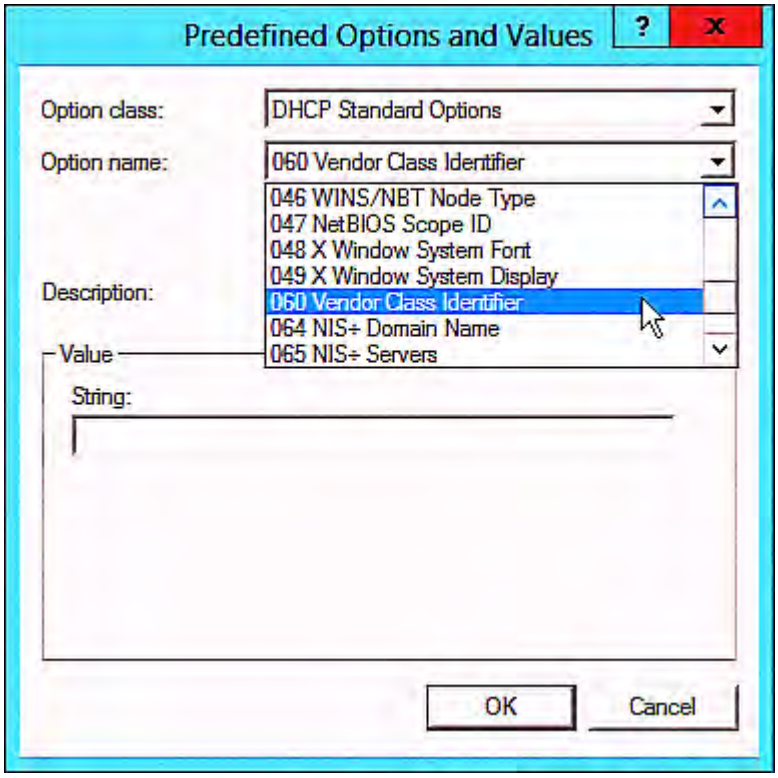
c. Specify a unique name for this vendor class and type the binary codes of "Raritan PDU 1.0" in the New Class dialog.

The vendor class is named "Raritan PDU" in this illustration.

2. Define one DHCP standard option - Vendor Class Identifier.

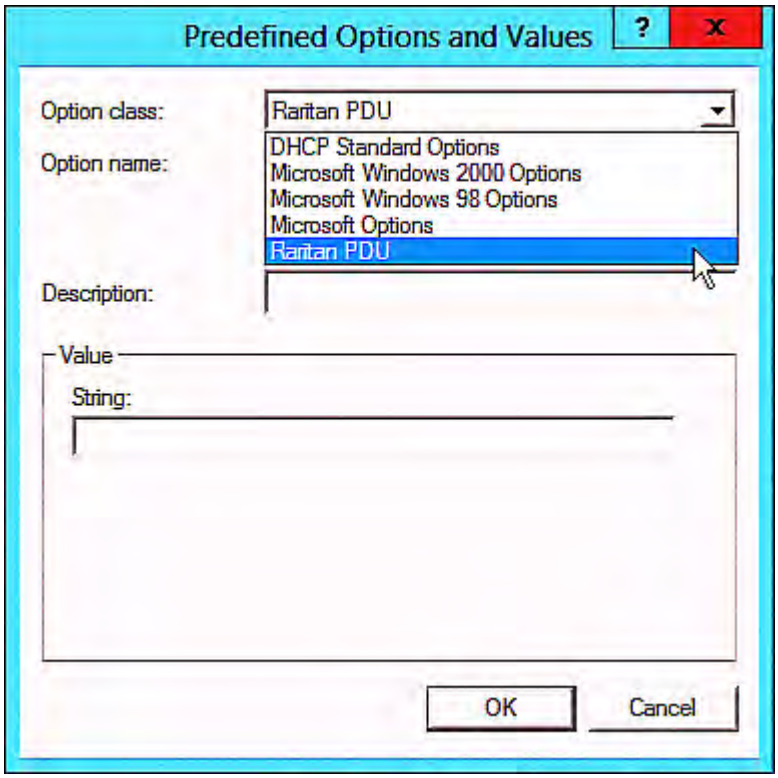
a. Right-click the IPv4 node in DHCP to select Set Predefined Options.

b. Select DHCP Standard Options in the "Option class" field, and Vendor Class Identifier in the "Option name" field. Leave the String field blank.

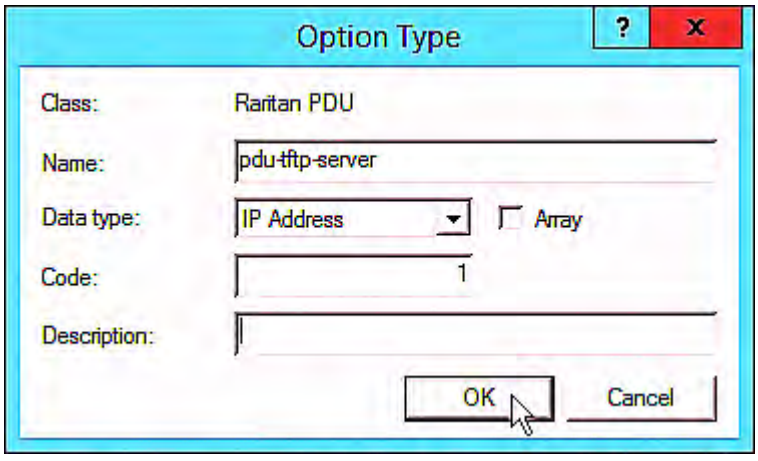


3. Add three options to the new vendor class "Raritan PDU" in the same dialog.

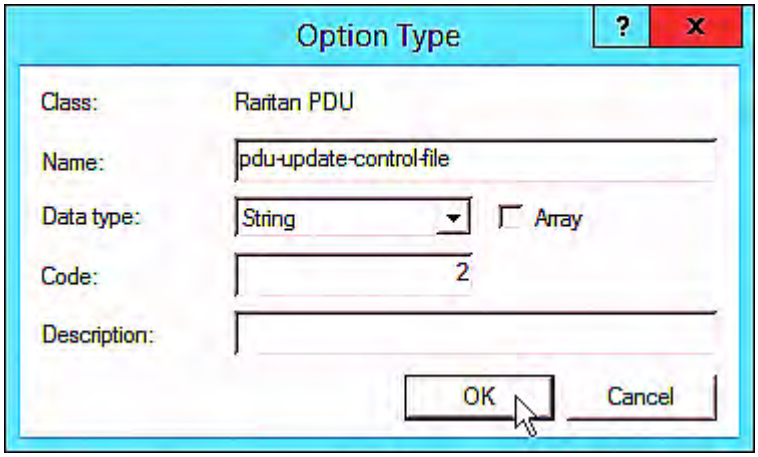
a. Select Raritan PDU in the "Option class" field.



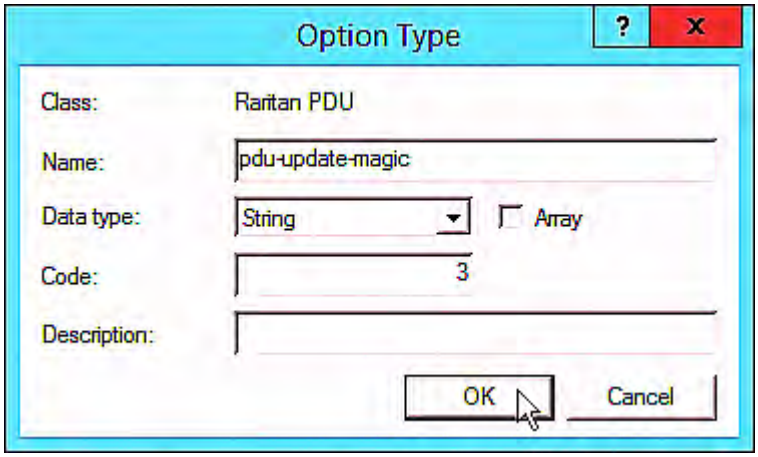
b. Click Add to add the first option. Type "pdu-tftp-server" in the Name field, select IP Address as the data type, and type 1 in the Code field.



c. Click Add to add the second option. Type "pdu-update-control-file" in the Name field, select String as the data type, and type 2 in the Code field.



d. Click Add to add the third one. Type "pdu-update-magic" in the Name field, select String as the data type, and type 3 in the Code field.

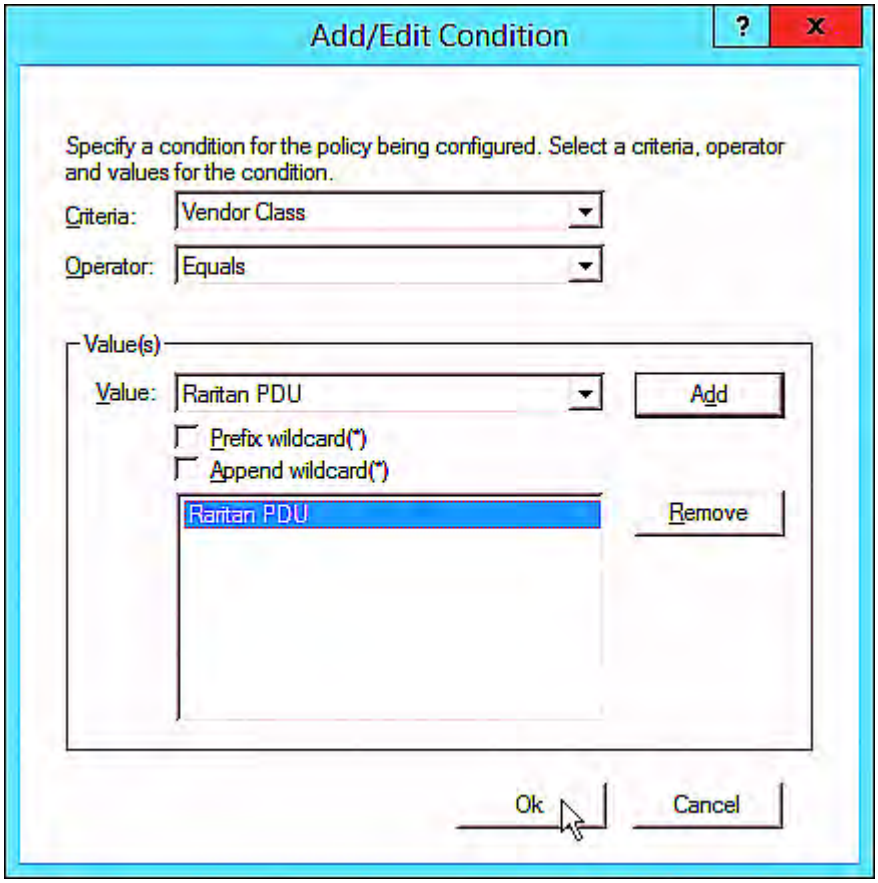


4. Create a new policy associated with the "Raritan PDU" vendor class.
   a. Right-click the Policies node under IPv4 to select New Policy.
   b. Specify a policy name, and click Next.

The policy is named "PDU" in this illustration.

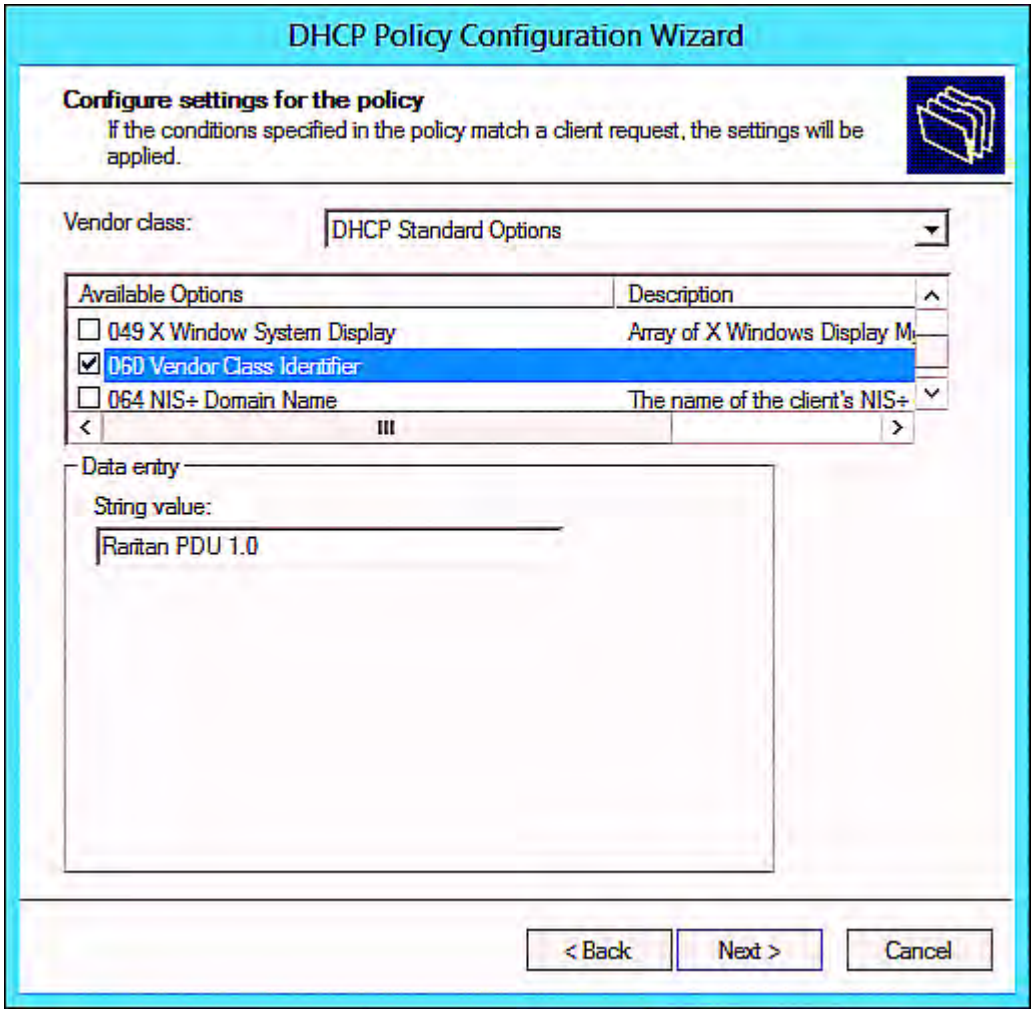
c. Click Add to add a new condition.

d. Select the vendor class "Raritan PDU" in the Value field, click Add and then Ok.

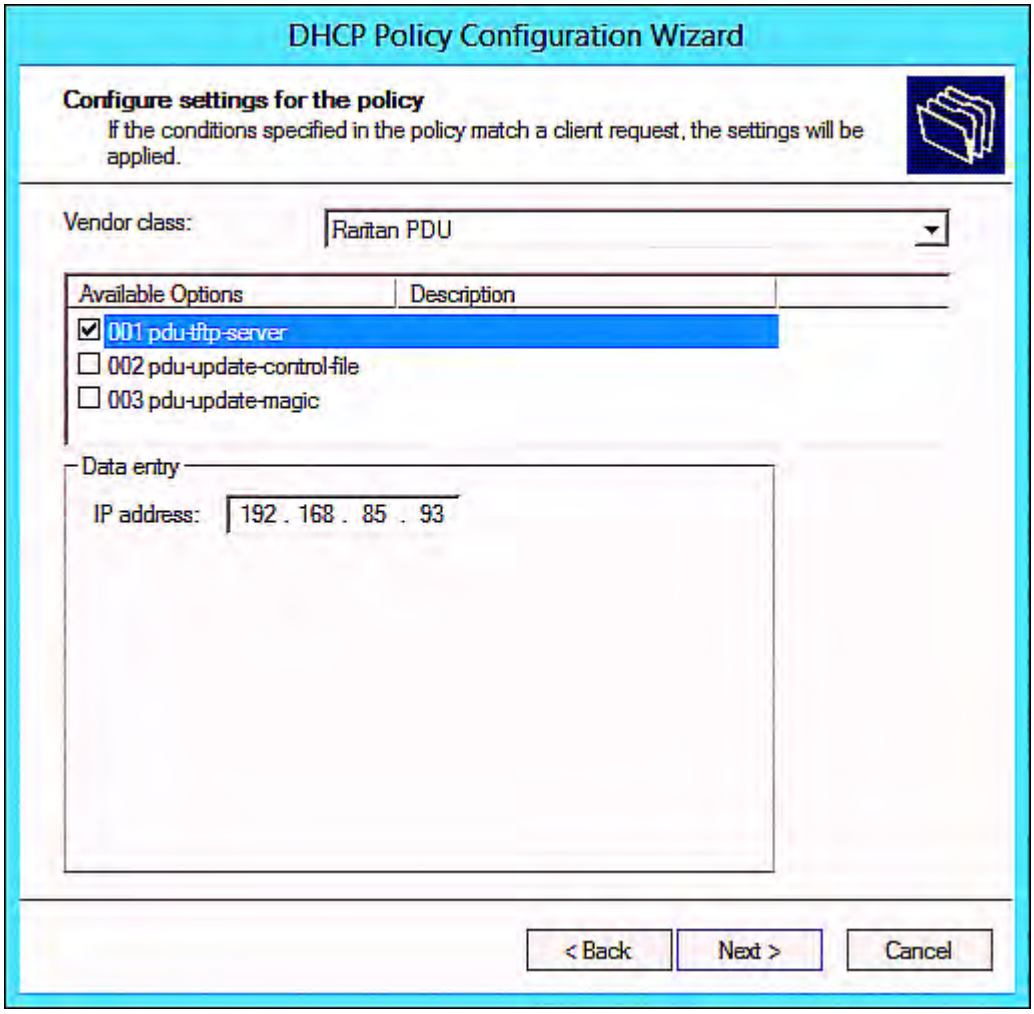


e. Click Next.

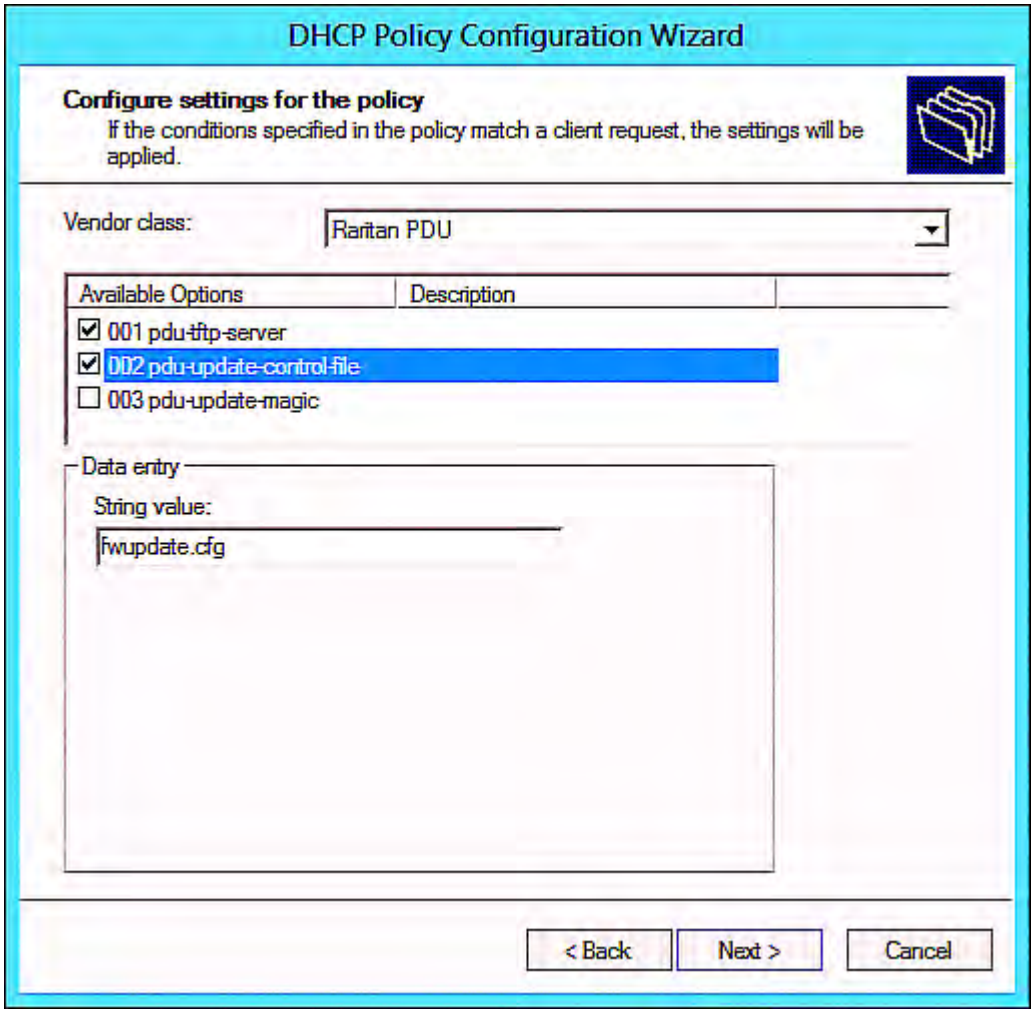
f. Select DHCP Standard Options in the "Vendor class" field, select "060 Vendor Class Identifier" from the Available Options list, and type "Raritan PDU 1.0" in the "String value" field.



g. Select the "Raritan PDU" in the "Vendor class" field, select "001 pdu-tftp-server" from the Available Options list, and type your TFTP server's IPv4 address in the "IP address" field.



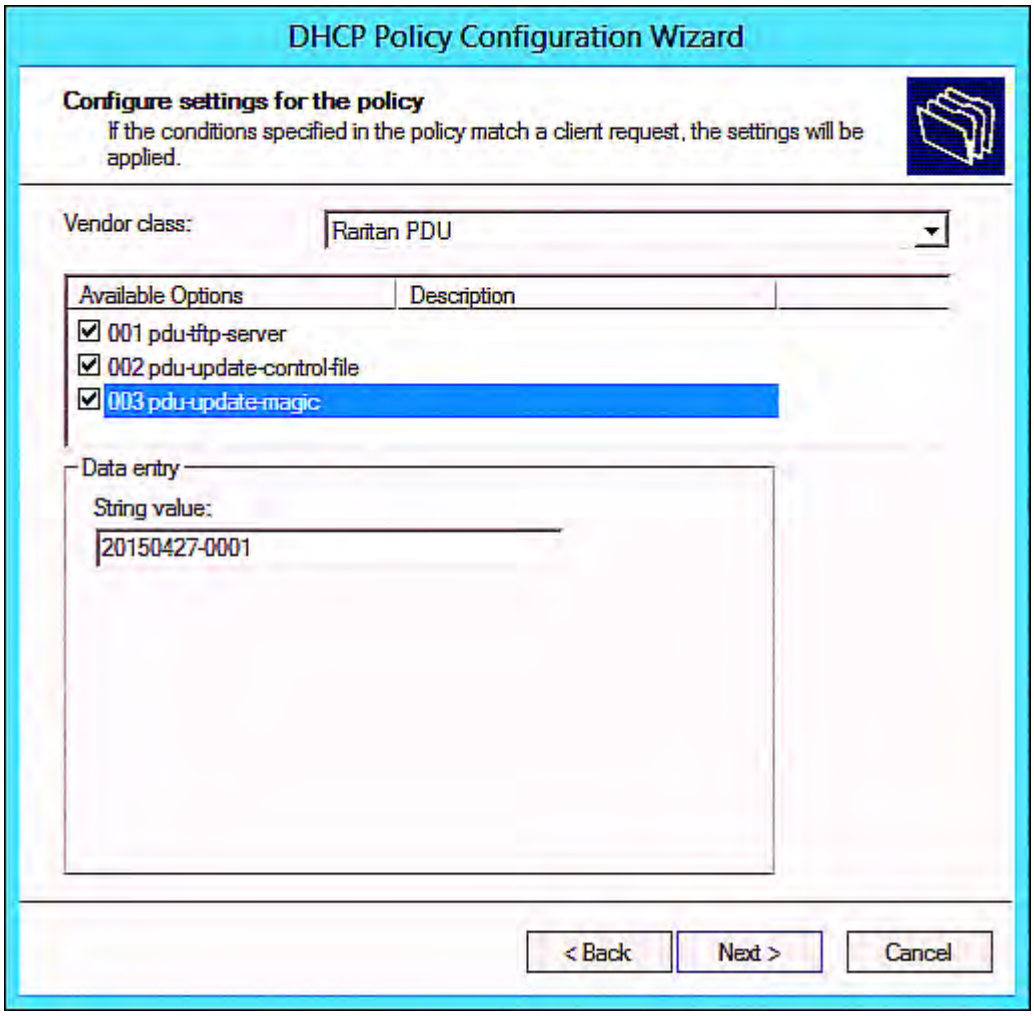
h. Select "002 pdu-update-control-file" from the Available Options list, and type the filename "fwupdate.cfg" in the "String value" field.



i. Select "003 pdu-update-magic" from the Available Options list, and type any string in the "String value" field. This third option/code is the magic cookie to prevent the *fwupdate.cfg* commands from being executed repeatedly. It does NOT matter whether the IPv4 magic cookie is identical to or different from the IPv6 magic cookie.

The magic cookie is a string comprising numerical and/or alphabetical digits in any format. In the following illustration diagram, it is a combination of a date and a serial number.

Important: The magic cookie is transmitted to and stored in PXC/PXO 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 PXC/PXO. 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

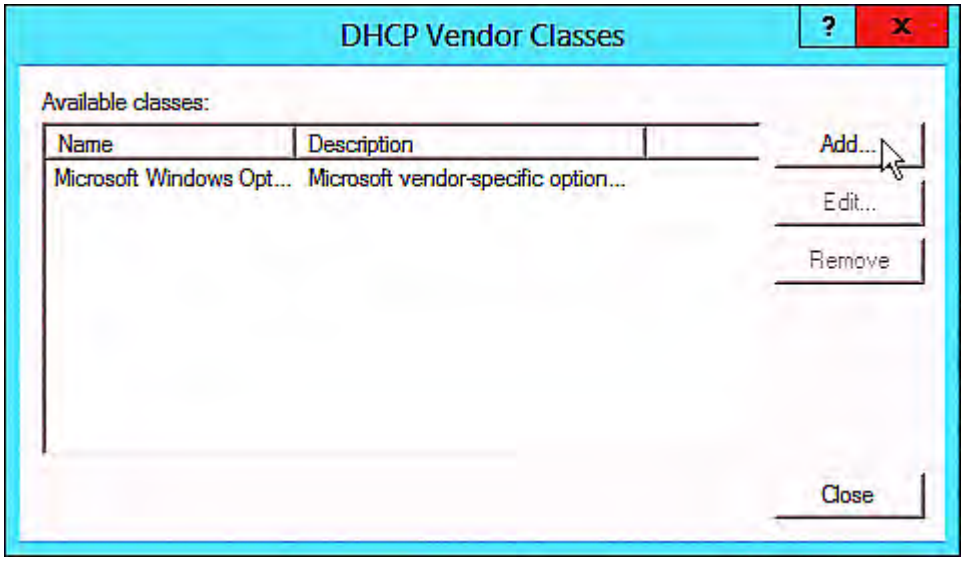
For those PXC/PXO devices using IPv6 addresses, follow this procedure to configure your DHCP server. The following illustration is based on Microsoft® Windows Server 2012 system.

Required Windows IPv6 settings in DHCP:

1. Add a new vendor class for PXC/PXO under IPv6.

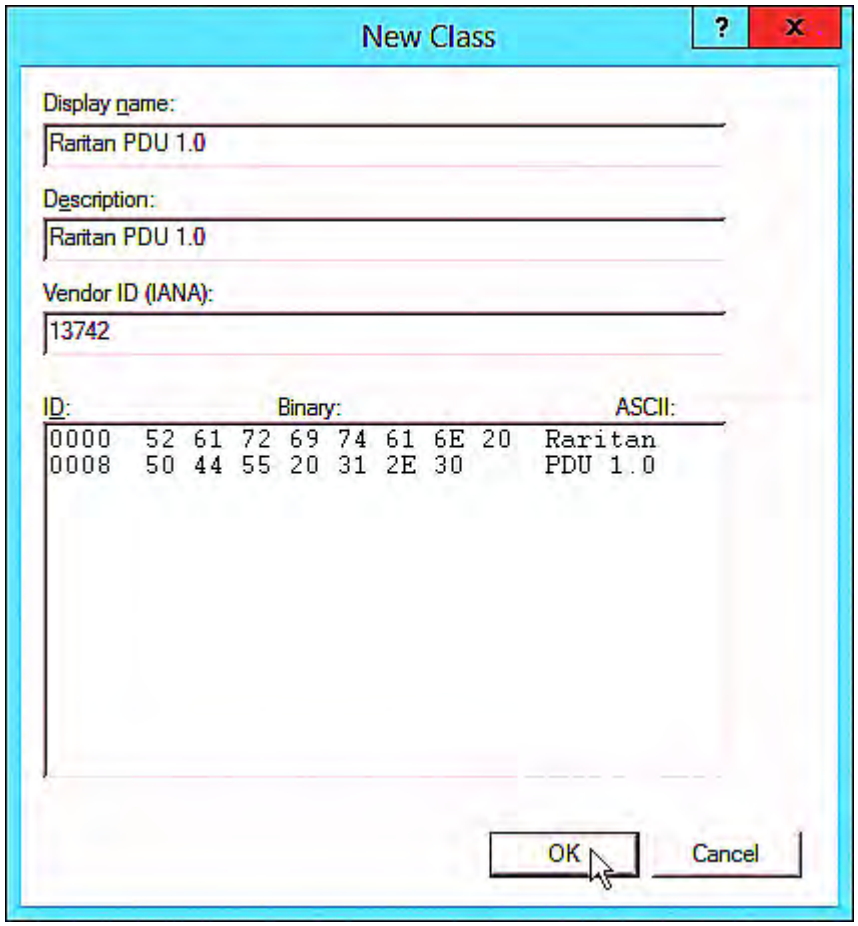
a. Right-click the IPv6 node in DHCP to select Define Vendor Classes.

b. Click Add to add a new vendor class.



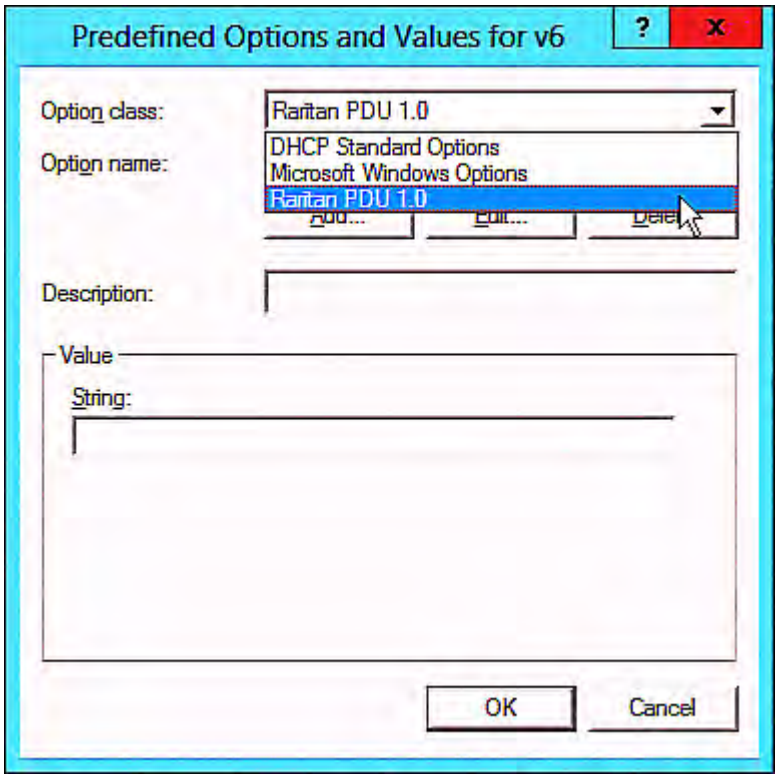
c. Specify a unique name for the vendor class, type "13742" in the "Vendor ID (IANA)" field, and type the binary codes of "Raritan PDU 1.0" in the New Class dialog.

The vendor class is named "Raritan PDU 1.0" in this illustration.

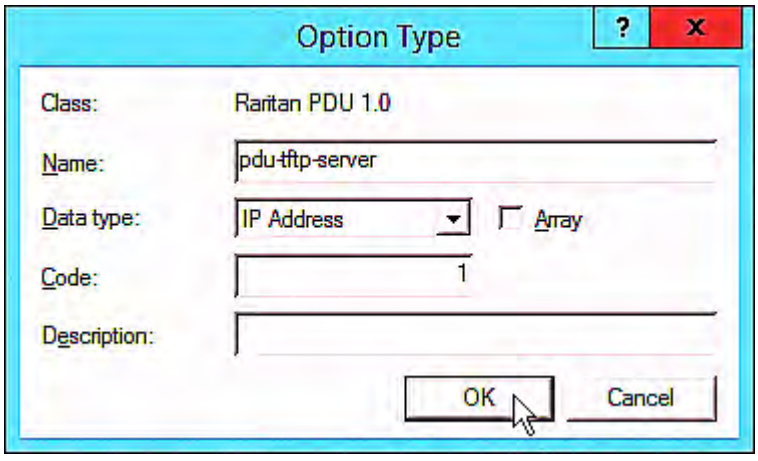


2. Add three options to the "Raritan PDU 1.0" vendor class.
   a. Right-click the IPv6 node in DHCP to select Set Predefined Options.

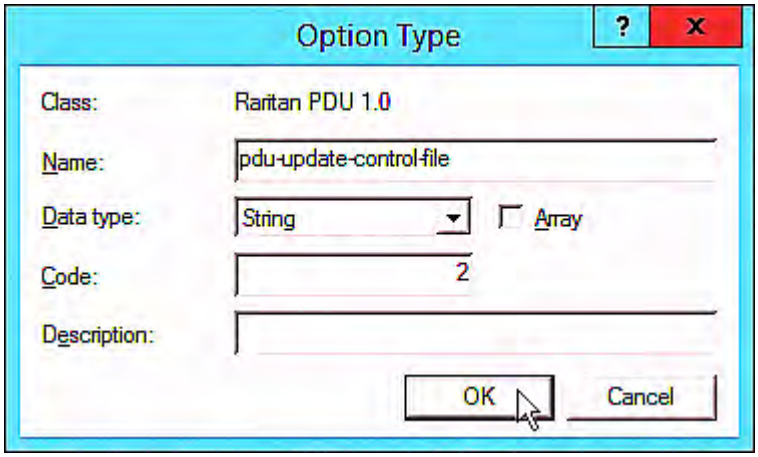
b. Select Raritan PDU 1.0 in the "Option class" field.



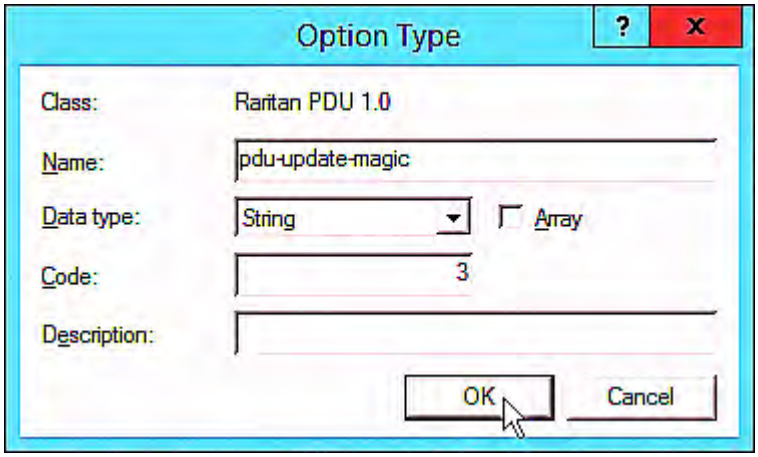
c. Click Add to add the first option. Type "pdu-tftp-server" in the Name field, select IP Address as the data type, and type 1 in the Code field.



d. Click Add to add the second option. Type "pdu-update-control-file" in the Name field, select String as the data type, and type 2 in the Code field.

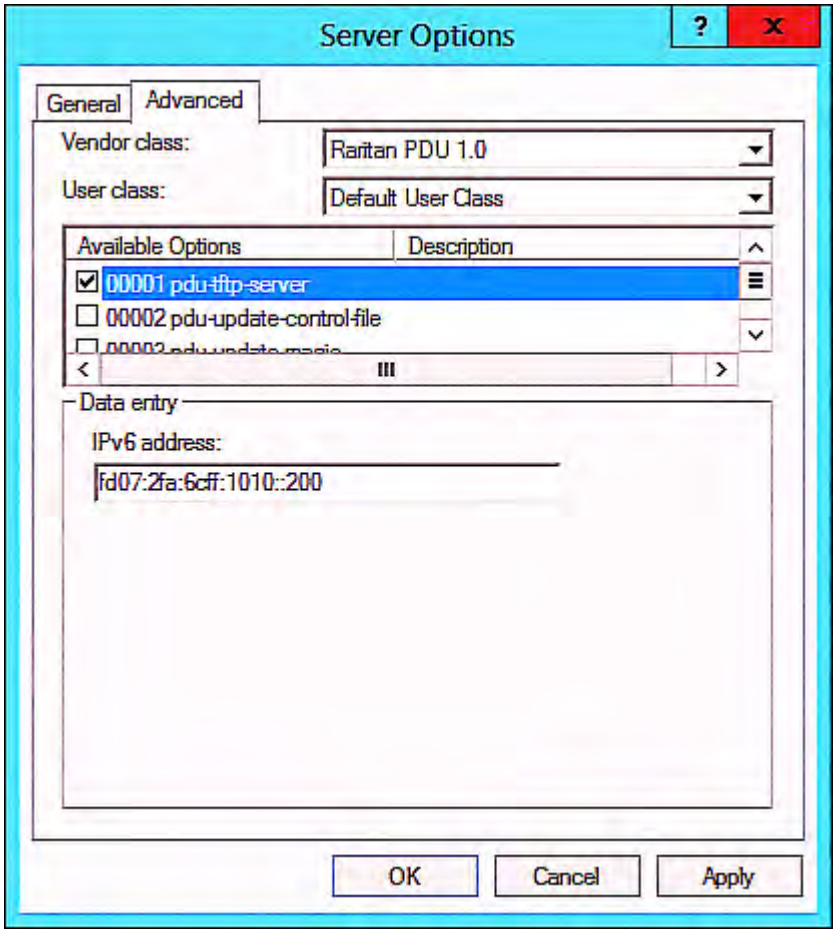


e. Click Add to add the third one. Type "pdu-update-magic" in the Name field, select String as the data type, and type 3 in the Code field.

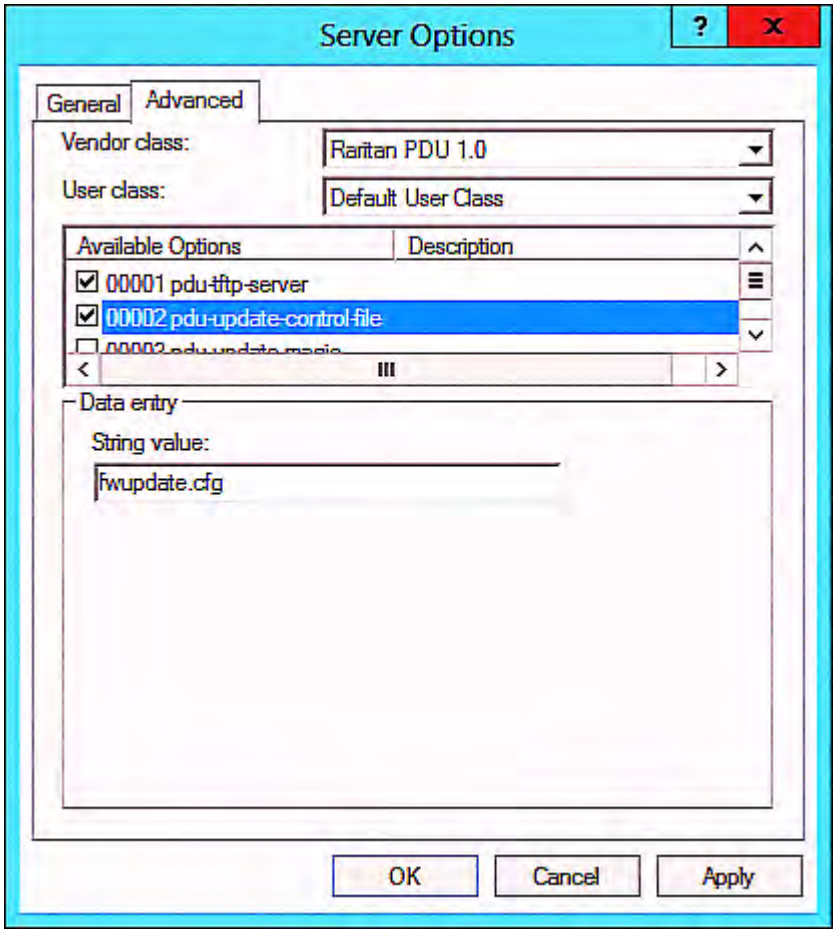


3. Configure server options associated with the "Raritan PDU 1.0" vendor class.
   a. Right-click the Server Options node under IPv6 to select Configure Options.
   b. Click the Advanced tab.

c. Select "Raritan PDU 1.0" in the "Vendor class" field, select "00001 pdu-tftp-server" from the Available Options list, and type your TFTP server's IPv6 address in the "IPv6 address" field.



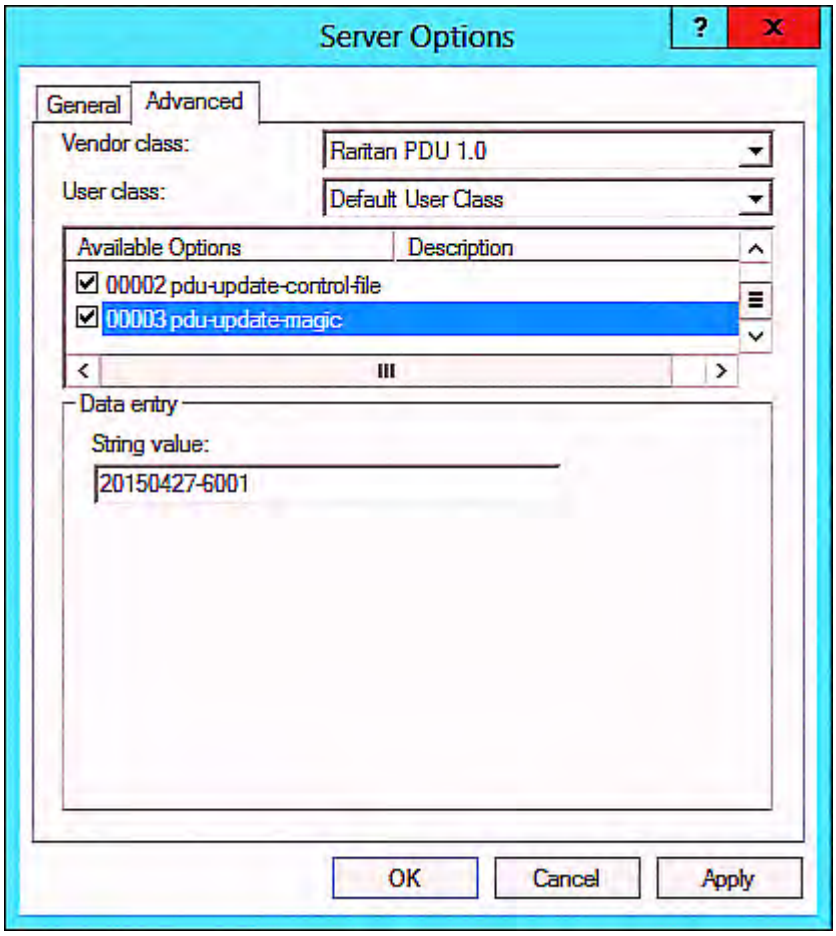
d. Select "00002 pdu-update-control-file" from the Available Options list, and type the filename "fwupdate.cfg" in the "String value" field.



e. Select "00003 pdu-update-magic" from the Available Options list, and type any string in the "String value" field. This third option/code is the magic cookie to prevent the *fwupdate.cfg* commands from being executed repeatedly. It does NOT matter whether the IPv6 magic cookie is identical to or different from the IPv4 magic cookie.

The magic cookie is a string comprising numerical and/or alphabetical digits in any format. In the following illustration diagram, it is a combination of a date and a serial number.

Important: The magic cookie is transmitted to and stored in PXC/PXO 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 PXC/PXO. 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 PXC/PXO 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 PXC/PXO 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 PXC/PXO 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 PXC/PXO. Therefore, you must modify the magic cookie's value in DHCP when intending to execute the "fwupdate.cfg" commands next time.

Raritan
A brand of legrand

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 PXC/PXO 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 PXC/PXO 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 PXC/PXO. Therefore, you must modify the magic cookie's value in DHCP when intending to execute the "fwupdate.cfg" commands next time.

IPv6 illustration example in dhcpd6.conf:

```
[...]

option space RARITAN code width 2 length width 2 hash size 3;
option RARITAN.pdu-tftp-server code 1 = ip6-address;
option RARITAN.pdu-update-control-file code 2 = text;
option RARITAN.pdu-update-magic code 3 = text;
option vsio.RARITAN code 13742 = encapsulate RARITAN;

[...]

subnet6 xxxx {

[...]
        option RARITAN.pdu-tftp-server 1::2;
        option RARITAN.pdu-update-control-file "fwupdate.cfg";
        option RARITAN.pdu-update-magic "20150123-0001";
[...]

}
```

Appendix E Raw Configuration Upload and Download

You can modify any existing "config.txt", and then upload it to a specific PXC/PXO for modifying part or all of its settings.

There are two ways to get one "config.txt":

- You create this file by yourself, either using or not using the Mass Deployment Utility. See ***Configuration Files*** (on page 577) and ***config.txt*** (on page 582).
- You download the raw configuration data from any PXC/PXO.

The downloaded raw configuration contains "almost" all of current settings on your PXC/PXO.

Warning: Some configuration keys in the downloaded raw configuration are commented out, and those must NOT be part of the configuration that will be uploaded to any PXC/PXO. See ***Keys that Cannot Be Uploaded*** (on page 567).

Both configuration download and upload operations require the Administrator Privileges.

In This Chapter

Downloading Raw Configuration 613
Uploading Raw Configuration 615

Downloading Raw Configuration

There are three download methods:

- *Web browsers:* See ***Download via Web Browsers*** (on page 613).
- *SCP or PSCP command:* See ***Uploading or Downloading Raw Configuration Data*** (on page 564).
- *CURL command:* See ***Download via Curl*** (on page 614).

Download via Web Browsers

There are two scenarios by using web browsers.

URL containing login credentials:

To log in immediately while issuing the download request, type an URL containing the login credentials in the web browser.

```
http(s)://<user>:<password>@<device IP>/cgi-bin/raw_config_download.cgi
```

Parameter	Description
<user>	Any user name that has the Administrator Privileges.
<password>	The password of the specified user name.
<device IP>	Hostname or IP address of the PXC/PXO whose raw configuration you want to download.

- For example:

```
https://admin:raritan@192.168.84.114/cgi-bin/raw_config_download.cgi
```

URL without login credentials contained:

If you would like to log in after issuing the download request, type an URL without login credentials contained in the web browser. The system will then prompt you to enter the login credentials.

```
http(s)://<device IP>/cgi-bin/raw_config_download.cgi
```

- For example:

```
https://192.168.84.114/cgi-bin/raw_config_download.cgi
```

Download via Curl

If you have installed curl on your computer, you can download the raw configuration from your PXC/PXO by performing the curl command.

To download raw configuration from PXC/PXO via curl:

1. Type the following curl command in the command line interface.

```
curl -k https://<user>:<password>@<device
IP>/cgi-bin/raw_config_download.cgi > config.txt
```

Parameter	Description
<user>	Any user name that has the Administrator Privileges.

Raritan
A brand of legrand

Parameter	Description
<password>	The password of the specified user name.
<device IP>	Hostname or IP address of the PXC/PXO whose raw configuration you want to download.

2. When the download is complete, a line indicates 100 in the first % column.

3. Go to the directory where you perform the curl command to find the "config.txt" file.

Tip: In the above curl command, you can replace the filename "config.txt" with any filename you prefer.

Example:

```
curl -k https://admin:raritan@192.168.84.114/cgi-bin/raw_config_download.cgi > config.txt
```

Uploading Raw Configuration

There are two upload methods:

- *SCP or PSCP command:* See ***Uploading or Downloading Raw Configuration Data*** (on page 564).
- *CURL command:* See ***Upload via Curl*** (on page 616).

The uploaded raw configuration file can contain only partial configuration keys that you want to modify. Other settings that are not contained in the uploaded file will remain unchanged.

Authentication-related data or HTTP(S) port may be no longer the same after uploading raw configuration. Therefore, it is suggested to **double check** what configuration keys will be changed in the raw configuration file that you will upload.

Upload via Curl

If curl is available on your computer, you can upload the raw configuration to PXC/PXO with the curl command.

There are two scenarios with the curl upload methods.

- When there are NO device-specific settings involved, you upload the configuration file only, regardless of the number of PXC/PXO devices to update.
- When there are device-specific settings involved for updating more than one PXC/PXO devices, you must upload two files. including one configuration file and one device list file.

To upload one configuration file only:

1. Type the following curl command in the command line interface.

```
curl -k -F "config_file=@<config file>" https://<user>:<password>@<device IP>/cgi-bin/raw_config_update.cgi
```

Parameter	Description
<user>	Any user name that has the Administrator Privileges.
<password>	The password of the specified user name.
<device IP>	Hostname or IP address of the PXC/PXO whose raw configuration you want to upload.
<config file>	Filename of the configuration file. ▪ For the syntax, see ***config.txt*** (on page 582).

2. When the upload is completed successfully, the curl returns the code 0 (zero).

Note: If the upload fails and curl returns other codes, see **Curl Upload Return Codes** *(on page 617).*

3. After several seconds, PXC/PXO reboots automatically. Changed settings take effect after the reboot process finishes.

To upload both configuration and device list files:

1. Type the following curl command in the command line interface.

```
curl -k -F "config_file=@<config file>" -F "device_list_file=@<dev_list file>" https://<user>:<password>@<device IP>/cgi-bin/raw_config_update.cgi?match=<dev_col>
```


Raritan
A brand of legrand

Parameter	Description
<user>, <password>, <device IP>, <config file>	Refer to the above table for explanation. ▪ For device-specific settings in the <config file>, refer each device-specific configuration key to a specific column in the <dev_list file>. See ***config.txt*** (on page 582).
<dev_list file>	Filename of the device list file in CSV format. ▪ For the content format, see ***devices.csv*** (on page 585).
<dev_col>	<dev_col> comprises "serial:" or "mac:" and the number of the column where the serial number or MAC address of each PXC/PXO is in the uploaded CSV file. This is the data based on which each device finds its device-specific settings. For example: ▪ If the second column contains each device's serial number, the parameter is then serial:2. ▪ If the seventh column contains each device's MAC address, the parameter is then mac:7.

2. PXC/PXO will reboot after Curl shows the return code 0. For details, refer to above steps 2 to 3.

Examples:

- Upload of the configuration file only:

```
curl -k -F "config_file=@config.txt"
https://admin:raritan@192.168.84.114/cgi-bin/raw_config_download.cgi
```

- Upload of both configuration and device list files:

```
curl -k -F "config_file=@config.txt" -F "device_list_file=@devices.csv"
https://admin:raritan@192.168.84.114/cgi-bin/raw_config_download.cgi
```

Curl Upload Return Codes

After performing raw configuration ***Upload via Curl*** (on page 616), curl will return a code to indicate the result of the file upload.

Code	Description
0	Operation was successful.

Code	Description
1	An internal error occurred.
2	A parameter error occurred.
3	A raw configuration update operation is already running.
4	The file is too large.
5	Invalid raw configuration file provided.
6	Invalid device list file or match provided.
7	Device list file required but missing.
8	No matching entry in device list found.
9	Macro substitution error.
10	Decrypting value failed.
11	Unknown magic line.
12	Processing magic line failed.

Appendix F Resetting to Factory Defaults

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

Resetting to factory defaults will reset the admin password to default.

Important: Exercise caution before resetting the PXC/PXO 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 354).

In This Chapter

Using the Reset Button 619
Using the CLI Command 620

Using the Reset Button

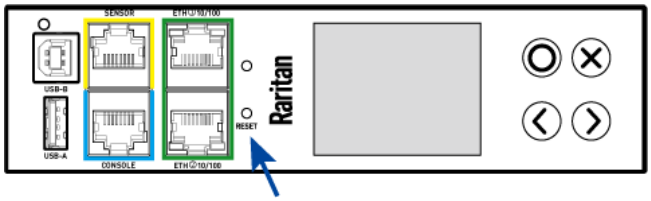
An RS-232 serial connection to a computer is required for using the reset button.

To reset to factory defaults using the reset button:

1. Connect a computer to the PXC/PXO. See ***Connecting the PXC/PXO to a Computer*** (on page 21).
2. Launch a terminal emulation program such as Kermit or PuTTY, and open a window on the PXC/PXO. For information on the serial port configuration, see Step 2 of ***Initial Network Configuration via CLI*** (on page 694).

   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 PXC/PXO 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 PXC/PXO to its factory defaults.
5. Wait until the reset is complete.

This diagram illustrates the reset button on Zero U PXC models so it may look slightly different from your PDU model's front panel.



Using the CLI Command

The Command Line Interface (CLI) provides a reset command for restoring the PXC/PXO to factory defaults. For information on CLI, see ***Using the Command Line Interface*** (on page 386).

To reset to factory defaults after logging in to the CLI:

1. Connect to the PXC/PXO. See ***Logging in to CLI*** (on page 387) or ***Connecting the PXC/PXO to a Computer*** (on page 21).
2. Launch a terminal emulation program such as HyperTerminal, Kermit, or PuTTY, and open a window on the PXC/PXO. For information on the serial port configuration, see Step 2 of ***Initial Network Configuration via CLI*** (on page 694).
3. Log in to the CLI by typing the user name "admin" and its password.
4. After the # system prompt appears, type either of the following commands and press Enter.

   ```
   #      reset factorydefaults
   ```

   -- OR --

   ```
   #      reset factorydefaults /y
   ```

5. If you entered the command without "`/y`" in Step 4, a message appears prompting you to confirm the operation. Type y to confirm the reset.
6. Wait until the reset is complete.

To reset to factory defaults without logging in to the CLI:

The PXC/PXO provides an easier way to reset the product to factory defaults in the CLI prior to login.

1. Connect to the PXC/PXO 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.

Raritan
A brand of legrand

Appendix G 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 PXC/PXO
b. Create user groups for the PXC/PXO on the AD server
c. Configure LDAP authentication on the PXC/PXO
d. Configure roles on the PXC/PXO

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

In This Chapter

Step A. Determine User Accounts and Roles 621
Step B. Configure User Groups on the AD Server 622
Step C. Configure LDAP Authentication on the PXC/PXO 623
Step D. Configure Roles on the PXC/PXO 626

Step A. Determine User Accounts and Roles

Determine the user accounts and roles (groups) that are authenticated for accessing the PXC/PXO. 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 PXC/PXO on the AD server, and then make appropriate users members of these groups.

In this illustration, we assume:

- The groups (roles) for the PXC/PXO 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.

Raritan
A brand of legrand

Step C. Configure LDAP Authentication on the PXC/PXO

You must enable and set up LDAP authentication properly on the PXC/PXO to use external authentication.

In the illustration, we assume:

- The DNS server settings have been configured properly. See ***Wired Network Settings*** (on page 191) and ***Role of a DNS Server*** (on page 688).
- 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.

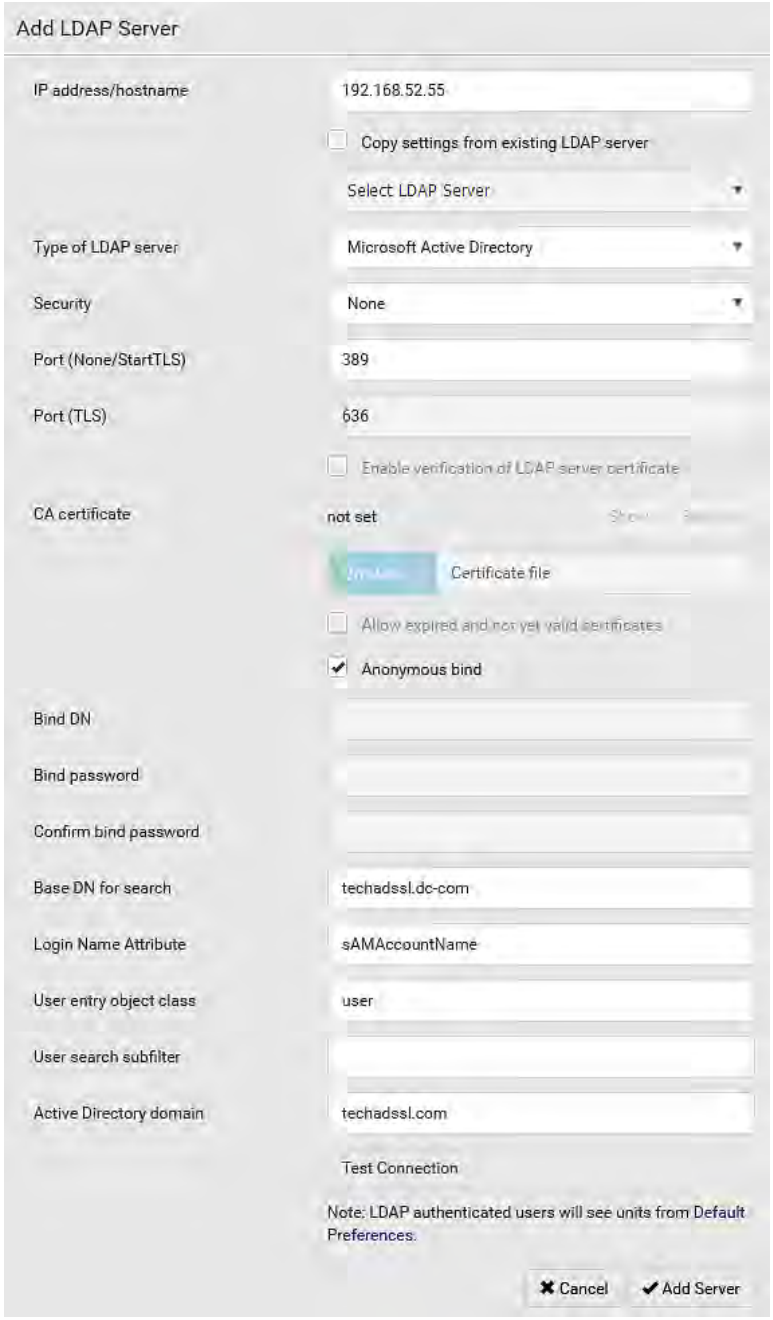
To configure LDAP authentication:

1. Choose Device Settings > Security > Authentication.
2. In the LDAP Servers section, click New to add an LDAP/LDAPS server.
3. Provide the PXC/PXO with the information about the AD server.

Field/setting	Do this...
IP address / hostname	Type the domain name `techadssl.com` or IP address `192.168.56.3`. ▪ Without the encryption enabled, you can type either the domain name or IP address in this field, but you must type the fully qualified domain name if the encryption is enabled.
Copy settings from existing LDAP server	Leave the checkbox deselected unless the new LDAP server's settings are similar to any existing LDAP settings.
Type of LDAP server	Select "Microsoft Active Directory."
Security	Select "None" since the TLS encryption is not applied in this example.
Port (None/StartTLS)	Ensure the field is set to `389`.
Port (TLS), CA certificate	Skip the two fields since the TLS encryption is not enabled.
Anonymous bind	Select this checkbox because anonymous bind is used.
Bind DN, Bind password, Confirm bind password	Skip the three fields because of anonymous bind.
Base DN for search	Type `dc=techadssl,dc=com` as the starting point where your search begins on the AD server.

Field/setting	Do this...
Login Name Attribute	Ensure the field is set to `sAMAccountName` because the LDAP server is Microsoft Active Directory.
User entry object class	Ensure the field is set to `user` because the LDAP server is Microsoft Active Directory.
User search subfilter	The field is optional. The subfilter information is also useful for filtering out additional objects in a large directory structure. In this example, we leave it blank.
Active Directory domain	Type `techadssl.com`.

Raritan
A brand of legrand



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 PXC/PXO 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 PXC/PXO and the LDAP server to use the same NTP server(s).

Step D. Configure Roles on the PXC/PXO

A role on the PXC/PXO determines the system and outlet permissions. You must create the roles whose names are identical to the user groups created for the PXC/PXO 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:

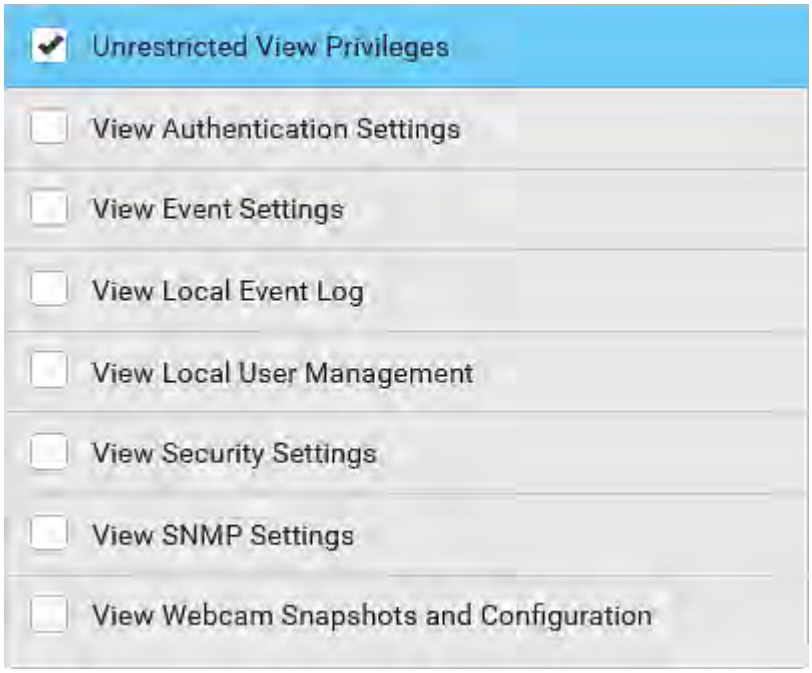
- Users assigned to the *PX_User* role can view settings only, but they can neither configure PXC/PXO nor access the outlets.
- Users assigned to the *PX_Admin* role have the Administrator Privileges so they can both configure PXC/PXO and access the outlets.

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.

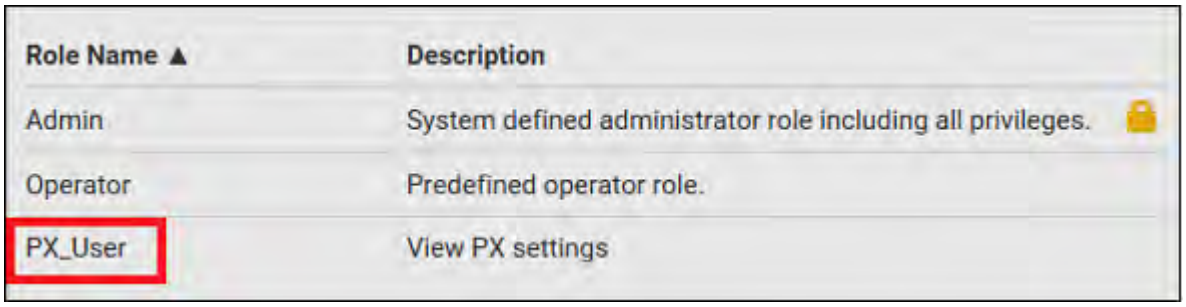
Raritan
A brand of legrand

c. In the Privileges list, select Unrestricted View Privileges, which includes all View permissions. The Unrestricted View Privileges permission lets users view all settings without the capability to configure or change them.



d. Click Save.

3. The PX_User role is created.

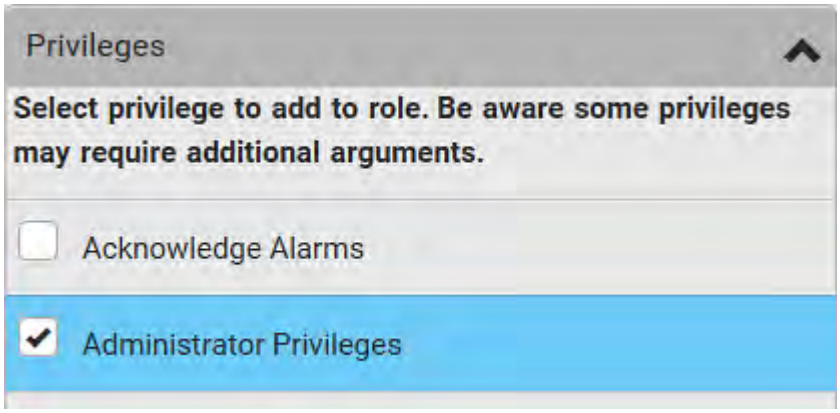


4. Keep the Roles page open to create the PX_Admin role.

To create the PX_Admin role with full permissions assigned:

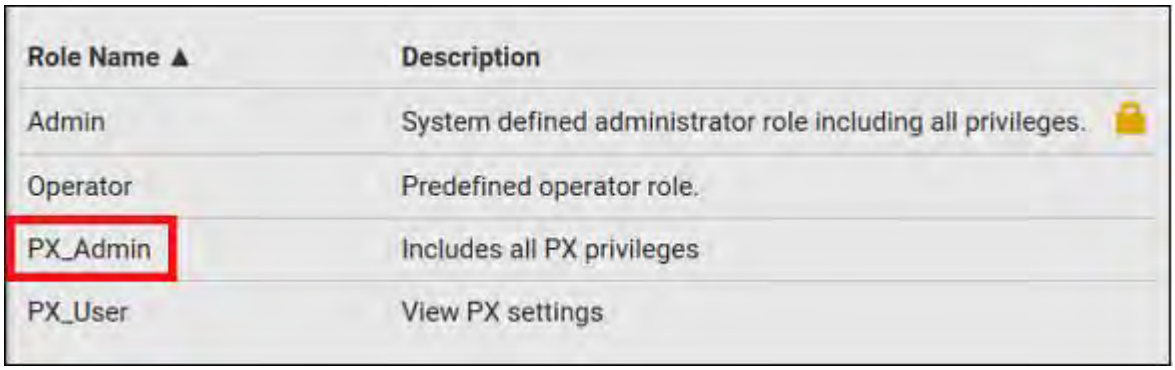
1. Click to add another role.
   a. Type PX_Admin in the Role Name field.
   b. Type a description for the PX_Admin role in the Description field. In this example, we type "Includes all PX privileges" to describe the role.

c. In the Privileges list, select Administrator Privileges. The Administrator Privileges allows users to configure or change all PXC/PXO settings.



d. Click Save.

2. The PX_Admin role is created.



Appendix H Updating the LDAP Schema

In This Chapter

Returning User Group Information....629
Setting the Registry to Permit Write Operations to the Schema 630
Creating a New Attribute....630
Adding Attributes to the Class....631
Updating the Schema Cache....633
Editing rciusergroup Attributes for User Members....633

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 PXC/PXO 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.

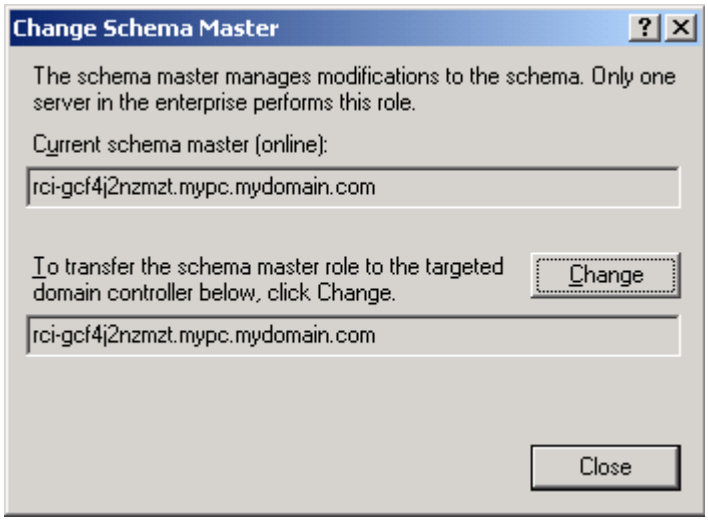
1. Install the schema plug-in for Active Directory. See Microsoft Active Directory documentation for instructions.
2. Run Active Directory Console and select Active Directory Schema.

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.

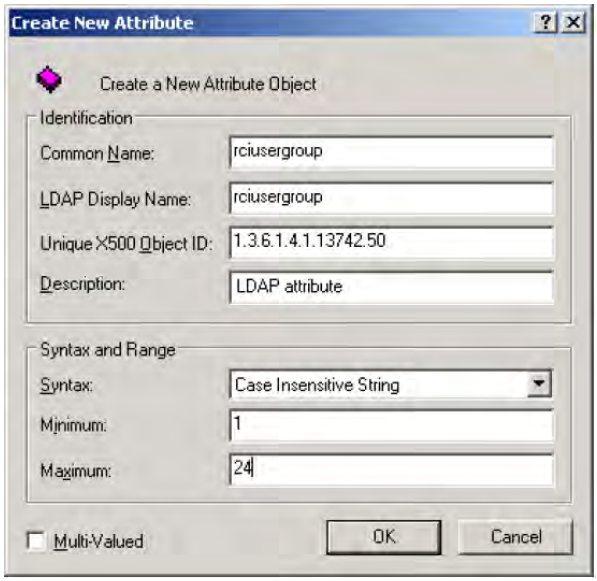
Creating a New Attribute

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.

Raritan
A brand of legrand

3. Click New and then choose Attribute. When the warning message appears, click Continue and the Create New Attribute dialog appears.



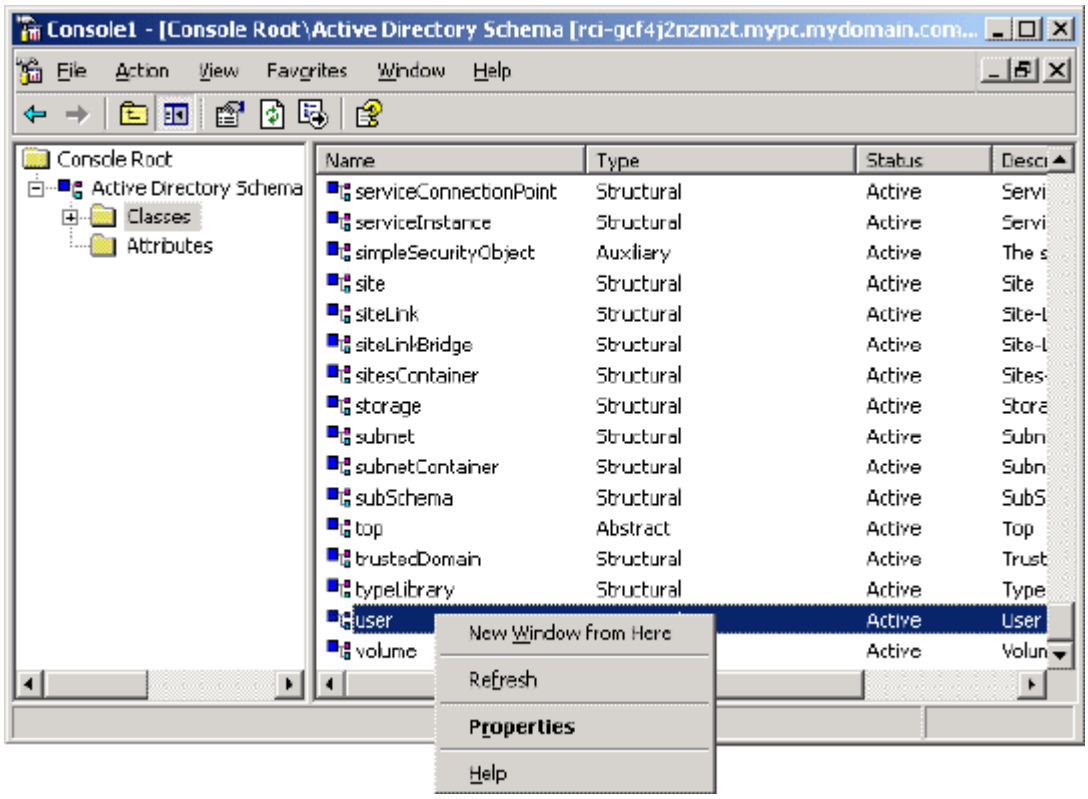
4. Type *rciusergroup* in the Common Name field.
5. Type *rciusergroup* in the LDAP Display Name field.
6. Type *1.3.6.1.4.1.13742.50* in the Unique x5000 Object ID field.
7. Type a meaningful description in the Description field.
8. Click the Syntax drop-down arrow and choose Case Insensitive String from the list.
9. Type *1* in the Minimum field.
10. Type *24* in the Maximum field.
11. Click OK to create the new attribute.

Adding Attributes to the Class

To add attributes to the class:

1. Click Classes in the left pane of the window.

2. Scroll to the user class in the right pane and right-click it.



3. Choose Properties from the menu. The user Properties dialog appears.
4. Click the Attributes tab to open it.
5. Click Add.
6. Choose rciusergroup from the Select Schema Object list.

Raritan
A brand of legrand

7. Click OK in the Select Schema Object dialog.
8. Click OK in the User Properties dialog.

Updating the Schema Cache

To update the schema cache:

1. Right-click Active Directory® Schema in the left pane of the window and select Reload the Schema.
2. Minimize the Active Directory Schema MMC (Microsoft® Management Console) console.

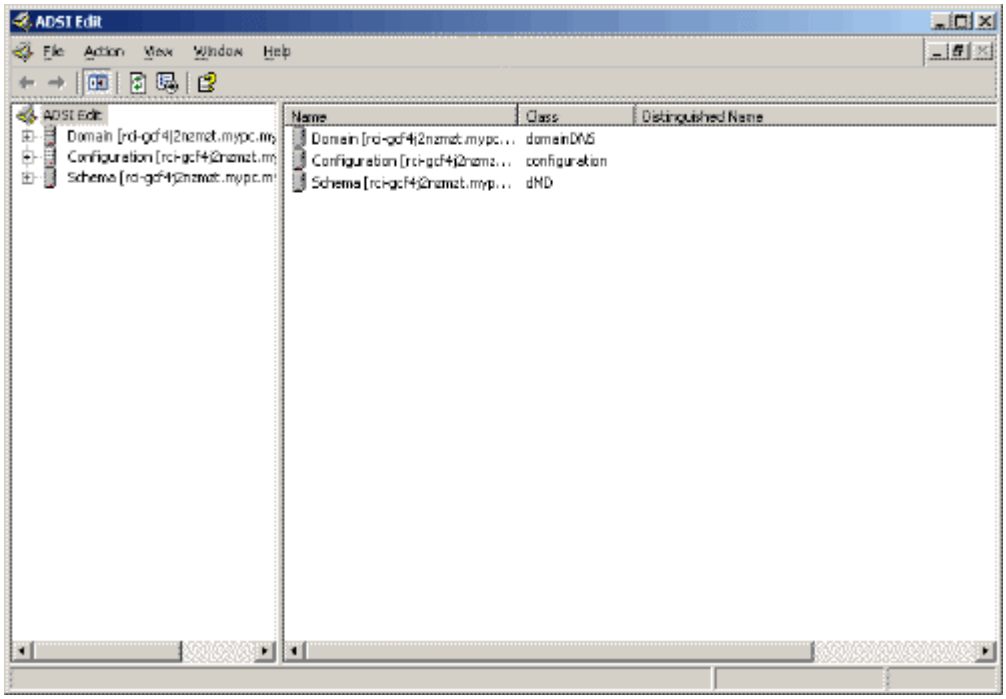
Editing rciusergroup Attributes for User Members

To run the Active Directory® script on a Windows 2003® server, use the script provided by Microsoft® (available on the Windows 2003 server installation CD). These scripts are loaded onto your system with a Microsoft® Windows 2003 installation. ADSI (Active Directory Service Interface) acts as a low-level editor for Active Directory, allowing you to perform common administrative tasks such as adding, deleting, and moving objects with a directory service.

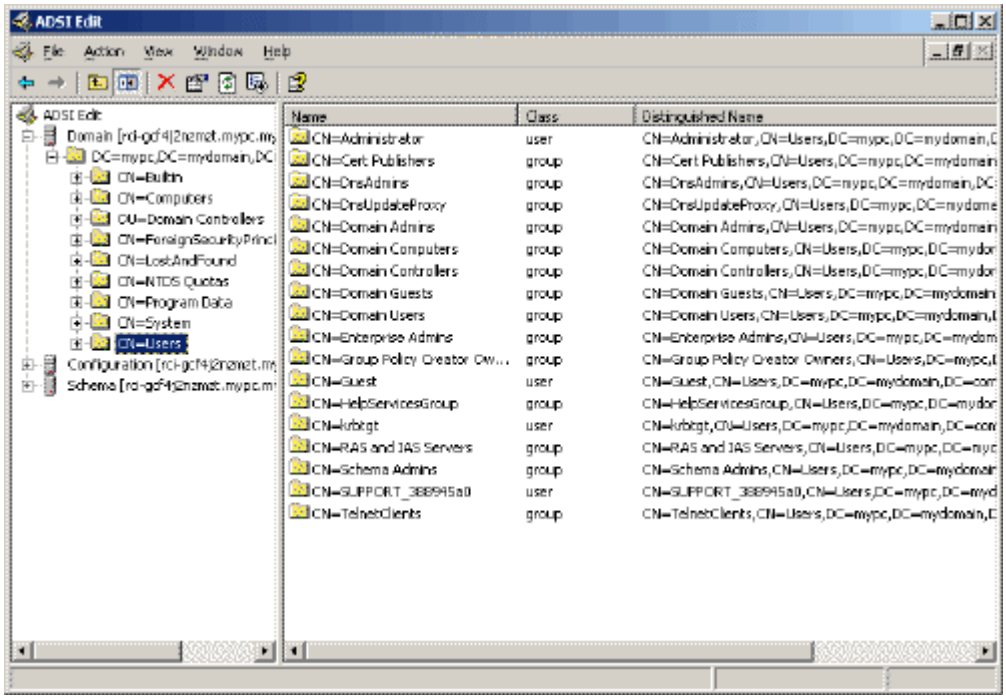
To edit the individual user attributes within the group rciusergroup:

1. From the installation CD, choose Support > Tools.
2. Double-click SUPTOOLS.MSI to install the support tools.

3. Go to the directory where the support tools were installed. Run adsiedit.msc. The ADSI Edit window opens.

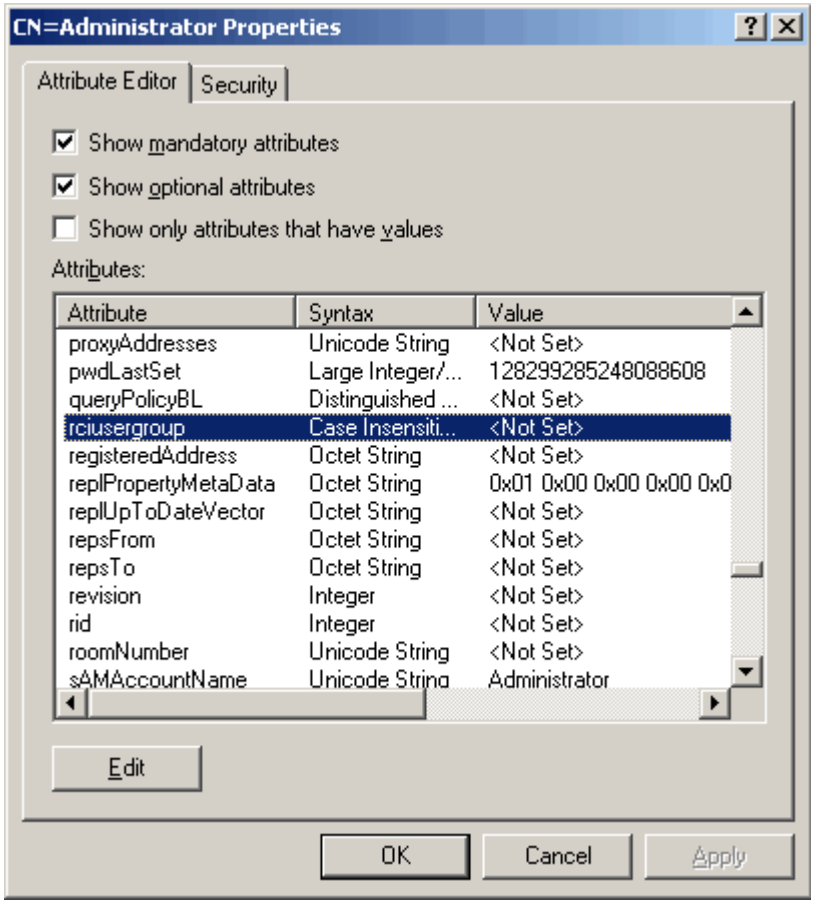


4. Open the Domain.
5. In the left pane of the window, select the CN=Users folder.

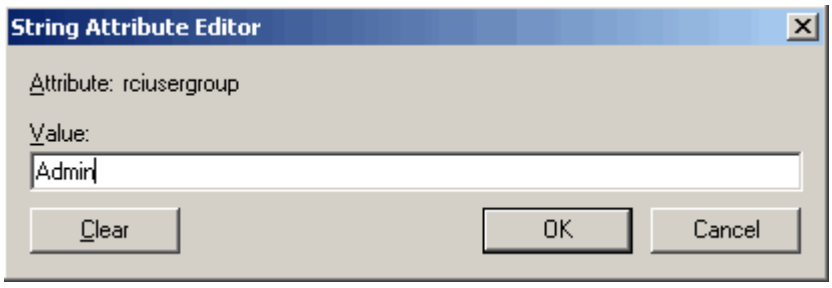


Raritan
A brand of legrand

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 PXC/PXO) in the Edit Attribute field. Click OK.



Appendix I 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 PXC/PXO. See ***Adding Radius Servers*** (on page 244).
2. Configure roles on the PXC/PXO. See ***Creating Roles*** (on page 182).
3. Configure PXC/PXO user credentials and roles on your RADIUS server.
   - To configure using standard attributes, see ***Standard Attributes*** (on page 636).
   - To configure using vendor-specific attributes, see ***Vendor-Specific Attributes*** (on page 655).

Note that we assume that the NPS is running on a Windows 2008 system in the NPS illustrations.

In This Chapter

Standard Attributes 636
Vendor-Specific Attributes 655
AD-Related Configuration 668

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 636).

For configuration on FreeRADIUS, see ***FreeRADIUS Standard Attribute Illustration*** (on page 654).

NPS Standard Attribute Illustration

To configure Windows 2008 NPS with the *standard attribute*, you must:

a. Add your PXC/PXO to NPS. See ***Step A: Add Your PXC/PXO as a RADIUS Client*** (on page 637).

b. On the NPS, configure Connection Request Policies and the standard attribute. See ***Step B: Configure Connection Policies and Standard Attributes*** (on page 641).

Some configuration associated with Microsoft Active Directory (AD) is also required for RADIUS authentication. See ***AD-Related Configuration*** (on page 668).

Step A: Add Your PXC/PXO as a RADIUS Client

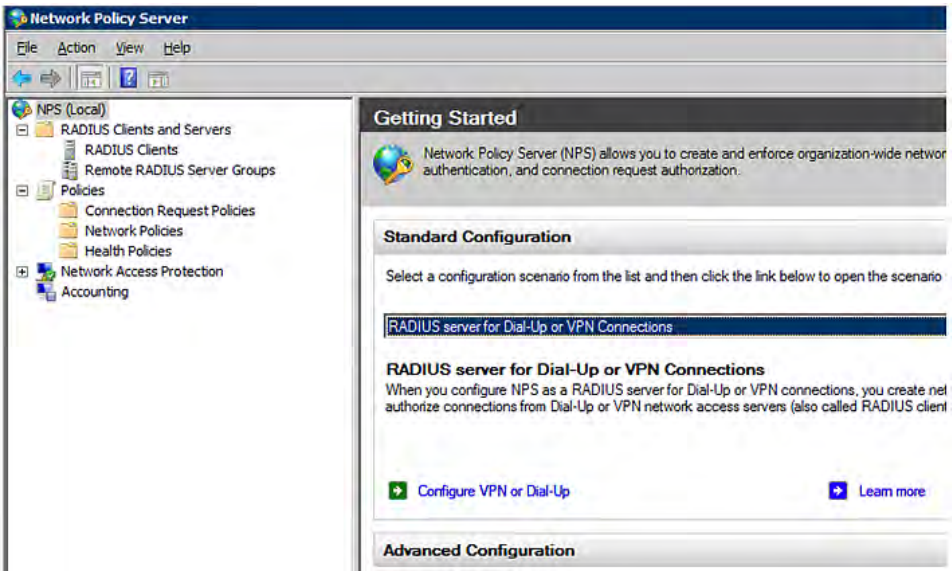
The RADIUS implementation on the PXC/PXO follows the standard RADIUS Internet Engineering Task Force (IETF) specification so you must select "RADIUS Standard" as its vendor name when configuring the NPS server.

Presumptions in the illustration:

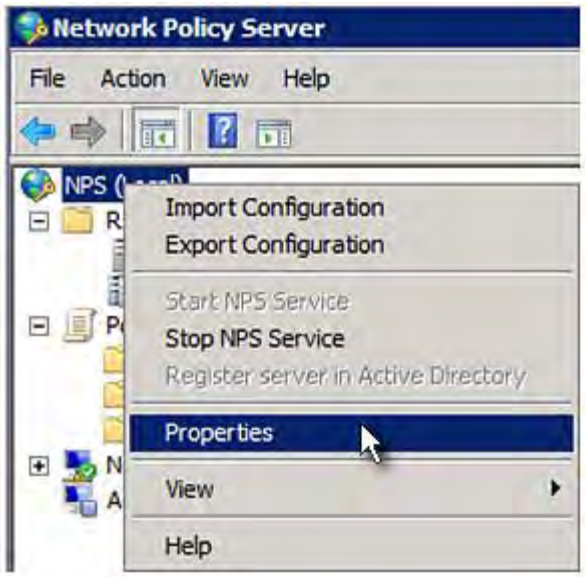
- IP address of your PXC/PXO = `192.168.56.29`
- RADIUS authentication port specified for PXC/PXO: *1812*
- RADIUS accounting port specified for PXC/PXO: *1813*

To add your PXC/PXO to the RADIUS NPS:

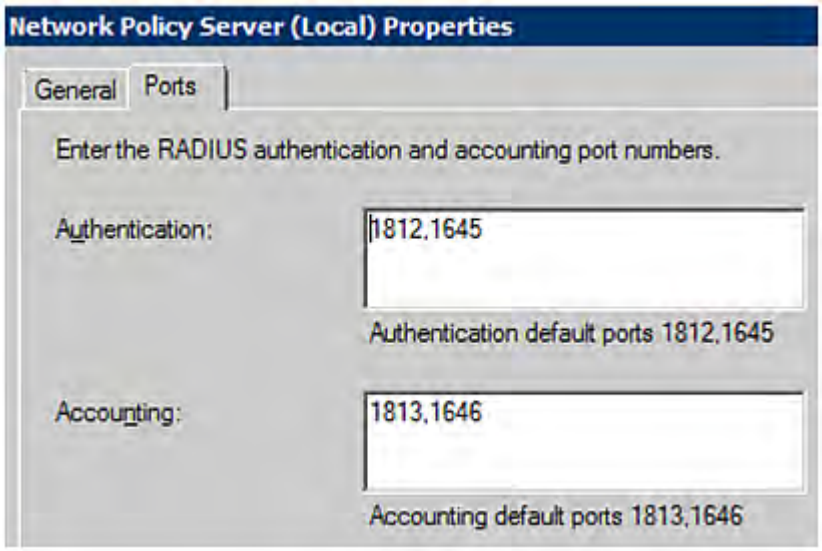
1. Choose Start > Administrative Tools > Network Policy Server. The Network Policy Server console window opens.



2. Right-click NPS (Local), and select Properties.

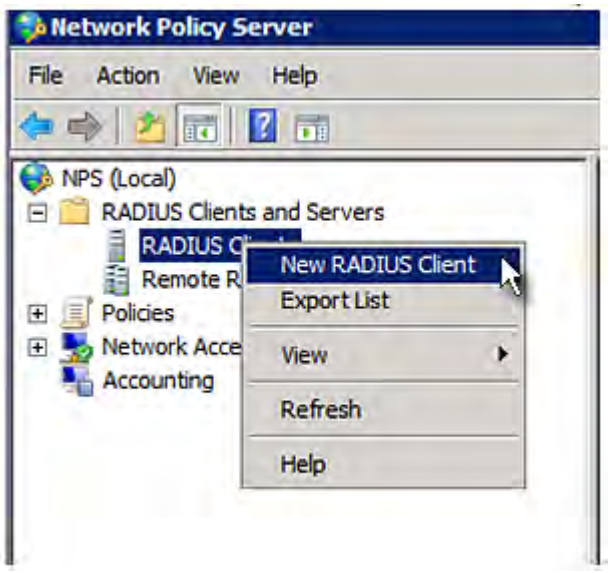


Verify the authentication and accounting port numbers shown in the properties dialog are the same as those specified on your PXC/PXO. In this example, they are 1812 and 1813. Then close this dialog.



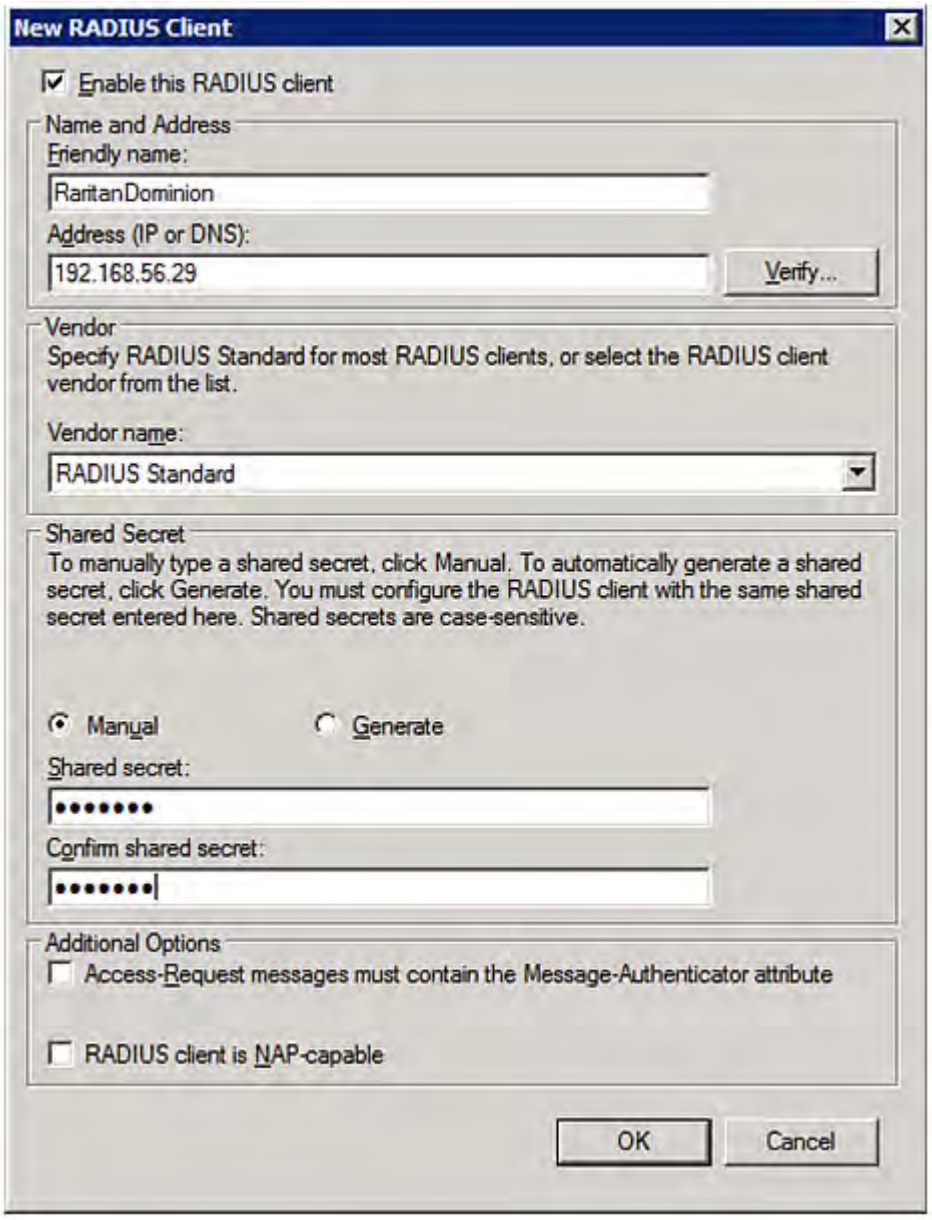
Raritan
A brand of legrand

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 PXC/PXO to NPS:
   a. Verify the "Enable this RADIUS client" checkbox is selected.
   b. Type a name for identifying your PXC/PXO 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 PXC/PXO.



5. Click OK.

Step B: Configure Connection Policies and Standard Attributes

You need to configure the following for connection request policies:

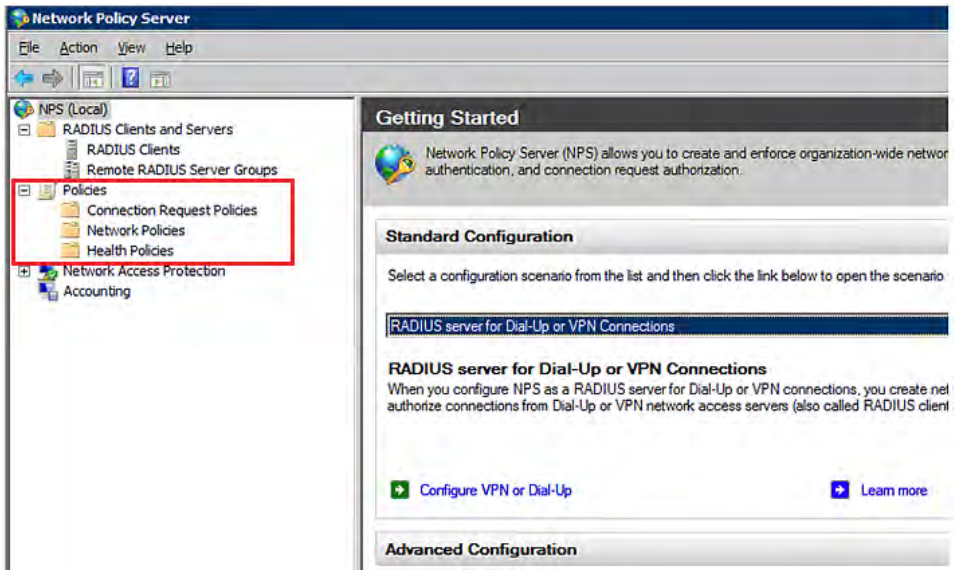
- IP address or host name of the PXC/PXO
- Connection request forwarding method
- Authentication method(s)
- Standard RADIUS attributes

Presumptions in the illustration:

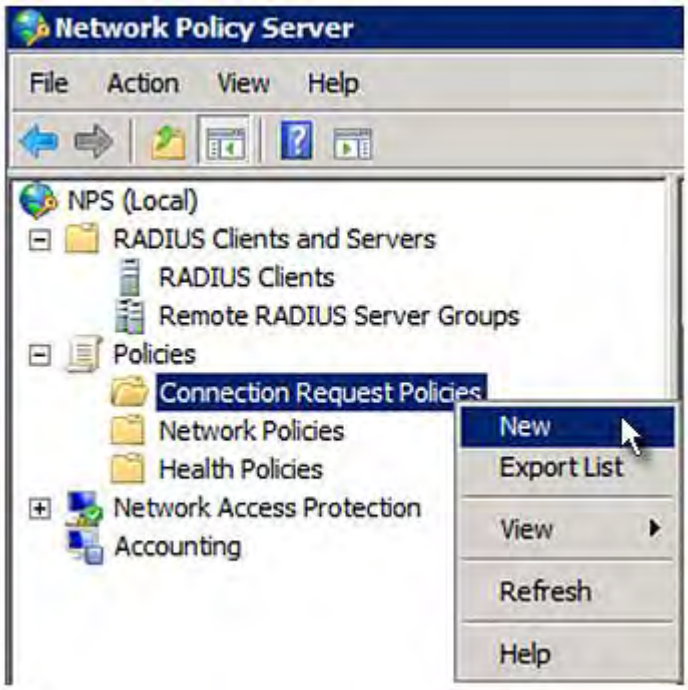
- IP address of your PXC/PXO = `192.168.56.29`
- *Local* NPS server is used
- RADIUS protocol selected on your PXC/PXO = CHAP
- Existing role of your PXC/PXO = `Admin`

Illustration:

1. Open the NPS console, and expand the Policies folder.



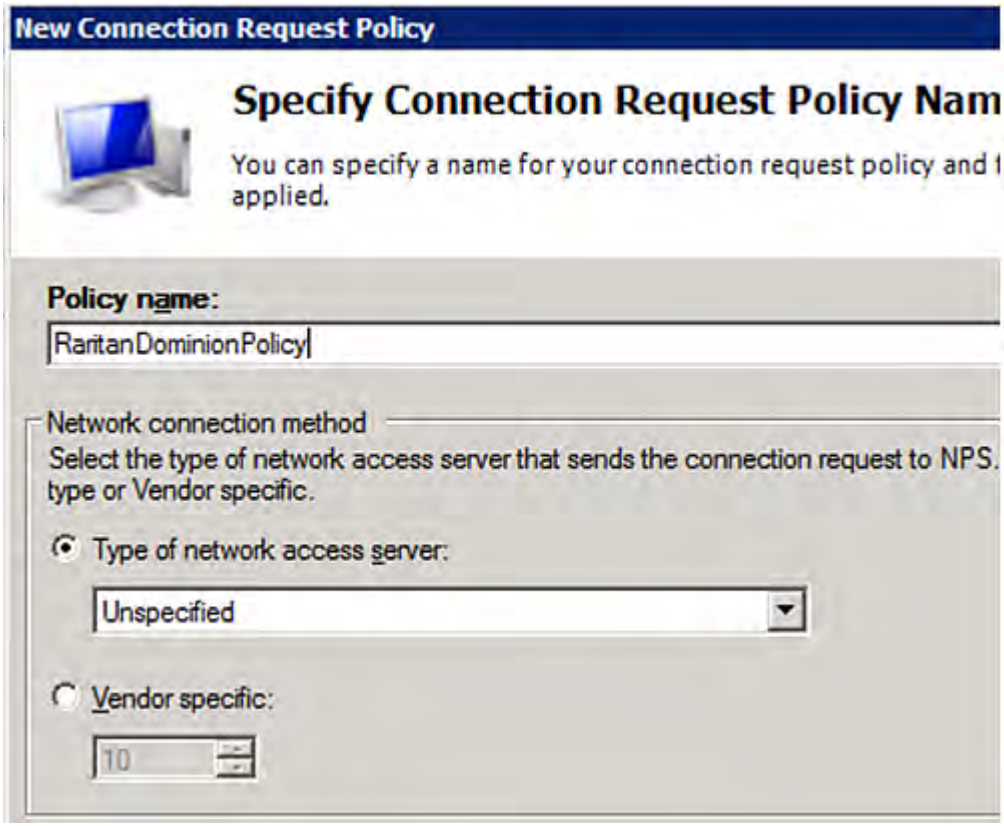
2. Right-click Connection Request Policies and select New. The New Connection Request Policy dialog appears.



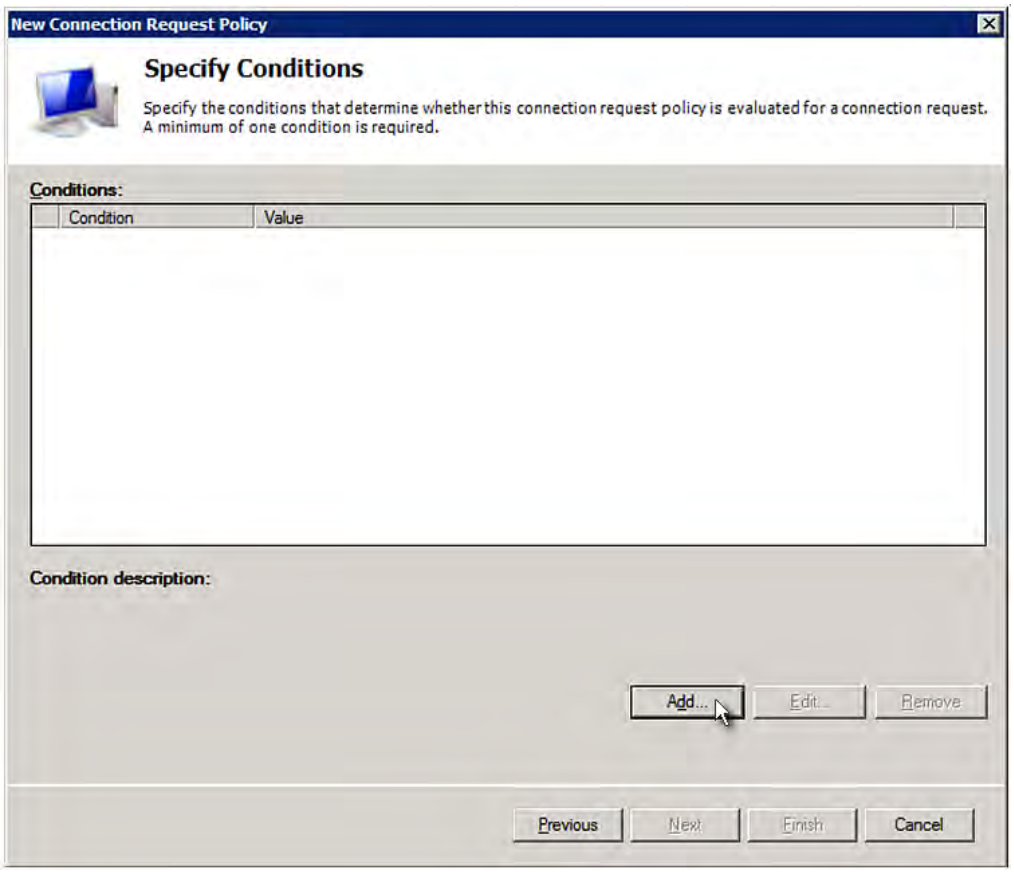
3. Type a descriptive name for identifying this policy in the "Policy name" field.

Raritan
A brand of legrand

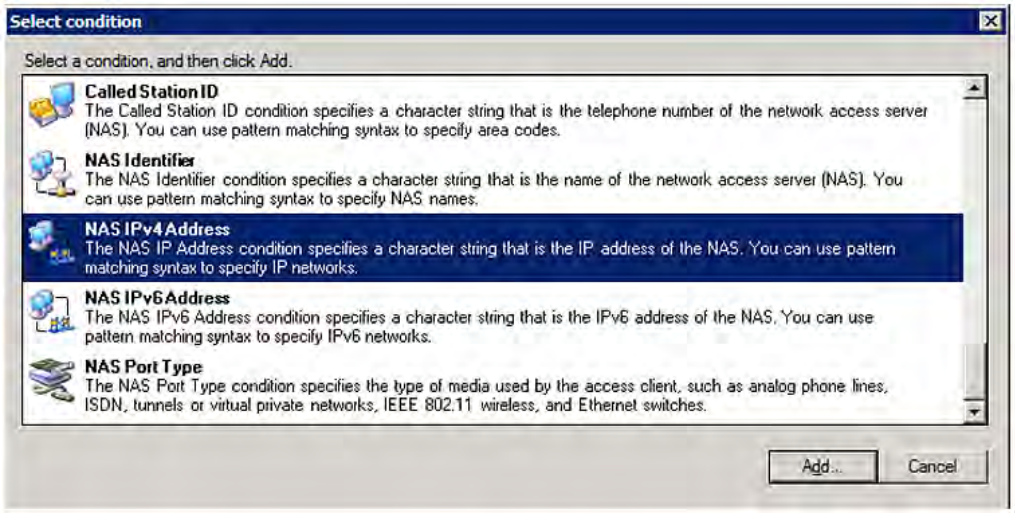
- You can leave the "Type of network access server" field to the default -- Unspecified.



4. Click Next to show the "Specify Conditions" screen. Click Add.

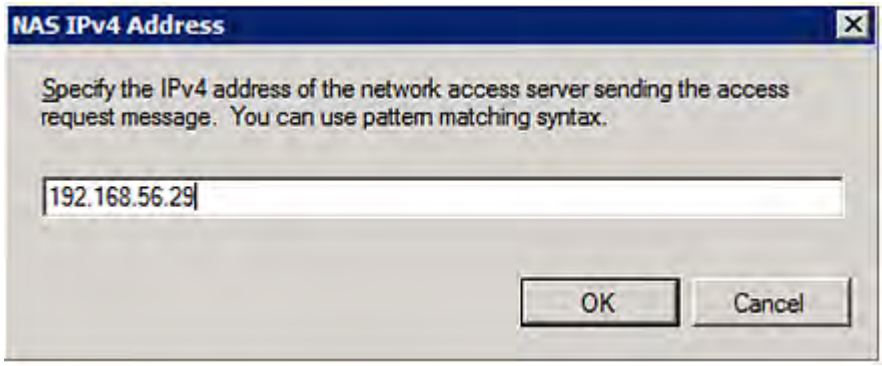


5. The "Select condition" dialog appears. Click Add.

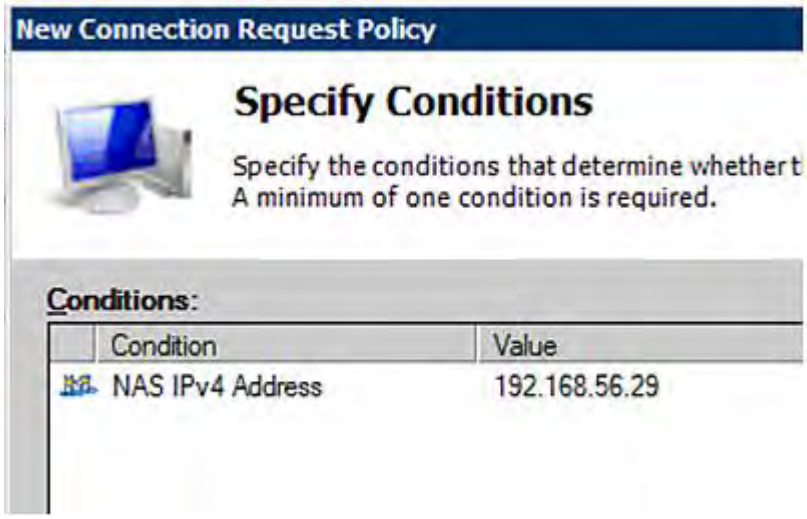


Raritan
A brand of legrand

6. The NAS IPv4 Address dialog appears. Type the PXC/PXO IP address -- *192.168.56.29*, and click OK.

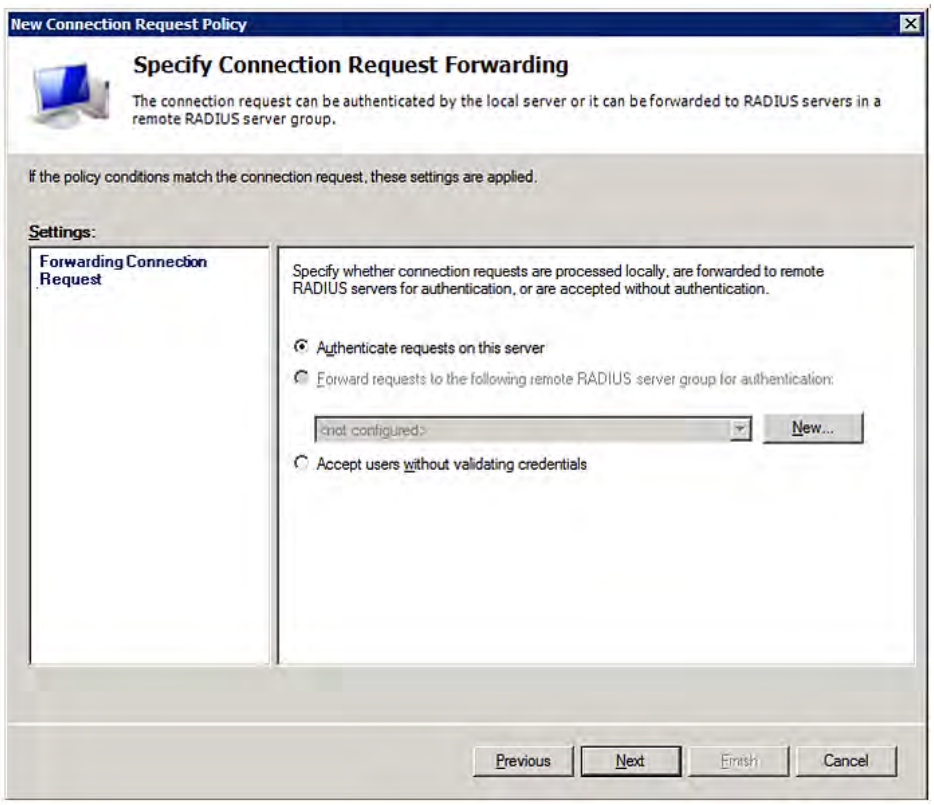


7. Click Next in the New Connection Request Policy dialog.



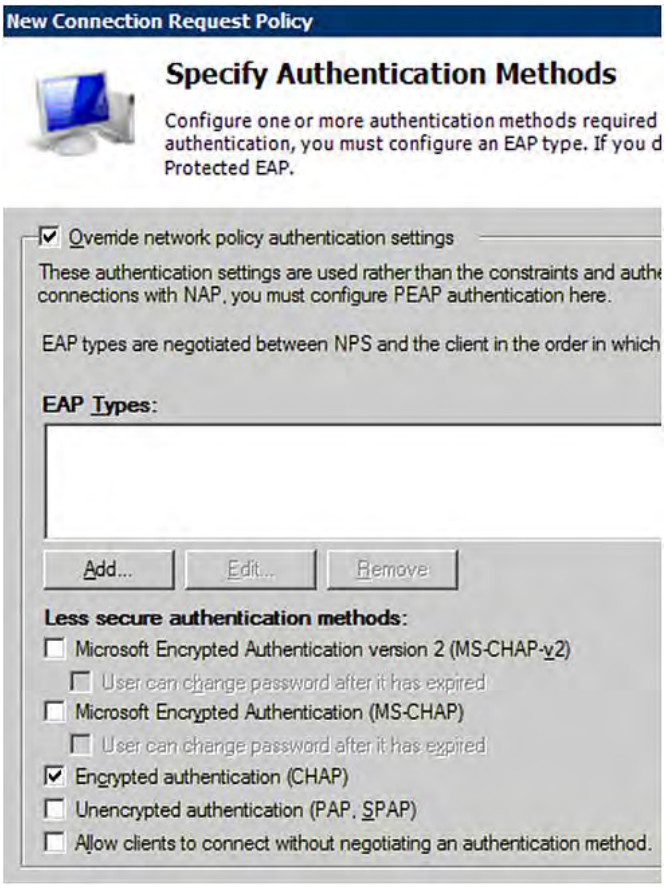
8. Select "Authenticate requests on this server" because a local NPS server is used in this example. Then click Next.

Note: Connection Request Forwarding options must match your environment.

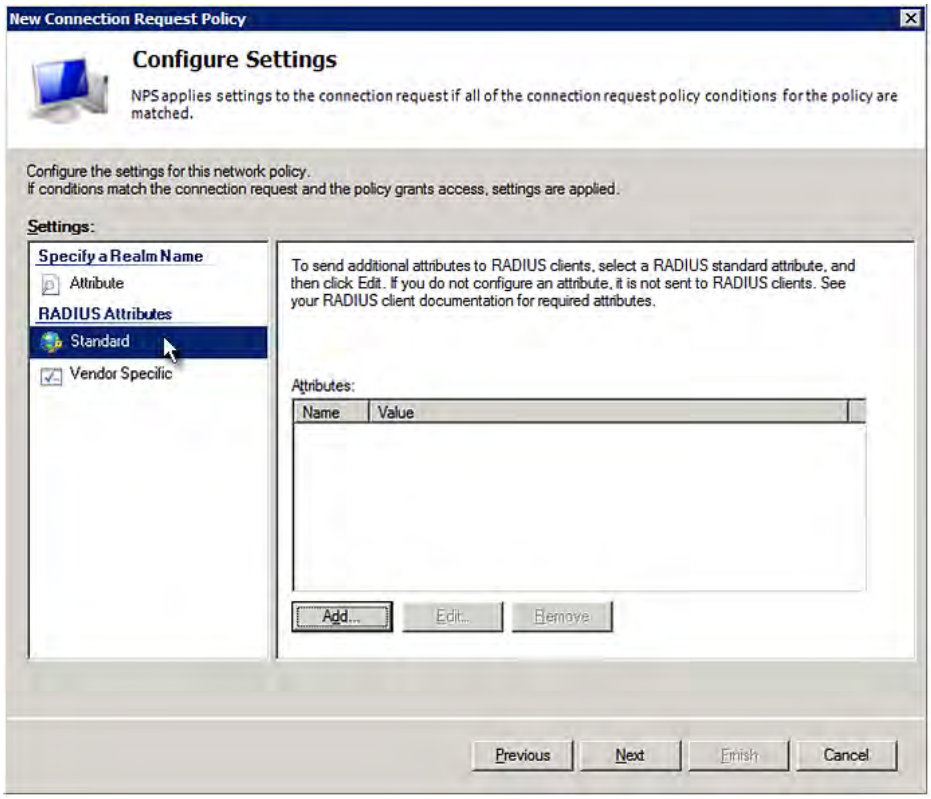


9. When the system prompts you to select the authentication method, select the following two options:
   - Override network policy authentication settings
   - CHAP -- the PXC/PXO uses "CHAP" in this example

Note: If your PXC/PXO uses PAP, then select "PAP."

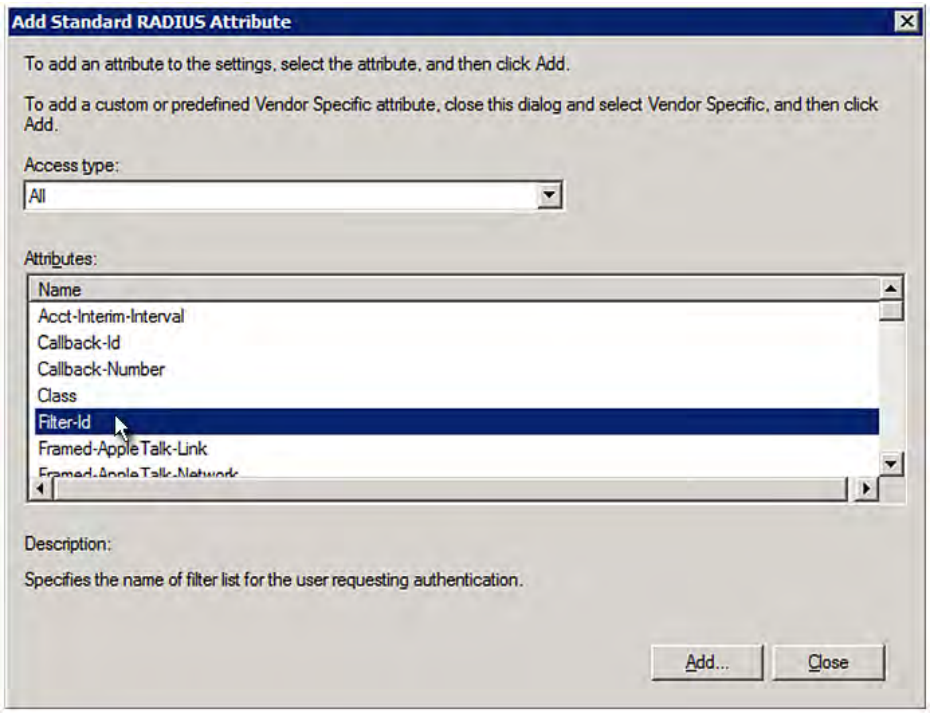


10. Select Standard to the left of the dialog and then click Add.

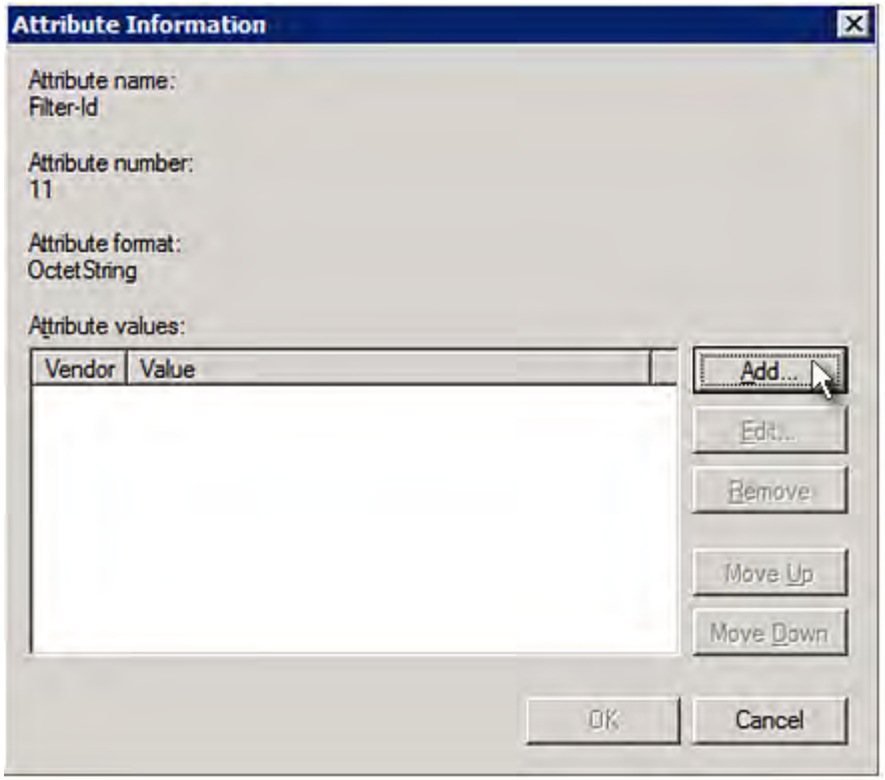


Raritan
A brand of legrand

11. Select Filter-Id from the list of attributes and click Add.

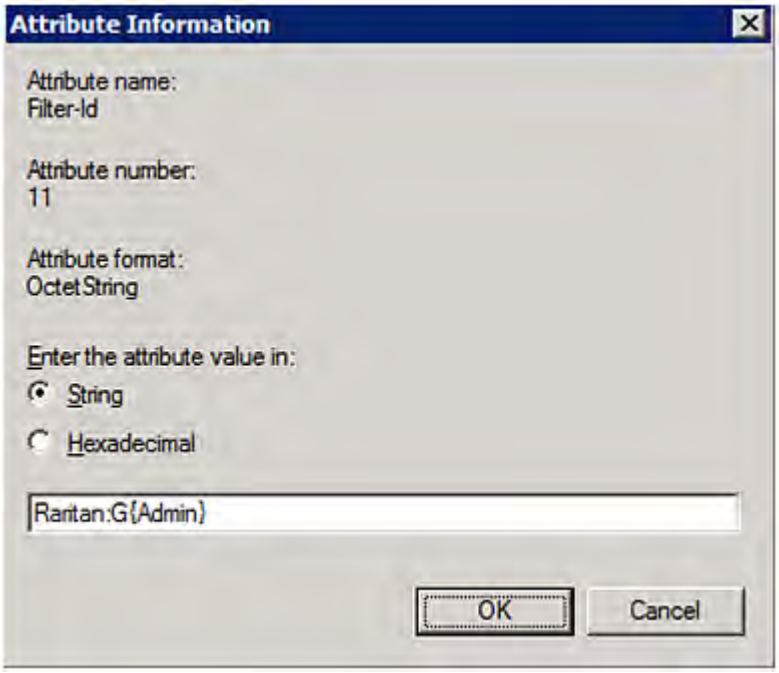


12. In the Attribute Information dialog, click Add.

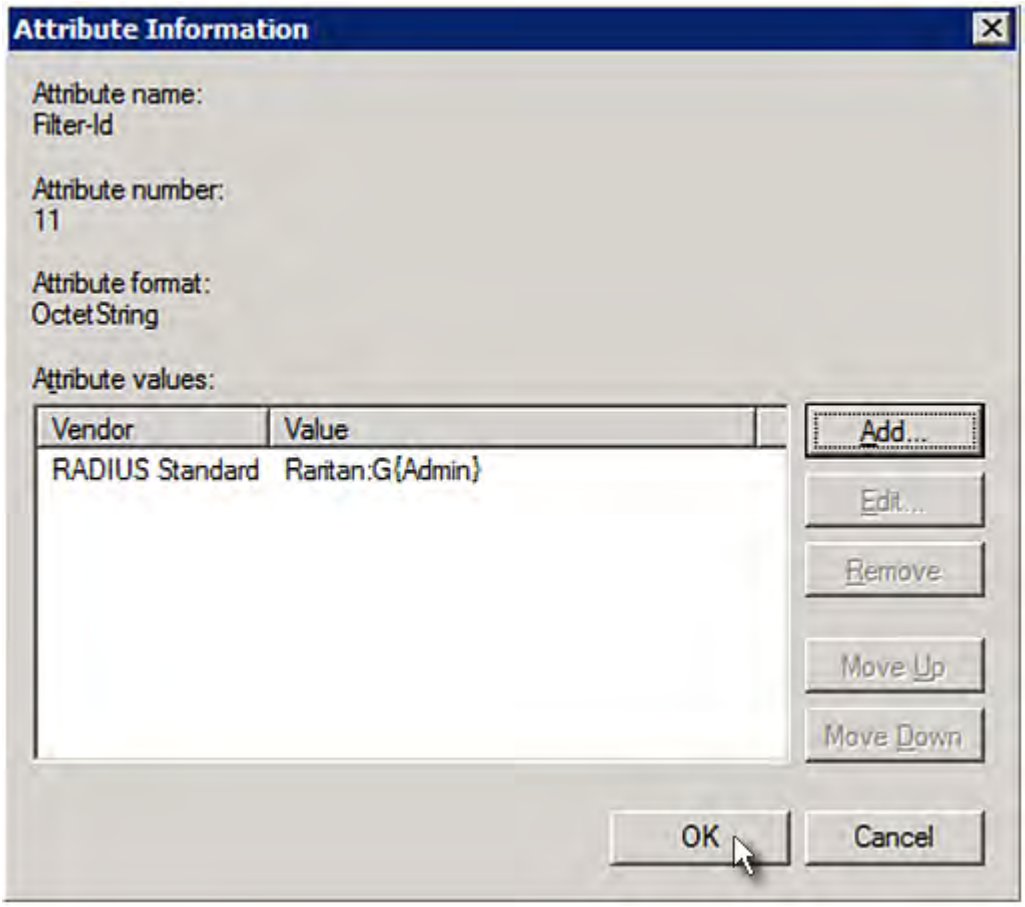


13. Select String, type *Raritan:G{Admin}* in the text box, and then click OK.

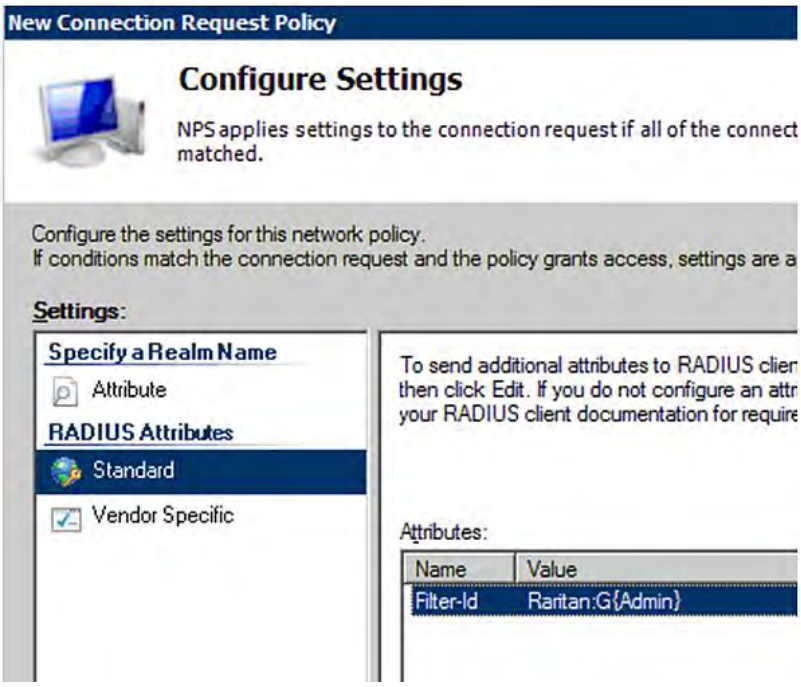
Admin inside the curved brackets {} is the existing role on the PXC/PXO. It is recommended to use the Admin role to test this configuration. The role name is case sensitive.



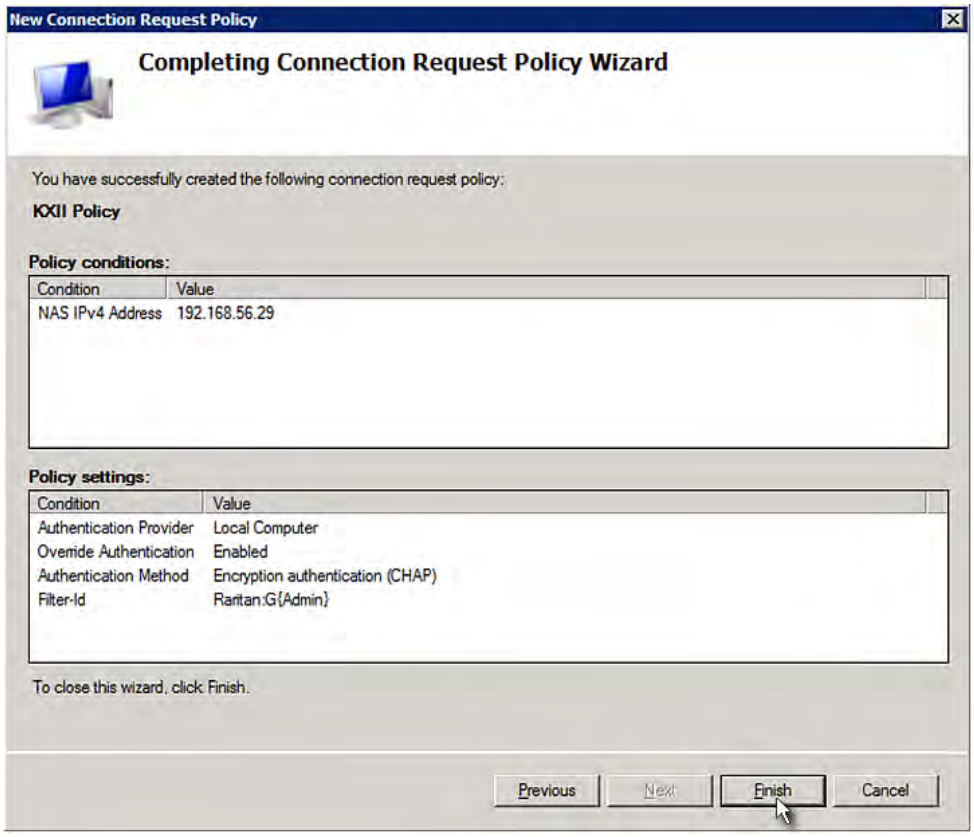
14. The new attribute is added. Click OK.



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 655).

For configuration on FreeRADIUS, see ***FreeRADIUS VSA Illustration*** (on page 667).

NPS VSA Illustration

To configure Windows 2008 NPS with the *vendor-specific attribute*, you must:

a. Add your PXC/PXO to NPS. See ***Step A: Add Your PXC/PXO as a RADIUS Client*** (on page 637).

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 660).

Some configuration associated with Microsoft Active Directory (AD) is also required for RADIUS authentication. See ***AD-Related Configuration*** (on page 668).

Step A: Add Your PXC/PXO as a RADIUS Client

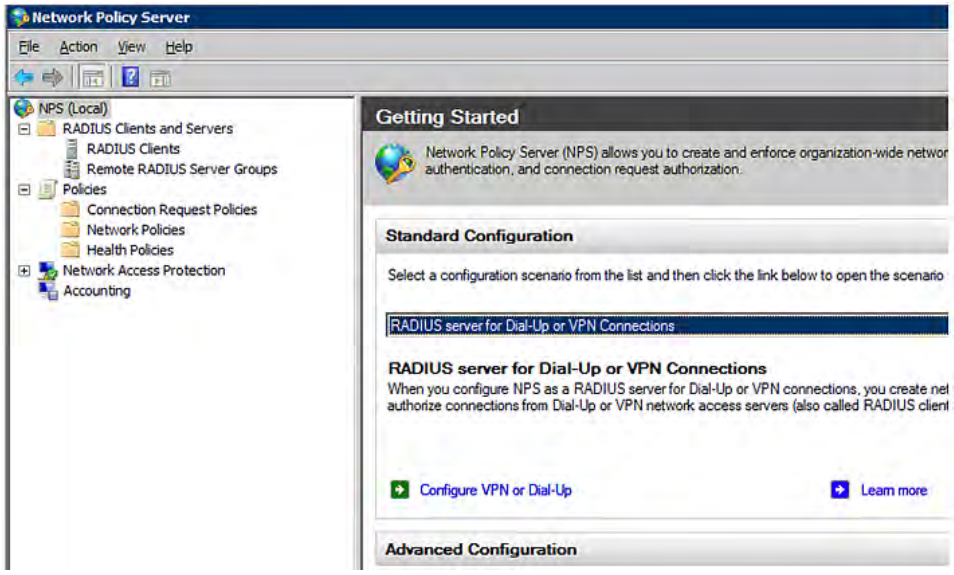
The RADIUS implementation on the PXC/PXO follows the standard RADIUS Internet Engineering Task Force (IETF) specification so you must select "RADIUS Standard" as its vendor name when configuring the NPS server.

Presumptions in the illustration:

- IP address of your PXC/PXO = `192.168.56.29`
- RADIUS authentication port specified for PXC/PXO: *1812*
- RADIUS accounting port specified for PXC/PXO: *1813*

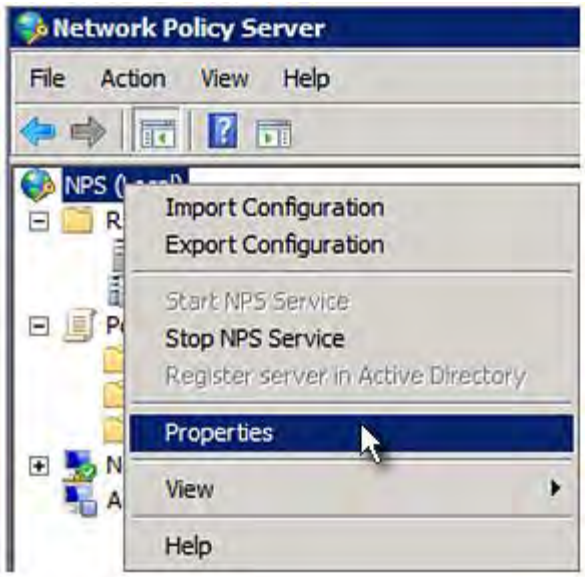
To add your PXC/PXO to the RADIUS NPS:

1. Choose Start > Administrative Tools > Network Policy Server. The Network Policy Server console window opens.

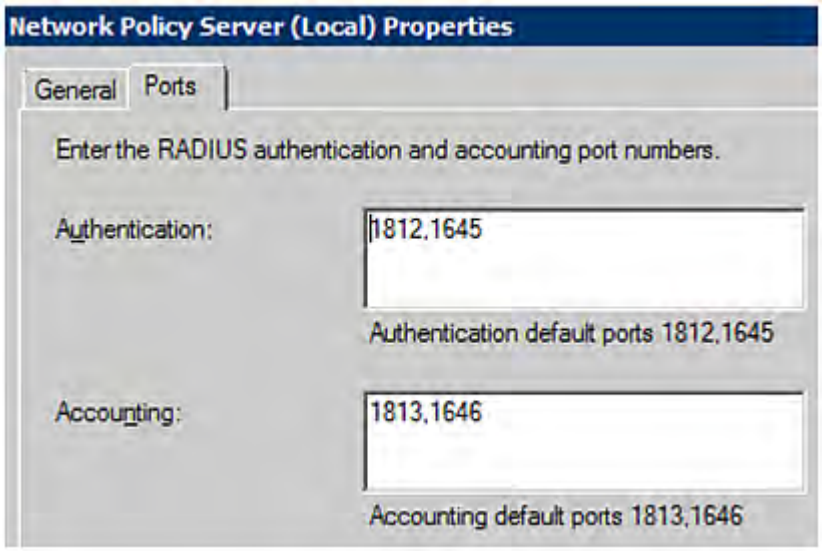


Raritan
A brand of legrand

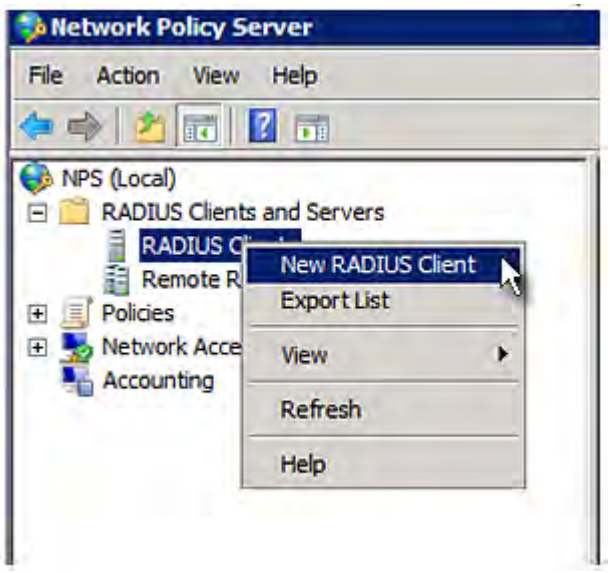
2. Right-click NPS (Local), and select Properties.



Verify the authentication and accounting port numbers shown in the properties dialog are the same as those specified on your PXC/PXO. In this example, they are 1812 and 1813. Then close this dialog.



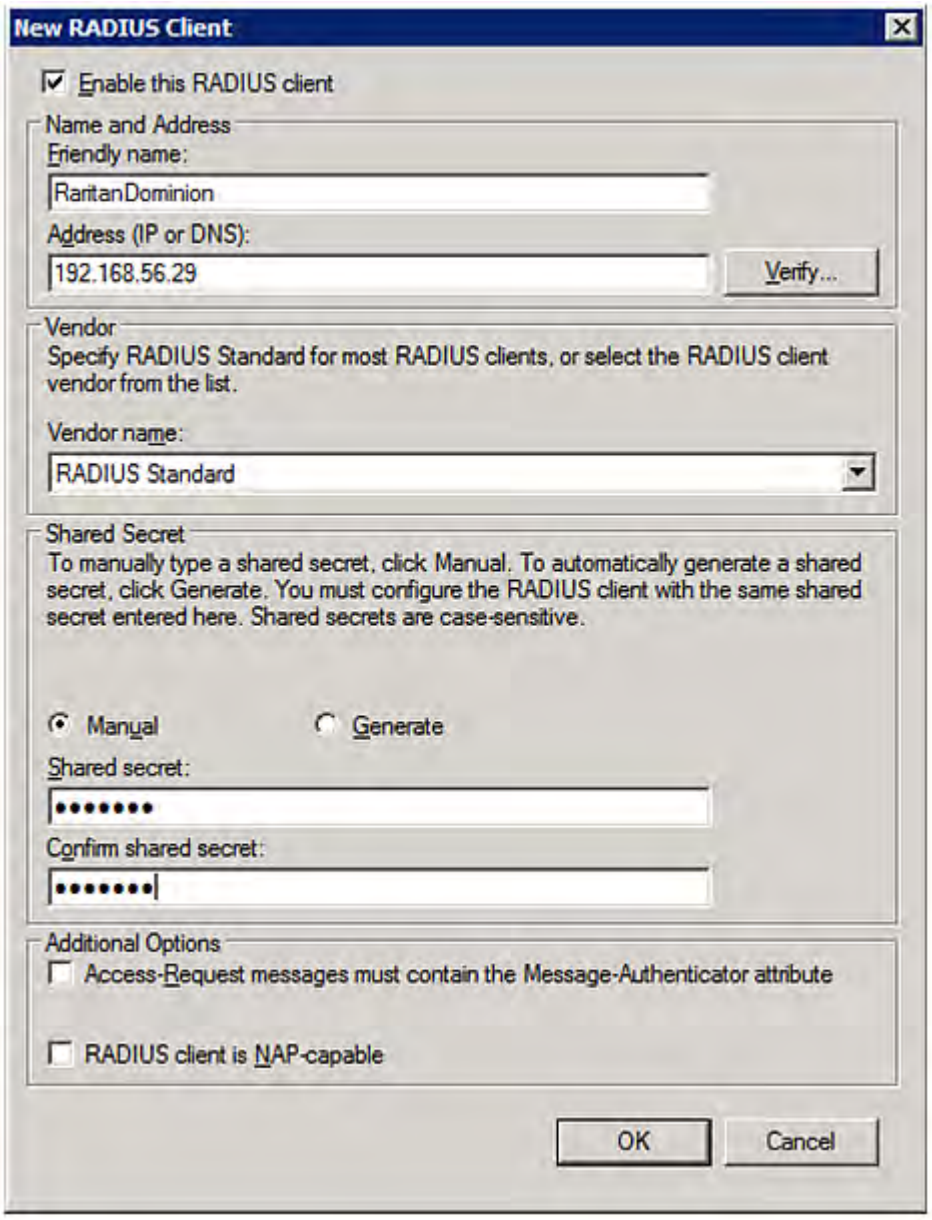
3. Under "RADIUS Clients and Servers," right-click RADIUS Client and select New RADIUS Client. The New RADIUS Client dialog appears.



4. Do the following to add your PXC/PXO to NPS:
   a. Verify the "Enable this RADIUS client" checkbox is selected.
   b. Type a name for identifying your PXC/PXO 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.

Raritan
A brand of legrand

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 PXC/PXO.



5. Click OK.

Step B: Configure Connection Policies and Vendor-Specific Attributes

You need to configure the following for connection request policies:

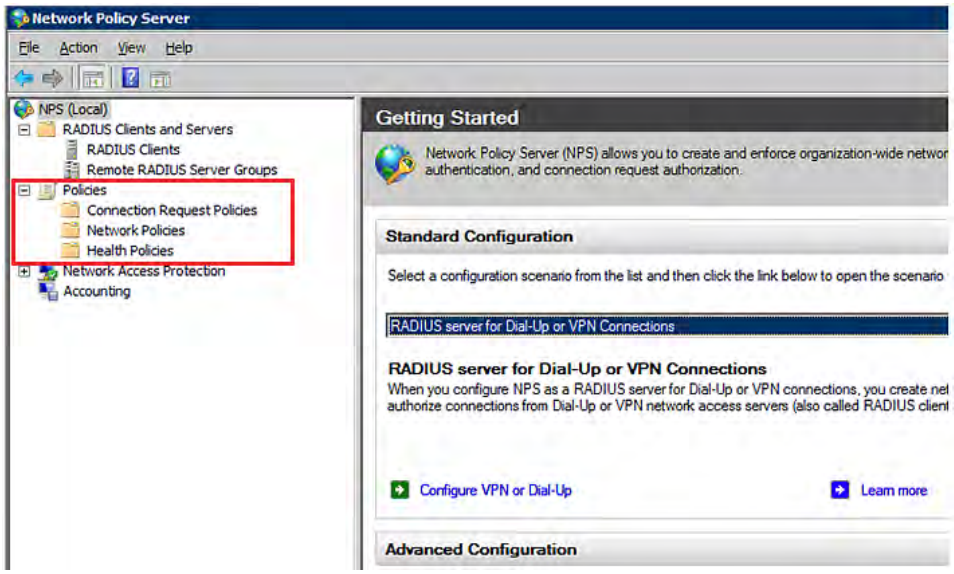
- IP address or host name of the PXC/PXO
- Connection request forwarding method
- Authentication method(s)
- Standard RADIUS attributes

Presumptions in the illustration:

- IP address of your PXC/PXO = `192.168.56.29`
- *Local* NPS server is used
- RADIUS protocol selected on your PXC/PXO = CHAP
- Existing roles of your PXC/PXO = `Admin`, `User` and `SystemTester`

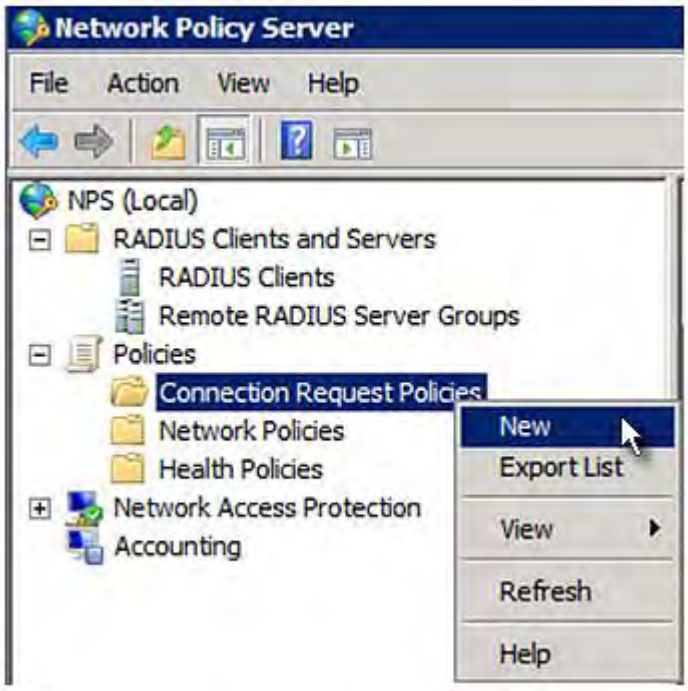
Illustration:

1. Open the NPS console, and expand the Policies folder.



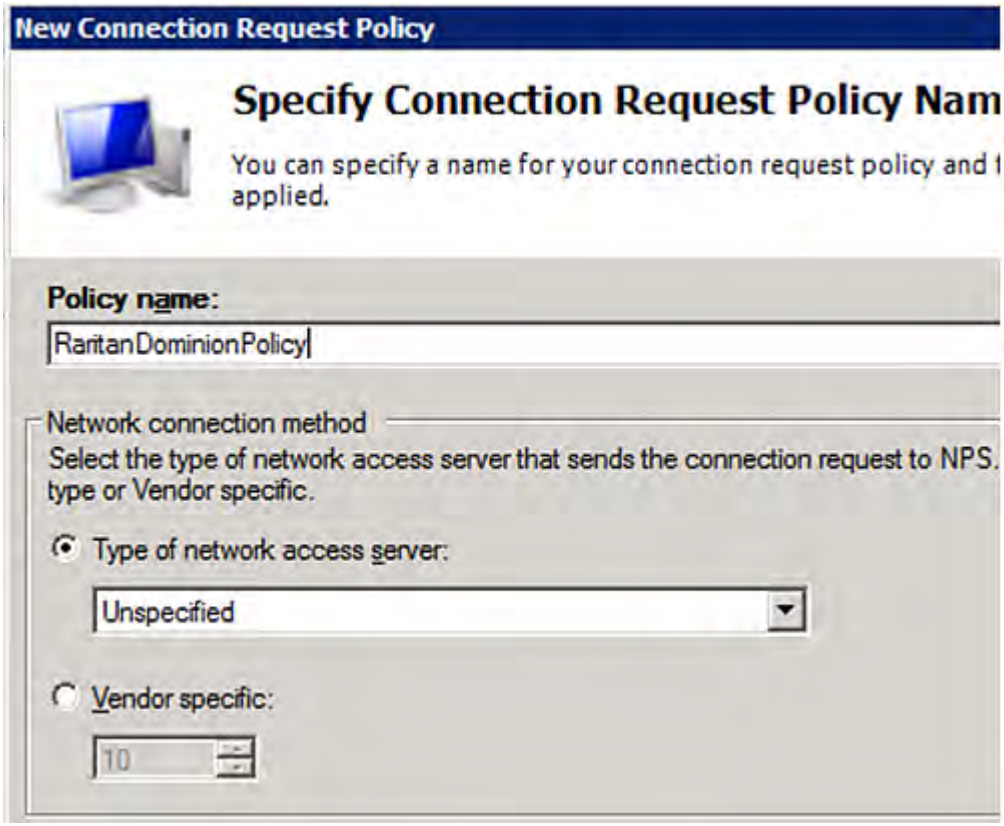
Raritan
A brand of legrand

2. Right-click Connection Request Policies and select New. The New Connection Request Policy dialog appears.

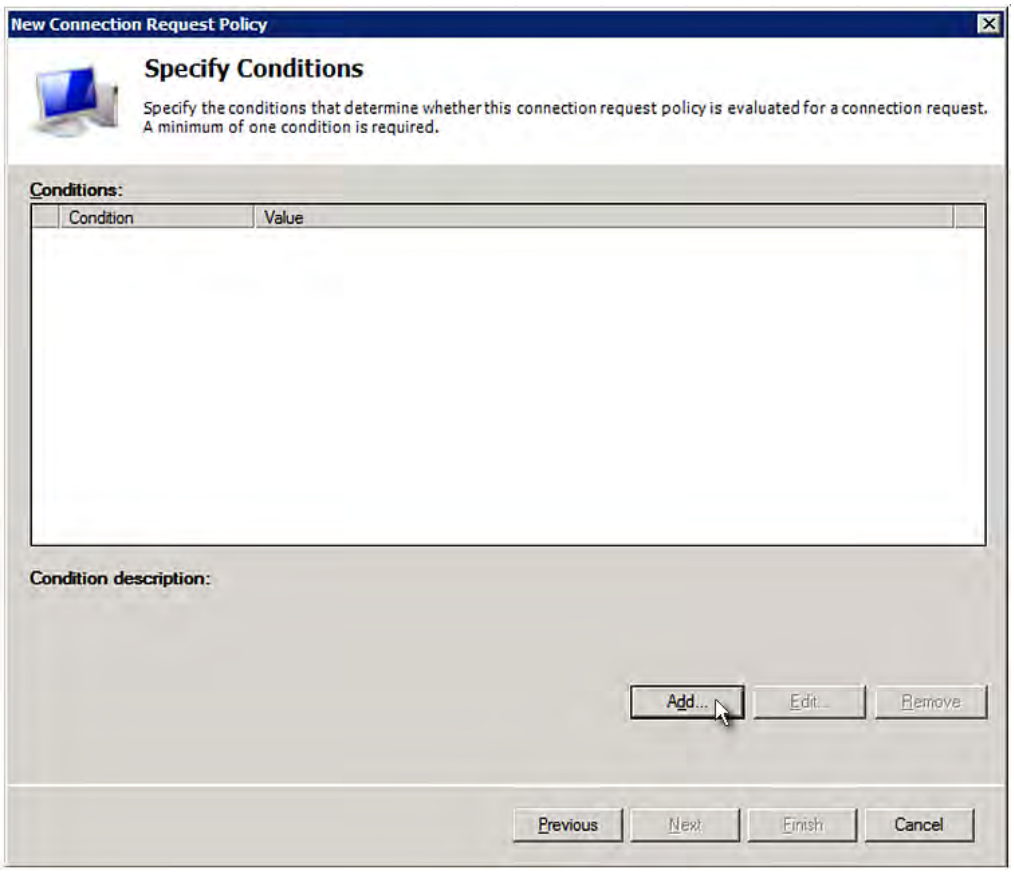


3. Type a descriptive name for identifying this policy in the "Policy name" field.

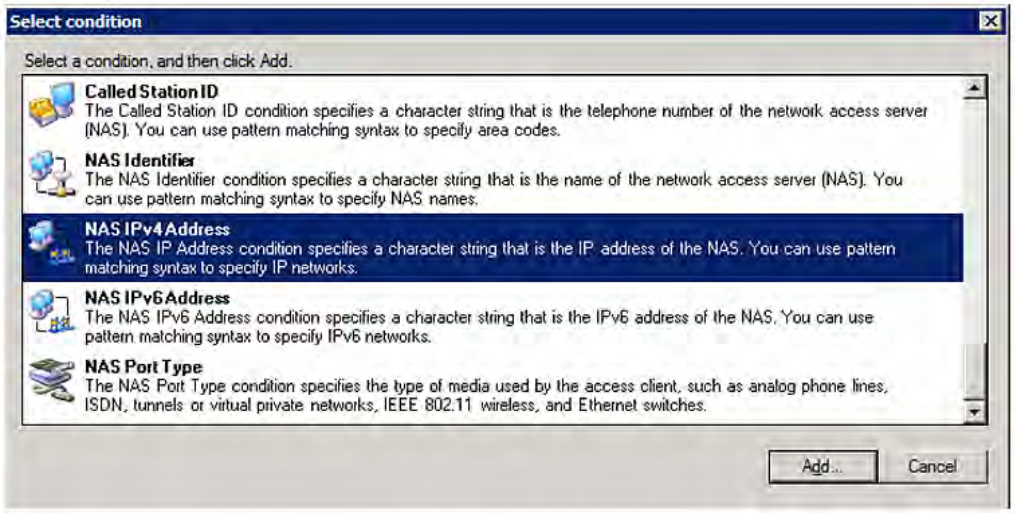
- You can leave the "Type of network access server" field to the default -- Unspecified.



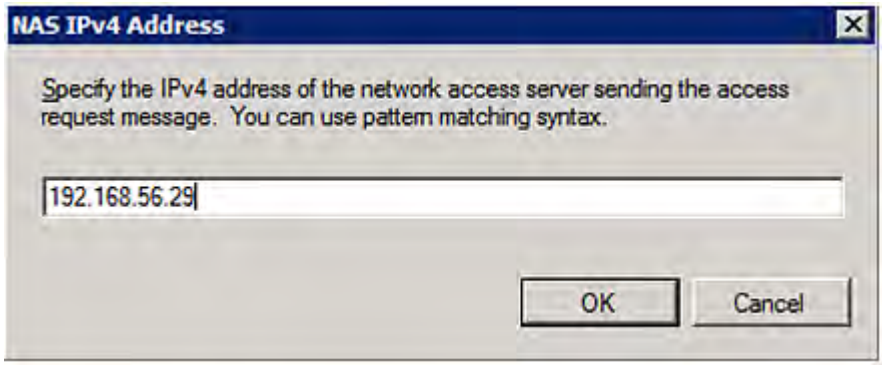
4. Click Next to show the "Specify Conditions" screen. Click Add.



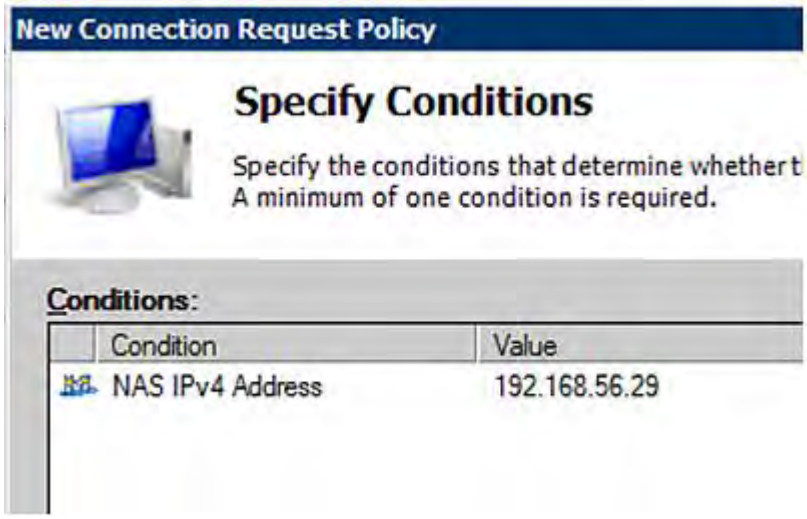
5. The "Select condition" dialog appears. Click Add.



6. The NAS IPv4 Address dialog appears. Type the PXC/PXO IP address -- *192.168.56.29*, and click OK.



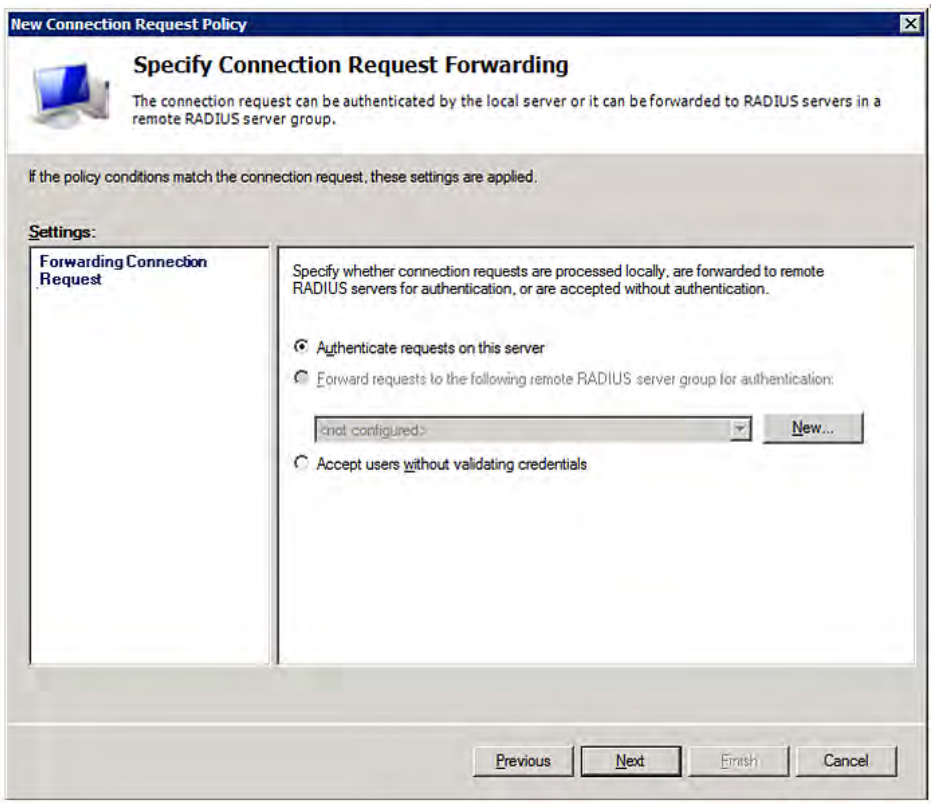
7. Click Next in the New Connection Request Policy dialog.



8. Select "Authenticate requests on this server" because a local NPS server is used in this example. Then click Next.

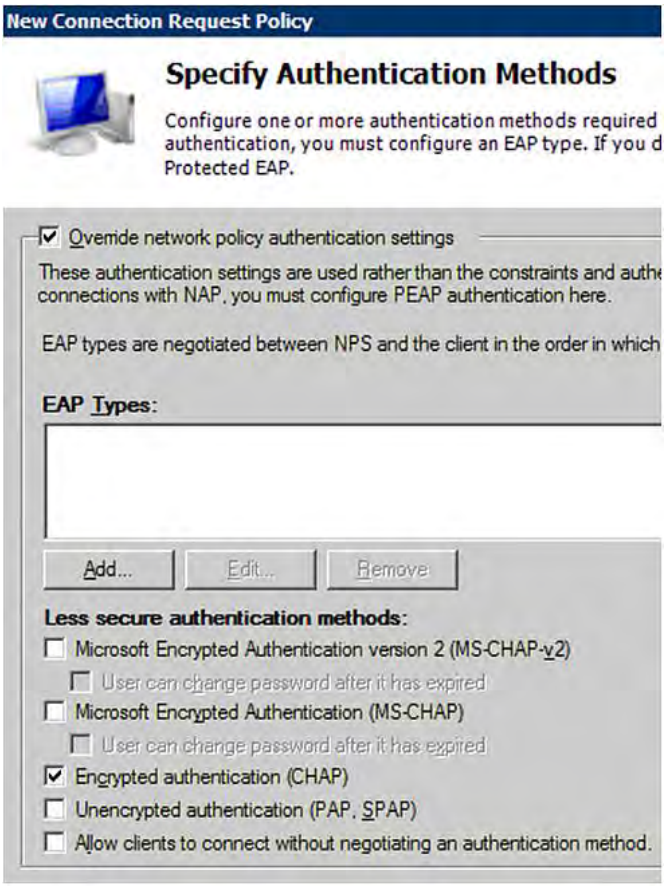
Raritan
A brand of legrand

Note: Connection Request Forwarding options must match your environment.



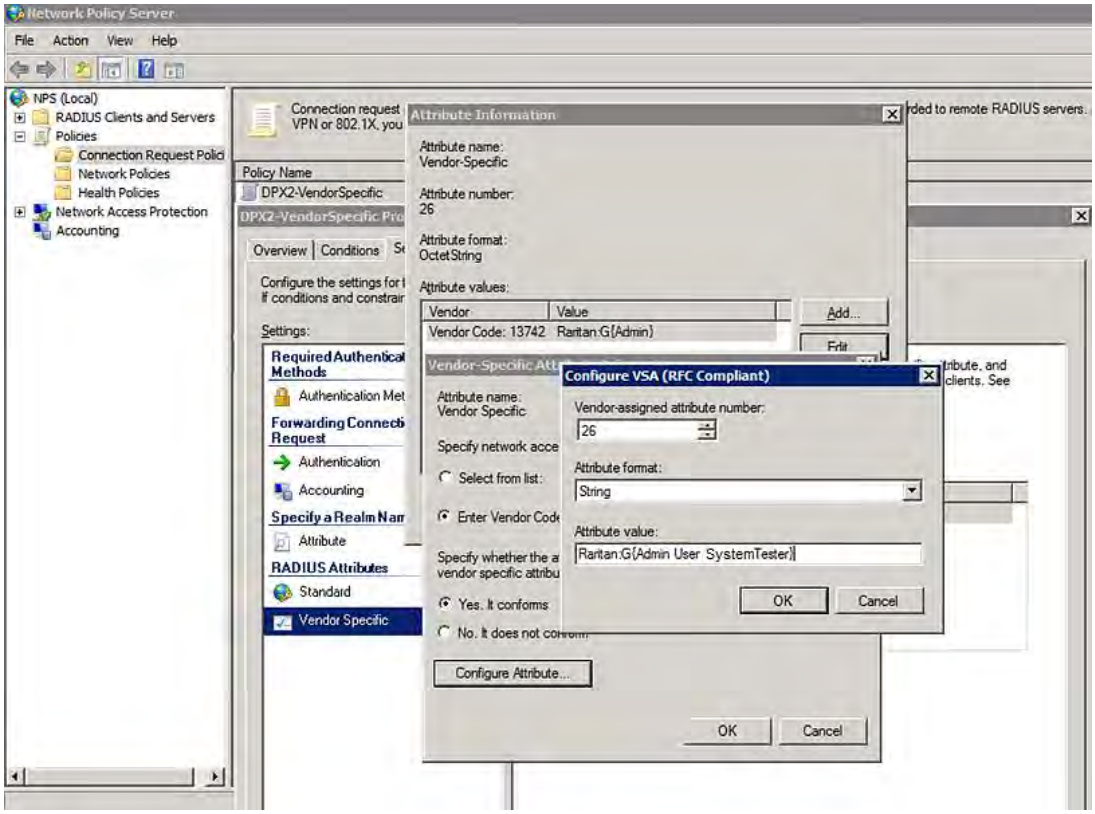
9. When the system prompts you to select the authentication method, select the following two options:
   - Override network policy authentication settings
   - CHAP -- the PXC/PXO uses "CHAP" in this example

Note: If your PXC/PXO uses PAP, then select "PAP."



10. Select Vendor Specific to the left of the dialog, and click Add. The Add Vendor Specific Attribute dialog appears.
11. Select Custom in the Vendor field, and click Add. The Attribute Information dialog appears.
12. Click Add, and the Vendor-Specific Attribute Information dialog appears.
13. Click "Enter Vendor Code" and type *13742*.
14. Select "Yes, it conforms" to indicate that the custom attribute conforms to the RADIUS Request For Comment (RFC).
15. Click Configure Attribute, and then:
    a. Type *26* in the "Vendor-assigned attribute number" field.
    b. Select String in the "Attribute format" field.
    c. Type *Raritan:G{Admin User SystemTester}* in the "Attribute value" field. In this example, three roles 'Admin,' 'User' and 'SystemTester' are specified inside the curved brackets {}.

Note that multiple roles are separated with a space.



16. Click OK.

FreeRADIUS VSA Illustration

A vendor-specific dictionary file is required for the vendor-specific-attribute configuration on FreeRADIUS. Therefore, there are two major configuration steps.

a. Use a dictionary to define the Raritan vendor-specific attribute
b. Add all user data, including user names, passwords, and roles

Presumptions in the illustration:

- Raritan attribute = `Raritan-User-Roles`
- User name = `steve`
- Steve's password = `test123`
- Steve's roles = `Admin`, `User` and `SystemTester`

Step A -- define the vendor-specific attribute in FreeRADIUS:

1. Go to this location: `/etc/raddb/dictionary`.
2. Type the following in the Raritan dictionary file.

```
VENDOR Raritan 13742
BEGIN-VENDOR Raritan
ATTRIBUTE Raritan-User-Roles 26 string
END-VENDOR Raritan
```

Step B -- create a user profile for "steve" in FreeRADIUS:

1. Go to this location: `/etc/raddb/users`.
2. Add the data of the user "steve" by typing the following. Note that the values after the equal sign (=) must be enclosed in double quotes (").

```
steve Cleartext-Password := "test123"
Raritan-PDU-User-Roles = "Raritan:G{Admin User SystemTester}"
```

AD-Related Configuration

When RADIUS authentication is intended, make sure you also configure the following settings related to Microsoft Active Directory (AD):

- Register the NPS server in AD
- Configure remote access permission for users in AD

The NPS server is registered in AD only when NPS is configured for the FIRST time and user accounts are created in AD.

If CHAP authentication is used, you must enable the following feature for user accounts created in AD:

- Store password using reversible encryption

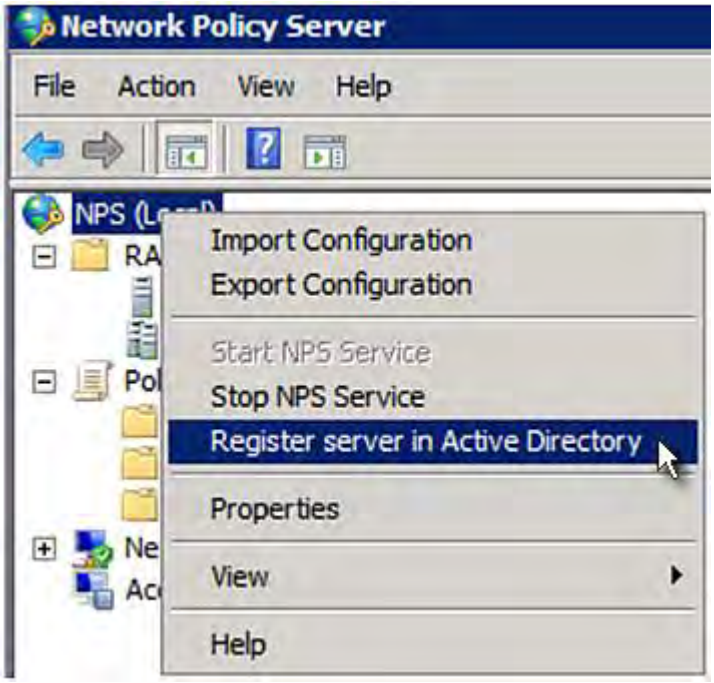
Important: Reset the user password if the password is set before you enable the "Store password using reversible encryption" feature.

To register NPS:

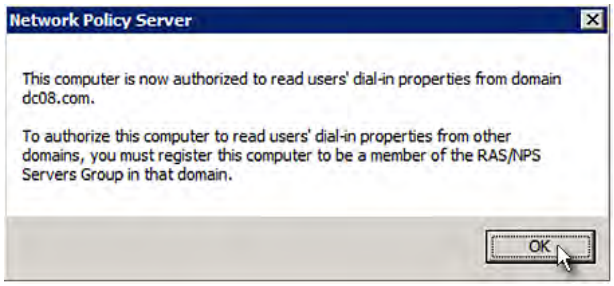
1. Open the NPS console.

Raritan
A brand of legrand

2. Right-click NPS (Local) and select "Register server in Active Directory."



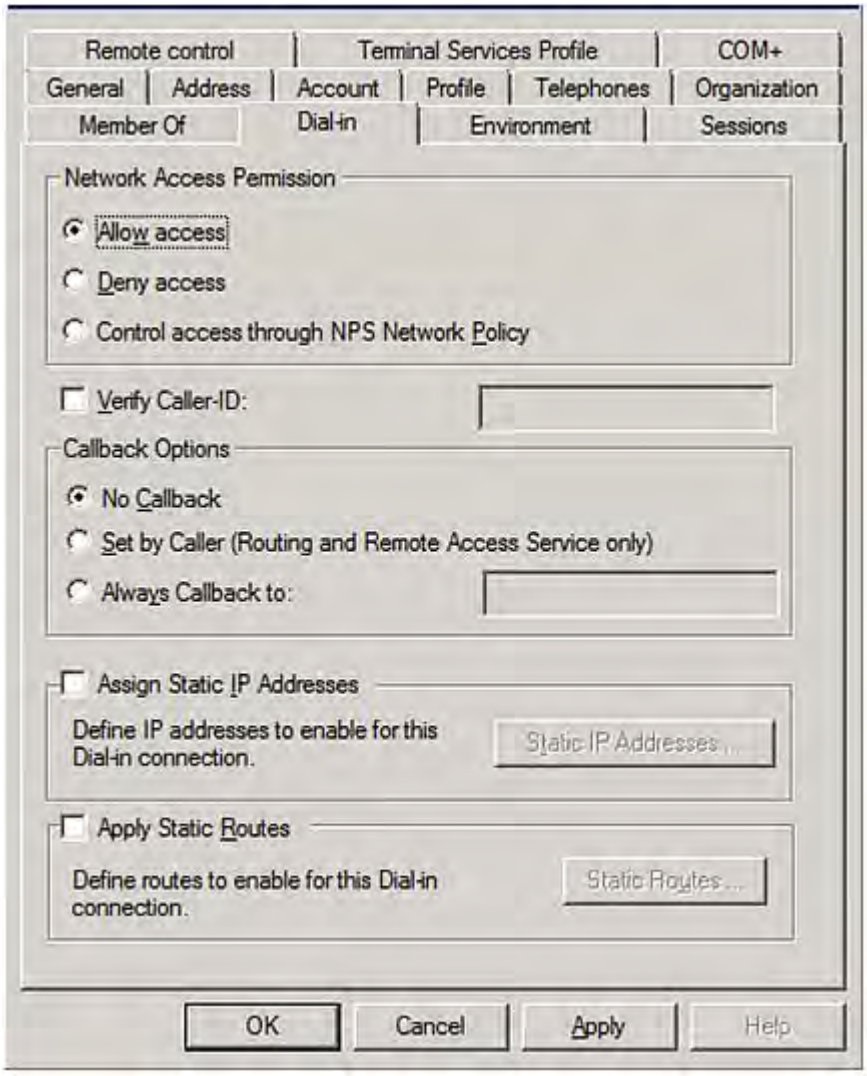
3. Click OK, and then OK again.



To grant PXC/PXO users remote access permission:

1. Open Active Directory Users and Computers.
2. Open the properties dialog of the user whom you want to grant the access permission.

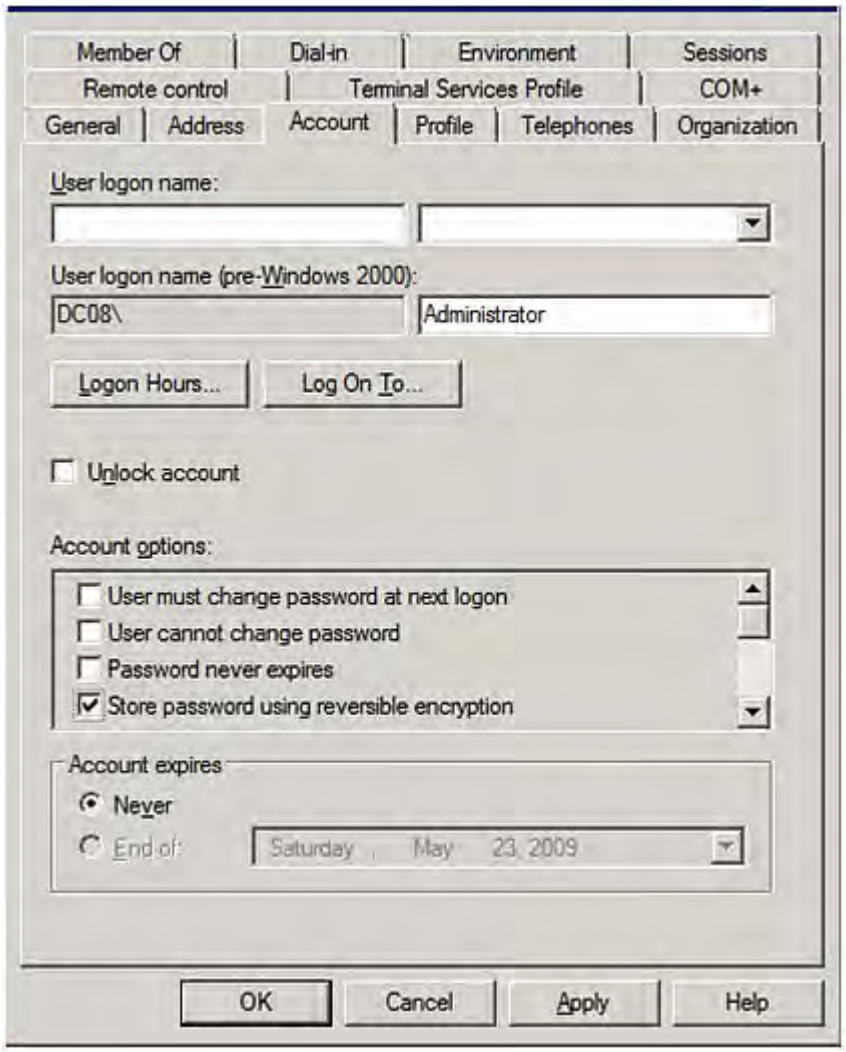
3. Click the Dial-in tab and select the "Allow access" checkbox.



To enable reversible encryption for CHAP authentication:

1. Open Active Directory Users and Computers.
2. Open the properties dialog of the user that you want to configure.

3. Click the Account tab and select the "Store password using reversible encryption" checkbox.



Appendix J Additional PXC/PXO Information

In This Chapter

Reserving IP Addresses in DHCP Servers 672
Sensor Threshold Settings 676
Default Voltage and Current Thresholds 684
Altitude Correction Factors 686
Unbalanced Current Calculation 686
Ways to Probe Existing User Profiles 688
Role of a DNS Server 688
Cascading Troubleshooting 688
Installing the USB-to-Serial Driver (Optional) 693
Initial Network Configuration via CLI 694
Device-Specific Settings 701
TLS Certificate Chain 702
Browsing through the Online Help 708

Reserving IP Addresses in DHCP Servers

PXC/PXO uses its serial number as the client identifier in the DHCP request. Therefore, to successfully reserve an IP address for the PXC/PXO in a DHCP server, use the PXC/PXO device's serial number as the unique ID instead of the MAC address.

Since all network interfaces of the PXC/PXO 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 PXC/PXO 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 672).

In the following illustration, it is assumed that the PXC/PXO serial number is PEG1A00003.

Windows IP address reservation illustration:

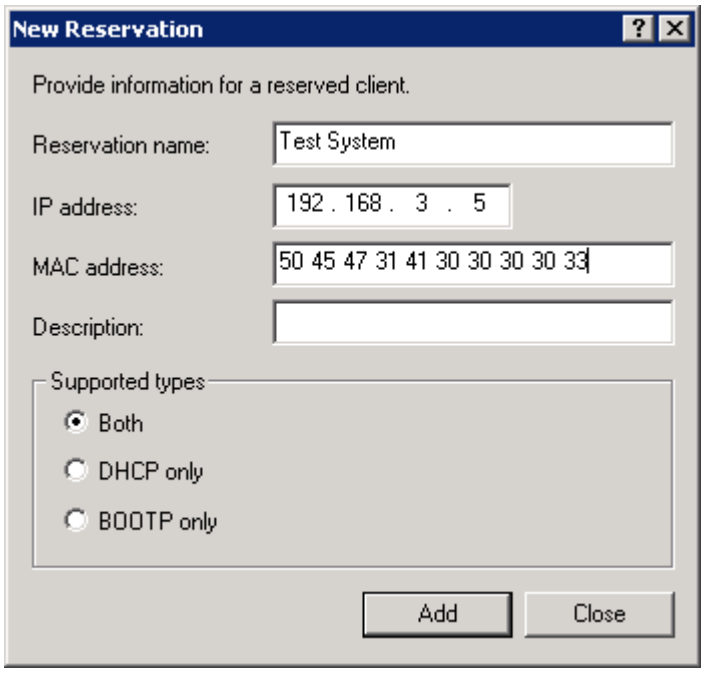
1. Convert the client identifier of the desired network interface into ASCII codes (*hexadecimal*).

Interface	Client identifier conversion
ETH1	PEG1A00003 = 50 45 47 31 41 30 30 30 30 33
ETH2	PEG1A00003-**ETH2** = 50 45 47 31 41 30 30 30 30 33 **2D 45 54 48 32** ▪ The suffix comprising the dash symbol and the word "ETH2" is also converted.
WIRELESS	PEG1A00003-**WIRELESS** = 50 45 47 31 41 30 30 30 30 33 **2D 57 49 52 45 4C 45 53 53** ▪ The suffix comprising the dash symbol and the word "WIRELESS" is also converted.
BRIDGE	PEG1A00003 = 50 45 47 31 41 30 30 30 30 33

2. In your DHCP server, bring up the New Reservation dialog, and separate the converted ASCII codes with spaces.

   For example, to reserve the ETH1 interface's IP address, enter the following data in the dialog.

Field	Data entered
IP address	The IP address you want to reserve.
MAC address	The following ASCII codes. `50 45 47 31 41 30 30 30 30 33`
Other fields	Configure as needed.



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 672).

In the following illustrations, it is assumed that the PXC/PXO 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.

Interface	Client identifier conversion
WIRELESS	PEG1A00003-**WIRELESS** = 50 45 47 31 41 30 30 30 30 33 **2D 57 49 52 45 4C 45 53 53** ▪ The suffix comprising the dash symbol and the word "WIRELESS" is also converted.
BRIDGE	PEG1A00003 = 50 45 47 31 41 30 30 30 30 33

2. Separate the converted ASCII codes with a colon, and a prefix "00:" must be added to the beginning of the converted codes.

   For example, the *converted* client identifier of the ETH1 interface looks like the following:

   `00:50:45:47:31:41:30:30:30:30:33`

3. Now enter the converted client identifier with the following syntax.

```
host mypx {
option dhcp-client-identifier = 00:50:45:47:31:41:30:30:30:30:33;
fixed-address 192.168.20.1;
}
```

Illustration without ASCII code conversion:

1. Use the original client identifier of the desired network interface. DO NOT convert them into ASCII codes.
2. A prefix "\000" must be added to the beginning of the client identifier.

   For example, the client identifier of the ETH1 interface looks like the following:

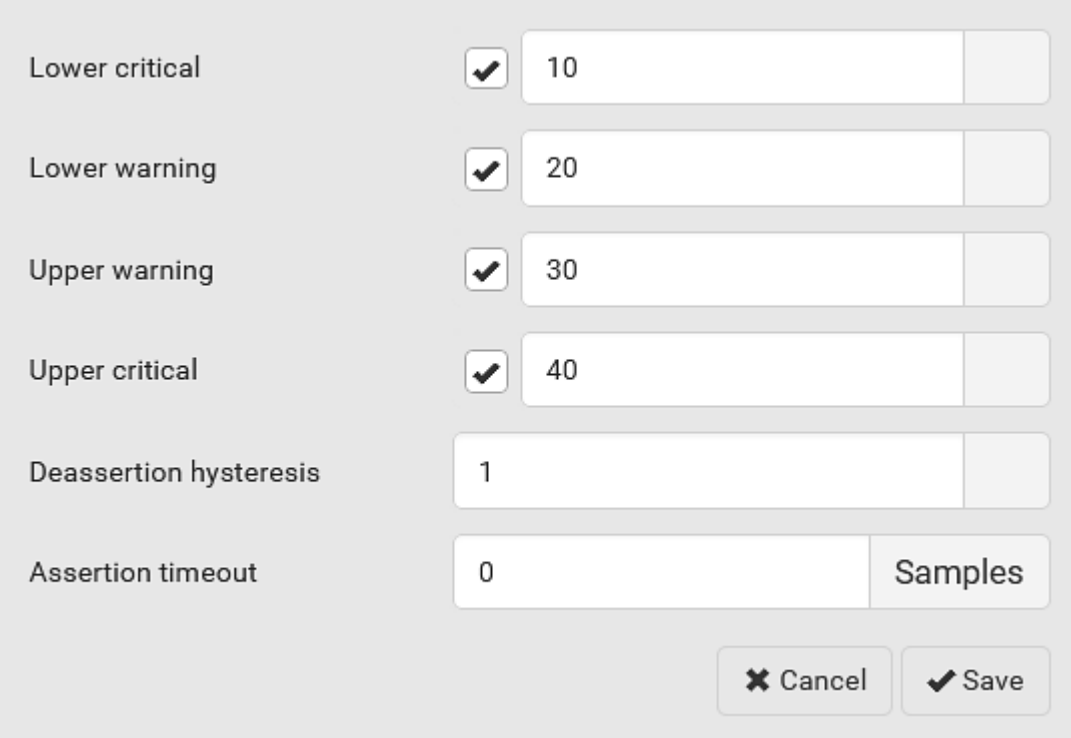
   `\000PEG1A00003`

3. Now enter the original client identifier with the following syntax. The client identifier is enclosed in quotation marks.

```
host mypx {
option dhcp-client-identifier = "\000PEG1A00003";
fixed-address 192.168.20.1;
}
```

Sensor Threshold Settings

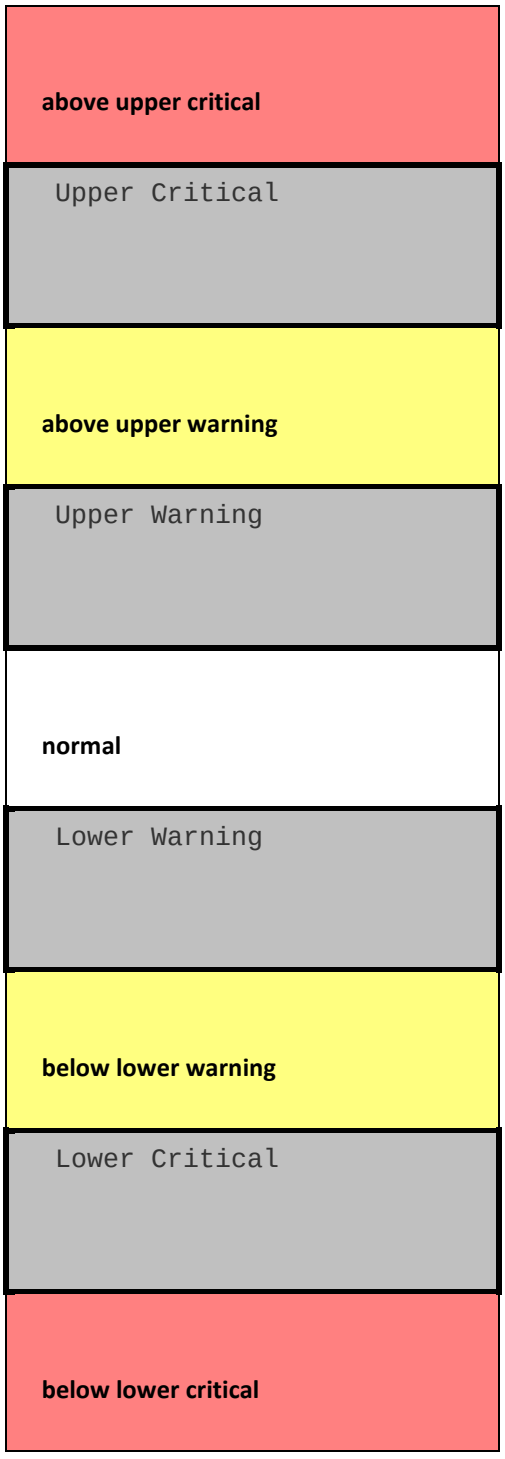
This section explains the thresholds settings for a numeric sensor.



Thresholds and Sensor States

A numeric sensor has four thresholds: Lower Critical, Lower Warning, Upper Warning and Upper Critical.

The threshold settings determine how many sensor states are available for a certain sensor and the range of each sensor state. The diagram below shows how each threshold relates to each state.



▶ **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 160).

Raritan
A brand of legrand

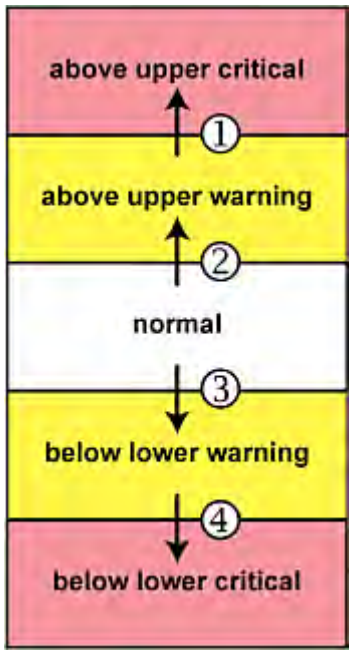
"To Assert" and Assertion Timeout

If multiple sensor states are available for a specific sensor, the PXC/PXO 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 PXC/PXO 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 PXC/PXO triggers the "assertion" action. If that sensor changes its state again within the specified wait time, the PXC/PXO 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 PXC/PXO 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 PXC/PXO 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 PXC/PXO performs the "assertion" action to announce the "above upper warning" state.
- If the temperature drops below 25 degrees Celsius within 5 seconds, the PXC/PXO does NOT perform the "assertion" action.

Raritan
A brand of legrand

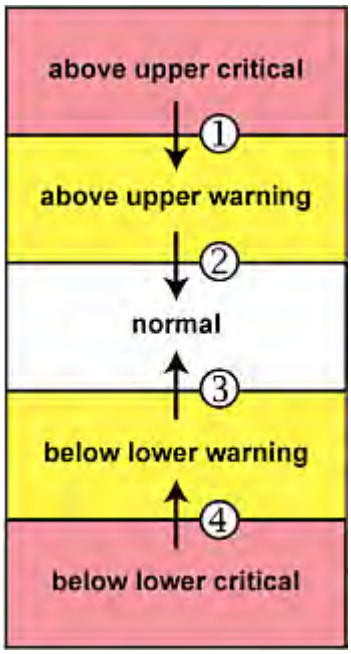
"To De-assert" and Deassertion Hysteresis

After the PXC/PXO 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 PXC/PXO 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:

Lower Critical
0
Lower Warning
0
Upper Warning
0
Upper Critical
0
Deassertion Hysteresis
0
Assertion Timeout
0
Samples
Cancel
Save

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 PXC/PXO to de-assert the worse state for a sensor only when that sensor's reading reaches the pre-determined "deassertion" level.

For upper thresholds, this "deassertion" level is a decrease against each threshold. For lower thresholds, this level is an increase to each threshold. The absolute value of the decrease/increase is exactly the hysteresis value.

For example, if Deassertion Hysteresis = 2, then the deassertion level of each threshold is either "+2" or "-2" as illustrated below.

Threshold value	Deassertion value
Upper Critical = 33	Deassertion level = 31 • 33 - 2 = 31
Upper Warning = 25	Deassertion level = 23 • 25 - 2 = 23
Lower Critical = 10	Deassertion level = 12 • 10 + 2 = 12
Lower Warning = 18	Deassertion level = 20 • 18 + 2 = 20

To use each threshold as the "deassertion" level instead of determining a new level, set the Deassertion Hysteresis to 0 (zero).

Note: The difference between Upper Warning and Lower Warning must be at least "two times" of the deassertion value.

How "Deassertion Hysteresis" is helpful:

If you have created an event rule that instructs the PXC/PXO 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 PXC/PXO 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 PXC/PXO does NOT perform the "deassertion" action.
- If the temperature drops to 17 degrees Celsius or lower, the PXC/PXO 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 Raritan 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

Raritan
A brand of legrand

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

- **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 Raritan differential air pressure sensor is attached to your device, the altitude you enter for the device can serve as an altitude correction factor. That is, the reading of the differential air pressure sensor will be multiplied by the correction factor to get a correct reading.

This table shows the relationship between different altitudes and correction factors.

Altitude (meters)	Altitude (feet)	Correction factor
0	0	0.95
250	820	0.98
425	1394	1.00
500	1640	1.01
740	2428	1.04
1500	4921	1.15
2250	7382	1.26
3000	9842	1.38

Unbalanced Current Calculation

Unbalanced current information is available on 3-phase models only. This section explains how PXC/PXO 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 PXC/PXO.

- 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 PXC/PXO may fail to connect to the given host.

Therefore, DNS server settings are important for external authentication. With appropriate DNS settings, the PXC/PXO 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 239).

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 PXC/PXO to a computer if network access to that PXC/PXO fails. See ***Connecting the PXC/PXO to a Computer*** (on page 21).

Raritan
A brand of legrand

Symptom	Probable cause
Failure to access the master device	• Anything below is lost or loose on the master device: ▪ Network connection ▪ Power supply • Anything below is disabled on the master device: ▪ The Ethernet or wireless interface ▪ IPv4 or IPv6 settings • In the Port Forwarding mode, related settings are incorrectly configured on the master device. ▪ The master device's role is incorrectly set to 'Slave'. ▪ The interface where the network is connected is incorrectly set as the downstream interface. • For the wireless networking, one of the following issues occurs: ▪ The USB wireless LAN adapter attached to the master device is not the Raritan USB WIFI LAN adapter. See ***USB Wireless LAN Adapters*** (on page 13). ▪ The wireless LAN configuration is not supported. See ***Supported Wireless LAN Configuration*** (on page 13). ▪ The installed CA certificate chain contains any certificate that has expired or is not valid yet.

Symptom	Probable cause
Failure to access a slave device	• One of the following issues occurs on the master device: ▪ Network connection is lost. ▪ Power is lost. ▪ The Ethernet or wireless interface is disabled. • One of the following issues occurs on the slave device in question or any upstream device (if available): ▪ Connection of the cascading cable is loose or lost. ▪ No power supply. ▪ The cascading mode is set incorrectly. For example, the master device is set to Bridging, but the slave device in question or any upstream device is set to Port Forwarding. • In the Bridging mode, IPv4 (or IPv6) settings are disabled on the slave device in question. • In the Port Forwarding mode, one of the following issues occurs: ▪ The master device's role is incorrectly set to 'Slave'. ▪ The master device's downstream interface is incorrectly set. For example, you use a USB cable to connect the 1st slave device, but select the Ethernet port as the downstream interface. ▪ The role of the slave device in question or any upstream device is set to 'Master' instead of 'Slave'. ▪ The port number you added to the IP address is incorrect. See ***Port Number Syntax*** (on page 211). ▪ 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 PXC/PXO may be the failure point of network, you may ping each PXC/PXO in the cascading chain, or check the slave-related events in the event log of each PXC/PXO. See **The Ping Tool** *(on page 692) and* **Slave Device Events in the Log** *(on page 691).*

For a cascading chain comprising only products with "dual" Ethernet ports, also check the following:

- Whether the Ethernet interface (ETH1 or ETH2) where the network or cascading cable is connected is disabled on the cascaded device in question or any upstream device.
- Whether the connection complies with the cascading guidelines, when set to the Port Forwarding mode. See ***Restrictions of Port-Forwarding Connections*** (on page 31).
- Whether a newer product model, if involved in the chain, runs the appropriate minimum firmware version or later.

Slave Device Events in the Log

The log messages for connection/disconnection of a cascaded device are different for USB-cascading and Ethernet-cascading chains.

Messages for the Ethernet-cascading chain:

Whenever the connection or disconnection of a master/slave device is detected, both PXC/PXO devices connected via that network cable record this event in their internal logs.

There are two slave-related events:

Event	Description
The ETH1/2 network interface link is now up.	This log entry is generated when the PXC/PXO 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 PXC/PXO 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 PXC/PXO at the USB-A end of the USB cable logs it in the internal log. Note that the PXC/PXO 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 PXC/PXO 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 PXC/PXO provides a ping tool in the web interface and CLI so you can ping any host or PXC/PXO in your data center.

Ping via the Web Interface:

To log in to the web interface, see ***Login*** (on page 96).

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 PXC/PXO or using SSH/Telnet. See ***With SSH or Telnet*** (on page 388).

1. You must perform the ping command in the diagnostic mode. See ***Entering Diagnostic Mode*** (on page 554).
2. Then perform the ping command. See ***Testing the Network Connectivity*** (on page 556).

Raritan
A brand of legrand

Installing the USB-to-Serial Driver (Optional)

The PXC/PXO 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 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 PXC/PXO 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 PXC/PXO to the computer via a USB cable. The driver is automatically installed.

Manual driver installation in Windows®:

1. Make sure the PXC/PXO 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 PXC/PXO 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 PXC/PXO 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 PXC/PXO 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 190).

To configure the PXC/PXO:

1. On the computer connected to the PXC/PXO, 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 PXC/PXO.
3. The PXC/PXO 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.

Raritan
A brand of legrand

- To change it, follow onscreen instructions to type your new password.
- To ignore it, simply press Enter.

5. The # prompt appears.
6. Type `config` and press Enter.
7. To configure network settings, type appropriate commands and press Enter. Refer to the following commands list. CLI commands are case sensitive.
8. After finishing the network settings, type `apply` to save changes. To abort, type `cancel`.

Commands for wired networking:

The <ipvX> variable in the following commands is either ipv4 *or* ipv6*, depending on the type of IP protocol you are configuring.*

Replace the variable <ETH> with either 'ETH1' or 'ETH2', depending on which Ethernet port you are configuring.

- **General IP settings:**

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

- **Static IP configuration:**

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

Commands for "Ethernet" authentication method:

To set or enable	Use this command
Authentication method	`network ethernet <ETH> authMethod <method>` <method> = *none* or *eap*
EAP outer authentication	`network ethernet <ETH> eapOuterAuthentication <outer_auth>` <outer_auth> = *PEAP* or *TLS*
EAP inner authentication	`network ethernet <ETH> eapInnerAuthentication <inner_auth>` <inner_auth> = *MSCHAPv2* or *TLS*

Raritan
A brand of legrand

To set or enable	Use this command
EAP identity	`network ethernet <ETH> eapIdentity <identity>` <identity> = your user name for EAP authentication
EAP TLS client certificate	`network ethernet <ETH> eapClientCertificate` When prompted to enter the client certificate, open the certificate with a text editor, copy and paste the content into the communications program.
EAP TLS client private key	`network ethernet <ETH> eapClientPrivateKey` When prompted to enter the private key, open the key with a text editor, copy and paste the content into the communications program.
EAP password	`network ethernet <ETH> eapPassword` When prompted to enter the password for EAP authentication, type the password.
EAP CA certificate	`network ethernet <ETH> eapCACertificate` When prompted to enter the CA certificate, open the certificate with a text editor, copy and paste the content into the communications program.
Radius authentication server's name	`network ethernet <ETH> eapAuthServerName <FQDN>` <FQDN> = Fully qualified domain name of the Radius server name shown in the CA certificate

Note: When copying the content from the CA certificate start with and include the line containing "BEGIN CERTIFICATE" and copy everything through the final line containing "END CERTIFICATE." If a certificate is installed, configure the following:

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

Commands for wireless networking:

- **General wireless settings**:

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

Raritan
A brand of legrand

To set or enable	Use this command
802.11n protocol	`network wireless enableHT <option>` <option> = *true*, or *false*
Wireless authentication method	`network wireless authMethod <method>` <method> = *psk* or *eap*
PSK	`network wireless PSK <psk>` <psk> = PSK string
Wireless EAP outer authentication	`network wireless eapOuterAuthentication <outer_auth>` <outer_auth> = *PEAP* or *TLS*
Wireless EAP inner authentication	`network wireless eapInnerAuthentication <inner_auth>` <inner_auth> = *MSCHAPv2* or *TLS*
Wireless EAP identity	`network wireless eapIdentity <identity>` <identity> = your user name for EAP authentication
Wireless EAP TLS client certificate	`network wireless eapClientCertificate` When prompted to enter the client certificate, open the certificate with a text editor, copy and paste the content into the communications program.
Wireless EAP TLS client private key	`network wireless eapClientPrivateKey` When prompted to enter the private key, open the key with a text editor, copy and paste the content into the communications program.

To set or enable	Use this command
Wireless EAP password	`network wireless eapPassword` When prompted to enter the password for EAP authentication, type the password.
Wireless EAP CA certificate	`network wireless eapCACertificate` When prompted to enter the CA certificate, open the certificate with a text editor, copy and paste the content into the communications program.
Radius authentication server's name for wireless connection	`network wireless eapAuthServerName <FQDN>` <FQDN> = Fully qualified domain name of the Radius server name shown in the CA certificate

Note: When copying the certificate, select and copy the content including the starting line containing "BEGIN CERTIFICATE" and the ending 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*

Raritan
A brand of legrand

- **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
- 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 702).
- For an example of creating and uploading a TLS certificate to PXC/PXO, see ***Illustration - GMAIL SMTP Certificate Chain*** (on page 706).

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 706).

A certificate or a chain of certificates is used for trusting a TLS server that you want to connect.

The receiver, such as PXC/PXO, can trust a TLS server only after an appropriate certificate (chain) which is "related to" that TLS server's certificate is uploaded to the receiver.

How a certificate chain is generated:

To explain how a TLS server's certificate is "related to" the certificate (chain) that is uploaded to the receiver, we assume that there are three "related" certificates.

- **Certificate C**. The certificate issued to the TLS server you want to connect.

  'Certificate C' is issued by the certificate authority (CA) entity called 'Issuer B'.
- **Certificate B**. The certificate issued to 'Issuer B'.

  'Certificate B' is issued by a CA entity called 'Issuer A', and it is an intermediate certificate.

Raritan
A brand of legrand

- **Certificate A**. The self-signed certificate issued by Issuer A. Issuer A is a root CA.

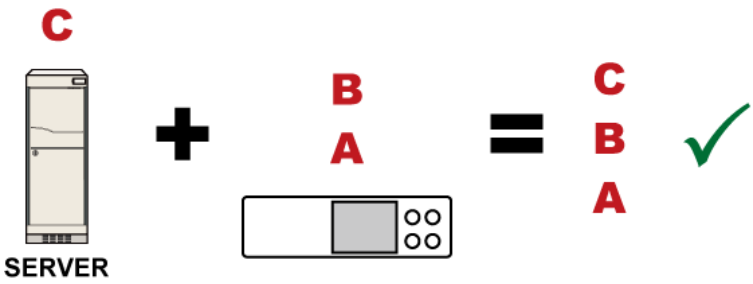
The above three certificates form a certificate path, which is called the "certificate chain".

Each certificate in the chain is the issuer certificate of the certificate that follows it. That is, A is the issuer certificate of B, and B is the issuer certificate of C.

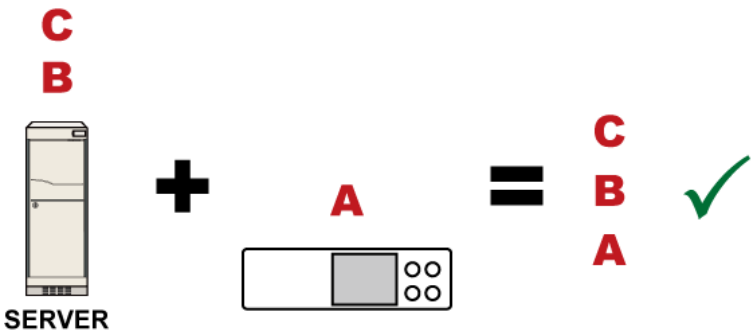
Note: In fact many certificate chains may comprise only the root certificate and a TLS server's certificate and do not have any intermediate certificate(s) like 'Certificate B' involved. Or some chains may contain more than one intermediate certificates.

Certificate (chain) that you must upload to the receiver, such as PXC/PXO:

Because the TLS server provides only 'Certificate C', you need to upload a file containing the missing certificates of the chain (that is, 'Certificate A' and 'Certificate B') to the receiver.

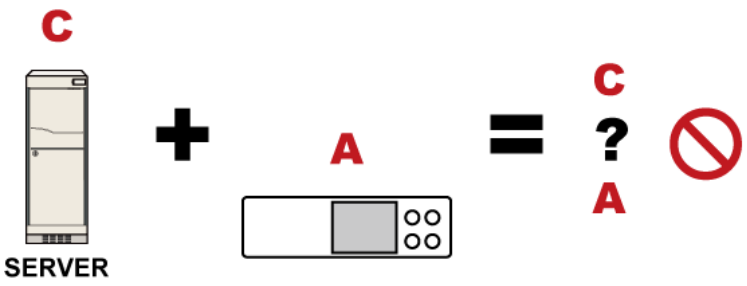


In reality some servers may provide a partial (or even a full) certificate chain instead of a single server certificate. If your server provides a partial certificate chain containing 'Certificate B' and 'Certificate C', then you only need to upload 'Certificate A" to the receiver. If the server has a full certificate chain containing Certificates 'A', 'B', and 'C', then you also need to upload the root certificate 'A".



Warning: The certificate (chain) uploaded to the receiver must always contain the ROOT certificate even though the TLS server provides the root certificate. When uploading a (partial) chain onto the PXC/PXO, it means you trust each certificate in the chain to certify the authenticity of certificates a server sends to PXC/PXO. 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.



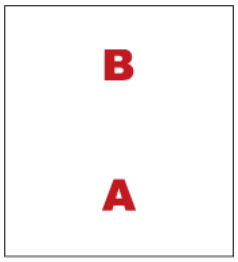
Raritan
A brand of legrand

For PXC/PXO, if any required certificate is missing, a certificate error message similar to the following is shown on the PXC/PXO 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 PXC/PXO, ignore this GMAIL illustration topic. Simply contact your IT department to retrieve the appropriate certificate (chain) file and upload it to the PXC/PXO.

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
.
.
```


Raritan
A brand of legrand

```
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 begins with the line "BEGIN CERTIFICATE" and ends with the line "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 PXC/PXO.
   - If not, you need to find all missing issuer certificates, including the root certificate, and upload them to PXC/PXO.

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 PXC/PXO:

1. Paste the root certificate's content into a plain text file that will be uploaded to PXC/PXO.
   - 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 PXC/PXO 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 702).*

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 PXC/PXO 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 PXC/PXO online help:

1. Click Online Documentation. See ***Web Interface Overview*** (on page 100).
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.

Raritan
A brand of legrand

- 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 Raritan, click the "Send feedback" icon .
11. To print the currently selected topic, click the "Print this page" icon .

Appendix K Integration

The PXC/PXO can work with certain Raritan or third-party products to provide diverse power solutions.

In This Chapter

Connection to Raritan Serial Access Products 710
Power IQ Configuration 710
dcTrack.....711

Connection to Raritan Serial Access Products

PXC/PXO supports the integration with Raritan's serial access products - Dominion SX and Dominion SX II.

You can access the CLI of the PXC/PXO via SX / SX II.

To only access the CLI of the PXC/PXO via SX / SX II, treat the PXC/PXO 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 PXC/PXO is categorized as a power item in dcTrack. dcTrack offers an import wizard for conveniently adding the PXC/PXO 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.

Raritan
A brand of legrand

Appendix L Third Party Licenses

This appendix contains third party licenses for software used by Xerus that require including the license in documentation.

For information on open source software, see raritan.com/about-us/legal/open-source-software-statement

In This Chapter

Licenses - Bind9 713
Licenses - Clish 723
Licenses - Dropbear 731
Licenses - FreeType 734
Licenses - IW 736
Licenses - JSON-C 737
Licenses - LIBTIRPC 738
Licenses - LIBXML2 738
Licenses - Mbus 739
Licenses - Net-SNMP 739
Licenses - Open LDAP 748
Licenses - OpenSSL 750
Licenses - Wireless-RegDB 753
Licenses - WPA Supplicant and Hostapd 753

Licenses - Bind9

Copyright (C) 2004-2016 Internet Systems Consortium, Inc. ("ISC")

Copyright (C) 1996-2003 Internet Software Consortium.

Permission to use, copy, modify, and/or distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Portions of this code release fall under one or more of the following Copyright notices. Please see individual source files for details.

For binary releases also see: OpenSSL-LICENSE.

Copyright (C) 1996-2001 Nominum, Inc.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND NOMINUM DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL NOMINUM BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Copyright (C) 1995-2000 by Network Associates, Inc.

Permission to use, copy, modify, and/or distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC AND NETWORK ASSOCIATES DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Copyright (C) 2002 Stichting NLnet, Netherlands, stichting@nlnet.nl.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND STICHTING NLNET DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL STICHTING NLNET BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

The development of Dynamically Loadable Zones (DLZ) for Bind 9 was conceived and contributed by Rob Butler.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ROB BUTLER DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL ROB BUTLER BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Copyright (c) 1987, 1990, 1993, 1994

The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (C) The Internet Society 2005. This version of this module is part of RFC 4178; see the RFC itself for full legal notices.

(The above copyright notice is per RFC 3978 5.6 (a), q.v.)

Copyright (c) 2004 Masarykova universita

(Masaryk University, Brno, Czech Republic)

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 1997 - 2003 Kungliga Tekniska Hogskolan

(Royal Institute of Technology, Stockholm, Sweden).

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of the Institute nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE INSTITUTE AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE INSTITUTE OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 1998 Doug Rabson

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright ((c)) 2002, Rice University

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of Rice University (RICE) nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

This software is provided by RICE and the contributors on an "as is" basis, without any representations or warranties of any kind, express or implied including, but not limited to, representations or warranties of non-infringement, merchantability or fitness for a particular purpose. In no event shall RICE or contributors be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data, or profits; or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this software, even if advised of the possibility of such damage.

Copyright (c) 1993 by Digital Equipment Corporation.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies, and that the name of Digital Equipment Corporation not be used in advertising or publicity pertaining to distribution of the document or software without specific, written prior permission.

THE SOFTWARE IS PROVIDED "AS IS" AND DIGITAL EQUIPMENT CORP. DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL DIGITAL EQUIPMENT CORPORATION BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Copyright 2000 Aaron D. Gifford. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of the copyright holder nor the names of contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR(S) AND CONTRIBUTOR(S) ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR(S) OR CONTRIBUTOR(S) BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 1998 Doug Rabson.

Copyright (c) 2001 Jake Burkholder.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (C) 1995, 1996, 1997, and 1998 WIDE Project.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of the project nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE PROJECT AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PROJECT OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 1999-2000 by Nortel Networks Corporation

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND NORTEL NETWORKS DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL NORTEL NETWORKS BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Copyright (c) 2000-2002 Japan Network Information Center. All rights reserved.

By using this file, you agree to the terms and conditions set forth bellow.

LICENSE TERMS AND CONDITIONS

The following License Terms and Conditions apply, unless a different license is obtained from Japan Network Information Center ("JPNIC"), a Japanese association, Kokusai-Kougyou-Kanda Bldg 6F, 2-3-4 Uchi-Kanda, Chiyoda-ku, Tokyo 101-0047, Japan.

1. Use, Modification and Redistribution (including distribution of any modified or derived work) in source and/or binary forms is permitted under this License Terms and Conditions.

2. Redistribution of source code must retain the copyright notices as they appear in each source code file, this License Terms and Conditions.

3. Redistribution in binary form must reproduce the Copyright Notice, this License Terms and Conditions, in the documentation and/or other materials provided with the distribution. For the purposes of binary distribution the "Copyright Notice" refers to the following language:

"Copyright (c) 2000-2002 Japan Network Information Center. All rights reserved."

4. The name of JPNIC may not be used to endorse or promote products derived from this Software without specific prior written approval of JPNIC.

5. Disclaimer/Limitation of Liability: THIS SOFTWARE IS PROVIDED BY JPNIC "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL JPNIC BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Copyright (C) 2004 Nominet, Ltd.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND NOMINET DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Portions Copyright RSA Security Inc.

License to copy and use this software is granted provided that it is identified as "RSA Security Inc. PKCS #11 Cryptographic Token Interface (Cryptoki)" in all material mentioning or referencing this software.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Security Inc. PKCS #11 Cryptographic Token Interface (Cryptoki)" in all material mentioning or referencing the derived work.

RSA Security Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

Copyright (c) 1996, David Mazieres <dm@uun.org>

Copyright (c) 2008, Damien Miller <djm@openbsd.org>

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Copyright (c) 2000-2001 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.OpenSSL.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact licensing@OpenSSL.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.OpenSSL.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 1995, 1997, 1998 The NetBSD Foundation, Inc.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE NETBSD FOUNDATION, INC. AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE FOUNDATION OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Licenses - Clish

This package contains code which is copyrighted to multiple sources. The initial public release of this software was developed by Graeme McKerrell whilst in the employment of 3Com Europe Ltd.

Copyright (c) 2005, 3Com Corporation

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of 3Com Corporation nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Newport Networks Ltd.

The 0.6-0.7 releases of this software was developed by Graeme McKerrell whilst in the employment of Newport Networks Ltd.

As well as enhancing the existing code the following new modules were developed.

Copyright (c) 2005,2006, Newport Networks Ltd

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of Newport Networks Ltd nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

tinyxml

Yves Berquin

As of release 0.6 the tinyxml library is included (unchanged) as part of the distribution.

tinyxml (v2.5.1)

http://www.sourceforge.net/projects/tinyxml

Original file by Yves Berquin.

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

GNU binutils

As of release 0.7.1 libbfd can be used to resolve symbols forstacktraces. This feature can be turned off if linking with GPL code is problematic, using "configure --without-gpl".

The Binary File Descriptor library is part of GNU binutils

http://www.gnu.org/software/binutils/

The following file is licensed under the GPLv2.

This file is part of the CLISH project http://clish.sourceforge.net/

The code in this file is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; version 2

This code is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA.

Derived from addr2line.c in the GNU binutils package by Ulrich.Lauther@mchp.siemens.de

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or, b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or, c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Licenses - Dropbear

Dropbear contains a number of components from different sources, hence there are a few licenses and authors involved. All licenses are fairly non-restrictive.

The majority of code is written by Matt Johnston, under the license below.

Portions of the client-mode work are (c) 2004 Mihnea Stoenescu, under the same license:

Copyright (c) 2002-2015 Matt Johnston

Portions copyright (c) 2004 Mihnea Stoenescu

All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

=====

LibTomCrypt and LibTomMath are written by Tom St Denis, and are Public Domain.

=====

sshpty.c is taken from OpenSSH 3.5p1,

Copyright (c) 1995 Tatu Ylonen <ylo@cs.hut.fi>, Espoo, Finland

All rights reserved

"As far as I am concerned, the code I have written for this software can be used freely for any purpose. Any derived versions of this software must be clearly marked as such, and if the derived work is incompatible with the protocol description in the RFC file, it must be called by a name other than "ssh" or "Secure Shell". "

=====

loginrec.c

loginrec.h

atomicio.h

atomicio.c

and strlcat() (included in util.c) are from OpenSSH 3.6.1p2, and are licensed under the 2 point BSD license.

loginrec is written primarily by Andre Lucas, atomicio.c by Theo de Raadt.

strlcat() is (c) Todd C. Miller

=====

Import code in keyimport.c is modified from PuTTY's import.c, licensed as follows:

PuTTY is copyright 1997-2003 Simon Tatham.

Portions copyright Robert de Bath, Joris van Rantwijk, Delian Delchev, Andreas Schultz, Jeroen Massar, Wez Furlong, Nicolas Barry, Justin Bradford, and CORE SDI S.A.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

=====

curve25519-donna:

/* Copyright 2008, Google Inc.

* All rights reserved.

*

* Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

*

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

* curve25519-donna: Curve25519 elliptic curve, public key function

* http://code.google.com/p/curve25519-donna/

* Adam Langley <agl@imperialviolet.org>

* Derived from public domain C code by Daniel J. Bernstein <djb@cr.yp.to>

* More information about curve25519 can be found here

* http://cr.yp.to/ecdh.html

* djb's sample implementation of curve25519 is written in a special assembly language called qhasm and uses the floating point registers.

* This is, almost, a clean room reimplementation from the curve25519 paper. It uses many of the tricks described therein. Only the crecip function is taken from the sample implementation.

Licenses - FreeType

The FreeType Project LICENSE

2006-Jan-27

Copyright 1996-2002, 2006 by

David Turner, Robert Wilhelm, and Werner Lemberg

Introduction

==========

The FreeType Project is distributed in several archive packages; some of them may contain, in addition to the FreeType font engine, various tools and contributions which rely on, or relate to, the FreeType Project.

This license applies to all files found in such packages, and which do not fall under their own explicit license. The license affects thus the FreeType font engine, the test programs, documentation and makefiles, at the very least.

This license was inspired by the BSD, Artistic, and IJG (Independent JPEG Group) licenses, which all encourage inclusion and use of free software in commercial and freeware products alike. As a consequence, its main points are that:

o We don't promise that this software works. However, we will be interested in any kind of bug reports. (`as is' distribution)

o You can use this software for whatever you want, in parts or full form, without having to pay us. (`royalty-free' usage)

o You may not pretend that you wrote this software. If you use it, or only parts of it, in a program, you must acknowledge somewhere in your documentation that you have used the FreeType code. (`credits')

We specifically permit and encourage the inclusion of this software, with or without modifications, in commercial products.

We disclaim all warranties covering The FreeType Project and assume no liability related to The FreeType Project.

Finally, many people asked us for a preferred form for a credit/disclaimer to use in compliance with this license. We thus encourage you to use the following text:

Portions of this software are copyright <year> The FreeType Project (www.freetype.org). All rights reserved.

Please replace <year> with the value from the FreeType version you actually use.

Legal Terms

==========

0. Definitions

Throughout this license, the terms `package', `FreeType Project', and `FreeType archive' refer to the set of files originally distributed by the authors (David Turner, Robert Wilhelm, and Werner Lemberg) as the `FreeType Project', be they named as alpha, beta or final release.

`You' refers to the licensee, or person using the project, where `using' is a generic term including compiling the project's source code as well as linking it to form a `program' or `executable'.

This program is referred to as `a program using the FreeType engine'.

This license applies to all files distributed in the original FreeType Project, including all source code, binaries and documentation, unless otherwise stated in the file in its original, unmodified form as distributed in the original archive.

If you are unsure whether or not a particular file is covered by this license, you must contact us to verify this.

The FreeType Project is copyright (C) 1996-2000 by David Turner, Robert Wilhelm, and Werner Lemberg. All rights reserved except as specified below.

1. No Warranty

THE FREETYPE PROJECT IS PROVIDED `AS IS' WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT WILL ANY OF THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY DAMAGES CAUSED BY THE USE OR THE INABILITY TO USE, OF THE FREETYPE PROJECT.

2. Redistribution

This license grants a worldwide, royalty-free, perpetual and irrevocable right and license to use, execute, perform, compile, display, copy, create derivative works of, distribute and sublicense the FreeType Project (in both source and object code forms) and derivative works thereof for any purpose; and to authorize others to exercise some or all of the rights granted herein, subject to the following conditions:

o Redistribution of source code must retain this license file (`FTL.TXT') unaltered; any additions, deletions or changes to the original files must be clearly indicated in accompanying documentation. The copyright notices of the unaltered, original files must be preserved in all copies of source files.

o Redistribution in binary form must provide a disclaimer that states that the software is based in part of the work of the FreeType Team, in the distribution documentation. We also encourage you to put an URL to the FreeType web page in your documentation, though this isn't mandatory.

These conditions apply to any software derived from or based on the FreeType Project, not just the unmodified files. If you use our work, you must acknowledge us. However, no fee need be paid to us.

3. Advertising

Neither the FreeType authors and contributors nor you shall use the name of the other for commercial, advertising, or promotional purposes without specific prior written permission.

We suggest, but do not require, that you use one or more of the following phrases to refer to this software in your documentation or advertising materials: `FreeType Project', `FreeType Engine', `FreeType library', or `FreeType Distribution'.

As you have not signed this license, you are not required to accept it. However, as the FreeType Project is copyrighted material, only this license, or another one contracted with the

authors, grants you the right to use, distribute, and modify it. Therefore, by using, distributing, or modifying the FreeType Project, you indicate that you understand and accept all the terms of this license.

4. Contacts

There are two mailing lists related to FreeType:

o freetype@nongnu.org

Discusses general use and applications of FreeType, as well as future and wanted additions to the library and distribution. If you are looking for support, start in this list if you haven't found anything to help you in the documentation.

o freetype-devel@nongnu.org

Discusses bugs, as well as engine internals, design issues, specific licenses, porting, etc.

Our home page can be found at http://www.freetype.org

Licenses - IW

Copyright (c) 2007, 2008 Johannes Berg

Copyright (c) 2007 Andy Lutomirski

Copyright (c) 2007 Mike Kershaw

Copyright (c) 2008-2009 Luis R. Rodriguez

Permission to use, copy, modify, and/or distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Licenses - JSON-C

Copyright (c) 2009-2012 Eric Haszlakiewicz

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Copyright (c) 2004, 2005 Metaparadigm Pte Ltd

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Licenses - LIBTIRPC

Copyright (c) Copyright (c) Bull S.A. 2005 All Rights Reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Licenses - LIBXML2

Except where otherwise noted in the source code (e.g. the files hash.c, list.c and the trio files, which are covered by a similar licence but with different Copyright notices) all the files are:

Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Licenses - Mbus

Copyright (c) 2002-2003, 2013-2019 Victor Antonovich (v.antonovich@gmail.com)

Copyright (c) 2011 Andrew Denysenko <nitr0@seti.kr.ua>

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of the copyright holder nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Licenses - Net-SNMP

Various copyrights apply to this package, listed in various separate parts below. Please make sure that you read all the parts.

Part 1: CMU/UCD copyright notice: (BSD like) -----

Copyright 1989, 1991, 1992 by Carnegie Mellon University

Derivative Work - 1996, 1998-2000

Copyright 1996, 1998-2000 The Regents of the University of California

All Rights Reserved

Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU and The Regents of the University of California not be used in advertising or publicity pertaining to distribution of the software without specific written permission.

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Part 2: Networks Associates Technology, Inc copyright notice (BSD) -----

Copyright (c) 2001-2003, Networks Associates Technology, Inc

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the Networks Associates Technology, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 3: Cambridge Broadband Ltd. copyright notice (BSD) -----

Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

The name of Cambridge Broadband Ltd. may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 4: Sun Microsystems, Inc. copyright notice (BSD) -----

Copyright (c) 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

Use is subject to license terms below.

This distribution may include materials developed by third parties.

Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the Sun Microsystems, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 5: Sparta, Inc copyright notice (BSD) -----

Copyright (c) 2003-2013, Sparta, Inc

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of Sparta, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 6: Cisco/BUPTNIC copyright notice (BSD) -----

Copyright (c) 2004, Cisco, Inc and Information Network

Center of Beijing University of Posts and Telecommunications.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of Cisco, Inc, Beijing University of Posts and Telecommunications, nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS;OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 7: Fabasoft R&D Software GmbH & Co KG copyright notice (BSD) -----

Copyright (c) Fabasoft R&D Software GmbH & Co KG, 2003

oss@fabasoft.com

Author: Bernhard Penz <bernhard.penz@fabasoft.com>

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

The name of Fabasoft R&D Software GmbH & Co KG or any of its subsidiaries, brand or product names may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 8: Apple Inc. copyright notice (BSD) -----

Copyright (c) 2007 Apple Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of Apple Inc. ("Apple") nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY APPLE AND ITS CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL APPLE OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 9: ScienceLogic, LLC copyright notice (BSD) -----

Copyright (c) 2009, ScienceLogic, LLC

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of ScienceLogic, LLC nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 10: Lennart Poettering copyright notice (BSD-like) -----

Copyright 2010 Lennart Poettering

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Part 11: IETF copyright notice (BSD) -----

Copyright (c) 2013 IETF Trust and the persons identified as authors of the code. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. Neither the name of Internet Society, IETF or IETF Trust, nor the names of specific contributors, may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 12: Arista Networks copyright notice (BSD) ----

Copyright (c) 2013, Arista Networks, Inc.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of Arista Networks, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 13: VMware, Inc. copyright notice (BSD) -----

Copyright (c) 2016, VMware, Inc.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of VMware, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR

OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 14: USC/Information Sciences Institute copyright notice (BSD) -----

Copyright (c) 2017-2018, Information Sciences Institute

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of Information Sciences Institue nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Licenses - Open LDAP

Copyright 1998-2019 The OpenLDAP Foundation

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted only as authorized by the OpenLDAP Public License.

A copy of this license is available in the file LICENSE in the top-level directory of the distribution or, alternatively, at <http://www.OpenLDAP.org/license.html>.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

Individual files and/or contributed packages may be copyright by other parties and/or subject to additional restrictions.

This work is derived from the University of Michigan LDAP v3.3 distribution. Information concerning this software is available at <http://www.umich.edu/~dirsvcs/ldap/ldap.html>.

This work also contains materials derived from public sources. Additional information about OpenLDAP can be obtained at <http://www.openldap.org/>.

Portions Copyright 1998-2012 Kurt D. Zeilenga.

Portions Copyright 1998-2006 Net Boolean Incorporated.

Portions Copyright 2001-2006 IBM Corporation.

All rights reserved.

Redistribution and use in source and binary forms, with or without

modification, are permitted only as authorized by the OpenLDAP

Public License.

Portions Copyright 1999-2008 Howard Y.H. Chu.

Portions Copyright 1999-2008 Symas Corporation.

Portions Copyright 1998-2003 Hallvard B. Furuseth.

Portions Copyright 2007-2011 Gavin Henry.

Portions Copyright 2007-2011 Suretec Systems Ltd.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that this notice is preserved. The names of the copyright holders may not be used to endorse or promote products derived from this software without their specific prior written permission. This software is provided "as is'' without express or implied warranty.

Portions Copyright (c) 1992-1996 Regents of the University of Michigan.

All rights reserved.

Redistribution and use in source and binary forms are permitted provided that this notice is preserved and that due credit is given to the University of Michigan at Ann Arbor. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission. This software is provided ``as is'' without express or implied warranty.

The OpenLDAP Public License

Version 2.8, 17 August 2003

Redistribution and use of this software and associated documentation ("Software"), with or without modification, are permitted provided that the following conditions are met:

1. Redistributions in source form must retain copyright statements and notices,

2. Redistributions in binary form must reproduce applicable copyright statements and notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution, and

3. Redistributions must contain a verbatim copy of this document.

The OpenLDAP Foundation may revise this license from time to time. Each revision is distinguished by a version number. You may use this Software under terms of this license revision or under the terms of any subsequent revision of the license.

THIS SOFTWARE IS PROVIDED BY THE OPENLDAP FOUNDATION AND ITS CONTRIBUTORS ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OPENLDAP FOUNDATION, ITS CONTRIBUTORS, OR THE AUTHOR(S) OR OWNER(S) OF THE SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The names of the authors and copyright holders must not be used in advertising or otherwise to promote the sale, use or other dealing in this Software without specific, written prior permission. Title to copyright in this Software shall at all times remain with copyright holders.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

Copyright 1999-2003 The OpenLDAP Foundation, Redwood City, California, USA. All Rights Reserved. Permission to copy and distribute verbatim copies of this document is granted.

Licenses - OpenSSL

LICENSE ISSUES

The OpenSSL toolkit stays under a double license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts.

OpenSSL License

Copyright (c) 1998-2019 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

==========

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.

If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used.

This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public License.]

Licenses - Wireless-RegDB

Copyright (c) 2008, Luis R. Rodriguez <mcgrof@gmail.com>

Copyright (c) 2008, Johannes Berg <johannes@sipsolutions.net>

Copyright (c) 2008, Michael Green <Michael.Green@Atheros.com>

Permission to use, copy, modify, and/or distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Licenses - WPA Supplicant and Hostapd

Copyright (c) 2002-2019, Jouni Malinen <j@w1.fi> and contributors

All Rights Reserved.

These programs are licensed under the BSD license (the one with advertisement clause removed).

If you are submitting changes to the project, please see CONTRIBUTIONS file for more instructions.

This package may include either wpa_supplicant, hostapd, or both. See README file respective subdirectories (wpa_supplicant/README or hostapd/README) for more details.

Source code files were moved around in v0.6.x releases and compared to earlier releases, the programs are now built by first going to a subdirectory (wpa_supplicant or hostapd) and creating build configuration (.config) and running 'make' there (for Linux/BSD/cygwin builds).

License

This software may be distributed, used, and modified under the terms of BSD license:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name(s) of the above-listed copyright holder(s) nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Index

A

A Note about Enabling Thresholds • 385
A Note about Firmware Upgrade Time • 341
A Note about Infinite Loop • 308
A Note about Untriggered Rules • 309
About the Interface • 386
Action Group • 274, 277
Actuator Configuration Commands • 521, 537
Actuator Control Operations • 551
Actuator Information • 403
Adding a Firewall Rule • 468
Adding a Monitored Device • 538
Adding a Radius Server • 518
Adding a Role-Based Access Control Rule • 481
Adding an LDAP Server • 511, 517
Adding Attributes to the Class • 631
Adding LDAP/LDAPS Servers • 239, 241, 246
Adding Radius Servers • 239, 244, 246, 636
Adding, Removing or Swapping Cascaded Devices • 215
Additional PXC/PXO Information • 672
AD-Related Configuration • 637, 655, 668
Alarm • 274, 276
Alerts • 64, 65, 91, 92
Alerts Notice in a Yellow or Red Screen • 60, 89, 116
All Privileges • 499, 505, 509
Altitude Correction Factors • 158, 427, 686
APIPA and Link-Local Addressing • 3, 21, 97, 207, 226
Applicable Models • xv
Assertion Timeout Example for Temperature Sensors • 680
Authentication Commands • 509
Authentication Settings • 412, 512, 515
Automatic and Manual Modes • 60, 64, 323
Automatically Completing a Command • 390, 557
Available Actions • 220, 259, 273, 277, 283, 291, 302, 357, 379
Available Data of the Outlets Overview Page • 124, 127, 130, 131
Available PDU Models • 1

B

Backup and Restore of Device Settings • 332, 343, 349, 580
Backup and Restore via SCP • 350, 561
Before You Begin • 4
Browsing through the Online Help • 102, 708
Built-in Rules and Rule Configuration • 259, 260, 302
Bulk Configuration • 23, 332, 343, 349, 560, 580
Bulk Configuration Methods • 15, 23
Bulk Configuration or Firmware Upgrade via DHCP/TFTP • 23, 341, 344, 348, 575, 590
Bulk Configuration Restrictions • 343, 344
Bulk Configuration via SCP • 344, 348, 560, 567
Bulk Configuration/Upgrade Procedure • 591, 592

C

Calendar • 251, 253
Canceling the Power-On Process • 551
Card Readers • 370, 375, 376
Cascading All Devices via USB • 26, 30, 58
Cascading Multiple PXC/PXO Devices for Sharing Ethernet Connectivity • 12, 14, 24, 193, 207, 334
Cascading Troubleshooting • 25, 215, 688
Change Load Shedding State • 274, 277
Changing a User's Password • 494
Changing an Outlet's Default State • 488
Changing HTTP(S) Settings • 188, 217, 227
Changing Measurement Units • 499, 503
Changing Modbus Settings • 55, 189, 217, 223
Changing SSH Settings • 177, 189, 217, 222
Changing Storage Settings • 279, 280, 357, 359, 360, 363, 365
Changing Telnet Settings • 189, 217, 223, 386
Changing the Inlet Name • 492
Changing the LAN Duplex Mode • 441
Changing the LAN Interface Speed • 440
Changing the Modbus Configuration • 459
Changing the Modbus Port • 460
Changing the Outlet Name • 487
Changing the Overcurrent Protector Name • 493
Changing the PDU Name • 423
Changing the Role(s) • 499

Changing the Sensor Description • 523
Changing the Sensor Name • 521
Changing the SSH Configuration • 456
Changing the SSH Port • 456
Changing the Telnet Configuration • 455
Changing the Telnet Port • 456
Changing the UDP Port • 542
Changing Your Own Password • 502
Changing Your Password • 98, 176, 177
Checking Lua Scripts States • 326, 327, 328
Checking the Accessibility of NTP Servers • 466
Checking the Branch Circuit Rating • 5
Circuit Breaker Orientation Limitation • 6, 7
Circuit Breakers • 94
Clearing Diagnostic Log for Network Connections • 421
Clearing Event Log • 421
Clearing Information • 420
Closing a Local Connection • 389
Command History • 417
Commands for Environmental Sensors • 533
Commands for Inlet Pole Sensors • 529
Commands for Inlet Sensors • 527
Commands for Overcurrent Protector Sensors • 531
Common Network Settings • 190, 193
config.txt • 23, 564, 566, 577, 579, 582, 613, 616, 617
Configuration Files • 575, 577, 591, 613
Configuration or Firmware Upgrade with a USB Drive • 24, 344, 348, 575, 586, 587, 590
Configuring Data Push Settings • 189, 279, 311
Configuring DNS Parameters • 438
Configuring Environmental Sensors' Default Thresholds • 525
Configuring IPv4 Parameters • 430
Configuring IPv6 Parameters • 434
Configuring Login Settings • 189, 227, 247
Configuring Network Services • 216, 388
Configuring Network Settings • 3, 13, 27, 30, 188, 190, 202, 694
Configuring NTP Server Settings • 385
Configuring Password Policy • 189, 227, 248
Configuring Security Settings • 227
Configuring SMTP Settings • 189, 217, 221, 281, 285
Configuring SNMP Settings • 178, 188, 217, 219, 274, 378
Configuring the Cascading Mode • 452
Configuring the PXC/PXO • 14
Configuring the PXC/PXO Device and Network • 421
Configuring the Serial Port • 189, 324
Configuring Webcams and Viewing Live Images • 54, 281, 357, 358, 361, 363, 368
Connecting a DPX2 Sensor Package to DX2, DX or DPX3 • 36, 39, 40, 42, 54
Connecting a DX2-ENVHUB4 Sensor Hub • 36, 37
Connecting a Logitech Webcam • 54, 356
Connecting a Mobile Device to PXC/PXO • 15, 58
Connecting a Modbus RTU Device or Bus • 54, 224
Connecting External Equipment (Optional) • 34
Connecting Raritan Environmental Sensor Packages • 34, 154
Connecting the PDU to a Power Source • 11
Connecting the PXC/PXO to a Computer • 3, 15, 21, 207, 619, 620, 688
Connecting the PXC/PXO to Your Network • 12, 14, 190
Connection Port Functions • 14, 57
Connection to Raritan Serial Access Products • 324, 710
Control Buttons • 61
Copying an Existing Server's Settings • 511, 515
Creating a CSR • 234, 235, 236
Creating a New Attribute • 630
Creating a Role • 505
Creating a Self-Signed Certificate • 234, 237
Creating a User Profile • 493
Creating an Outlet Group • 74, 137, 138, 489
Creating Configuration Files via Mass Deployment Utility • 577, 586, 587
Creating IP Access Control Rules • 189, 227, 228, 231
Creating Role Based Access Control Rules • 189, 227, 232, 234
Creating Roles • 99, 176, 180, 182, 636
Creating Users • 96, 176, 177, 181, 184, 186, 187, 223, 239, 378
Curl Upload Return Codes • 616, 617
Customizing Bulk Configuration Profiles • 343, 345
Customizing the Date and Time • 464

D

Dashboard • 103, 107, 149, 276, 353
Dashboard - Alarms • 108, 115, 274

Dashboard - Alerted Sensors • 65, 108, 112
Dashboard - Inlet History • 108, 114, 121
Dashboard - Inlet I1 • 108, 109, 121
Dashboard - OCP • 108, 111
Data Encryption in 'config.txt' • 582, 584, 587
Data Push Format • 311, 312
Date and Time Settings • 400
dcTrack • 711
dcTrack Overview • 712
Deassertion Hysteresis Example for Temperature Sensors • 683
Default Log Messages • 249, 260, 265, 278, 281
Default Measurement Units • 400
Default Voltage and Current Thresholds • 122, 148, 151, 684
Deleting a Firewall Rule • 471
Deleting a Monitored Device • 539
Deleting a Role • 509
Deleting a Role-Based Access Control Rule • 484
Deleting a User Profile • 501
Deleting an Outlet Group • 144
Detailed Information on Outlet Pages • 133, 136
Determining the Authentication Method • 510
Determining the SSH Authentication Method • 457
Determining the Time Setup Method • 462, 464
Device Configuration/Upgrade Procedure • 575
Device Info • 4, 14, 15, 64, 83, 207
Device Information • 281, 331, 333, 367
Device Settings • 104, 188
devices.csv • 23, 566, 577, 579, 583, 585, 617
Device-Specific Settings • 343, 701
DHCP IPv4 Configuration in Linux • 591, 609
DHCP IPv4 Configuration in Windows • 591, 592
DHCP IPv6 Configuration in Linux • 591, 611
DHCP IPv6 Configuration in Windows • 591, 602
Diagnostic Commands • 555
Diagnostic Log for Network Connections • 193, 201, 202
Different CLI Modes and Prompts • 388, 389, 391, 420, 422, 466, 491, 546, 547, 551, 555
Door Access Control • 255
Door Handle Status and Control • 160, 374
Download via Curl • 613, 614
Download via Web Browsers • 613
Downloading Diagnostic Data via SCP • 562
Downloading Diagnostic Information • 332, 352
Downloading Raw Configuration • 613
Downloading SNMP MIB • 220, 378, 383
DPX Sensor Packages • 34, 43
DPX2 Sensor Packages • 34, 40
DPX3 Sensor Packages • 34, 39
Dual Ethernet Connection • 12, 14
DX Sensor Packages • 34, 38
DX2 Sensor Packages • 34, 35, 289

E

EAP CA Certificate Example • 443, 445, 449
Editing or Deleting a Rule/Action • 274, 302, 323
Editing or Deleting IP Access Control Rules • 231
Editing or Deleting Ping Monitoring Settings • 321
Editing or Deleting Role Based Access Control Rules • 233
Editing or Deleting Roles • 141, 184
Editing or Deleting Users • 98, 181, 184, 185
Editing rciusergroup Attributes for User Members • 633
Enabling and Configuring SNMP • 304, 306, 310, 378
Enabling or Disabling 802.11n High Throughput • 448
Enabling or Disabling a User Profile • 496
Enabling or Disabling an Inlet (for Multi-Inlet PDUs) • 492
Enabling or Disabling Data Logging • 426
Enabling or Disabling EnergyWise • 541
Enabling or Disabling Front Panel Actuator Control • 485
Enabling or Disabling Front Panel Outlet Switching • 485
Enabling or Disabling Load Shedding • 546
Enabling or Disabling Modbus • 459
Enabling or Disabling Peripheral Device Auto Management • 428
Enabling or Disabling Service Advertising • 460
Enabling or Disabling SNMP v1/v2c • 457
Enabling or Disabling SNMP v3 • 458
Enabling or Disabling SSH • 456
Enabling or Disabling Strong Passwords • 477
Enabling or Disabling Telnet • 455
Enabling or Disabling the LAN Interface • 439
Enabling or Disabling the Read-Only Mode • 460
Enabling or Disabling the Restricted Service Agreement • 472
Enabling Service Advertising • 189, 217, 226, 460
Enabling the Restricted Service Agreement • 97, 189, 227, 249

EnergyWise Configuration Commands • 541
EnergyWise Settings • 415
Entering Configuration Mode • 389, 421, 445, 446, 494, 501, 502
Entering Diagnostic Mode • 389, 554, 692
Environmental Sensor Configuration Commands • 521
Environmental Sensor Default Thresholds • 410
Environmental Sensor Information • 401
Environmental Sensor Package Information • 402
Environmental Sensor Threshold Information • 409
Equipment Setup Worksheet • 5, 571
Ethernet Interface Settings • 14, 87, 190, 194, 442
Event Log • 415
Event Rules and Actions • 115, 121, 148, 169, 189, 219, 221, 259, 276, 311, 316, 326
Example • 464, 474, 494, 501, 502, 544, 546
  Ping Monitoring and SNMP Notifications • 316, 321
Example - Actuator Naming • 538
Example - Creating a Role • 509
Example - Default Upper Thresholds for Temperature • 527
Example - Inlet Naming • 492
Example - OCP Naming • 493
Example - Outlet Naming • 489
Example - Ping Command • 557
Example - Power Cycling Specific Outlets • 551
Example - Server Settings Changed • 541
Example - Setting Up EnergyWise • 543
Example - Turning On a Specific Actuator • 553
Example 1 • 309
Example 1 - Basic Security Information • 419
Example 1 - Combination of ETH1's Activation, Configuration Method and IP • 544
Example 1 - Creating a User Profile • 504
Example 1 - Environmental Sensor Naming • 525
Example 1 - IPv4 Firewall Control Configuration • 486
Example 1 - PDU Naming • 429
Example 1 - Time Setup Method • 465
Example 1 - Upper Critical Threshold for a Temperature Sensor • 535
Example 1 - Wireless Networking Mode • 461
Example 2 • 309
Example 2 - Adding an IPv4 Firewall Rule • 486
Example 2 - Combination of Upper Critical and Upper Warning Settings • 544
Example 2 - Enabling IPv6 Protocol on the Ethernet Interface • 461
Example 2 - In-Depth Security Information • 420
Example 2 - Modifying a User's Roles • 504
Example 2 - Outlet Sequence • 429
Example 2 - Primary NTP Server • 465
Example 2 - Sensor Threshold Selection • 525
Example 2 - Warning Thresholds for Inlet Sensors • 535
Example 3 • 309
Example 3 - Combination of SSID and PSK Parameters • 545
Example 3 - Default Measurement Units • 504
Example 3 - Outlet Sequence Delay • 429
Example 3 - Upper Thresholds for Overcurrent Protector Sensors • 535
Example 3 - User Blocking • 486
Example 3 - Wireless Authentication Method • 461
Example 4 - Adding an IPv4 Role-based Access Control Rule • 487
Example 4 - Combination of Upper Critical, Upper Warning and Lower Warning Settings • 545
Example 4 - Non-Critical Outlets • 430
Example 4 - Static IPv4 Configuration • 461
Examples • 418, 429, 461, 465, 485, 503, 524, 535
Existing Roles • 414
Existing User Profiles • 400, 413
Extended Cascading with PXC/PXO Devices • 28, 58

F

Filling Out the Equipment Setup Worksheet • 5
Finding the Sensor's Serial Number • 155, 164
Firewall Control • 466
Firmware Update via SCP • 341, 559
Firmware Upgrade via USB • 341, 576, 588
Forcing a Password Change • 496
FreeRADIUS Standard Attribute Illustration • 636, 654
FreeRADIUS VSA Illustration • 655, 667
From LDAP/LDAPS • 629
From Microsoft Active Directory • 629
Front Panel Display • 59
Front Panel Settings • 60, 71, 72, 74, 76, 160, 189, 323
Full Disaster Recovery • 342

Raritan
A brand of legrand

fwupdate.cfg • 575, 576, 577, 578, 582, 585, 588, 591

G

Gathering LDAP/Radius Information • 239, 240
Group's Power Control • 76

H

Hardware Issue Detection • 109, 332, 352, 418
How Long a Link Remains Accessible • 361, 363
How the Automatic Management Function Works • 157, 167, 428

I

Identifying Cascaded Devices • 334
Identifying Snapshots Folders on Remote Servers • 360, 366, 367
Identifying the Sensor Port • 35
Identifying the Sensor Position and Channel • 156, 165
Idle Timeout • 476
If Switchable Outlet Groups are Limited • 141
Illustration - GMAIL SMTP Certificate Chain • 702, 706
Illustrations of Adding LDAP Servers • 513, 514
Individual OCP Pages • 149
Individual Outlet Pages • 118, 119, 124, 126, 129, 133, 136
Individual Sensor/Actuator Pages • 82, 112, 155, 157, 158, 159, 169, 175
Initial Installation and Configuration • 11
Initial Network Configuration via CLI • 15, 22, 619, 620, 694
Initialization Delay Use Cases • 118, 119
Inlet • 56, 64, 68, 103, 109, 110, 121
Inlet Configuration Commands • 491
Inlet Information • 398
Inlet Pole Sensor Threshold Information • 406
Inlet Sensor Threshold Information • 404
Inrush Current and Inrush Guard Delay • 118, 120
Installing a CA-Signed Certificate • 234, 236
Installing or Downloading Existing Certificate and Key • 234, 238
Installing the USB-to-Serial Driver (Optional) • 21, 693
Integration • 710
Interface Names • 203, 206
Introduction • 1
Introduction to PDU Components • 56
IP Configuration • 392, 393
IPv4-Only or IPv6-Only Configuration • 392, 393

K

Keys that Cannot Be Uploaded • 564, 567, 613

L

Layout • 384
LDAP Configuration Illustration • 239, 621
LDAP Settings • 511
Licenses - Bind9 • 713
Licenses - Clish • 723
Licenses - Dropbear • 731
Licenses - FreeType • 734
Licenses - IW • 736
Licenses - JSON-C • 737
Licenses - LIBTIRPC • 738
Licenses - LIBXML2 • 738
Licenses - Mbus • 739
Licenses - Net-SNMP • 739
Licenses - Open LDAP • 748
Licenses - OpenSSL • 750
Licenses - Wireless-RegDB • 753
Licenses - WPA Supplicant and Hostapd • 753
Load Shedding Configuration Commands • 546
Load Shedding Mode • 125, 127, 129, 130, 135, 277, 426
Load Shedding Settings • 414
Locking Outlets • 10
Log an Event Message • 274, 278
Log Rows • 313, 315
Logging in to CLI • 387, 587, 620
Logging out of CLI • 558
Login • 14, 15, 21, 96, 207, 692
Login Limitation • 475
Login, Logout and Password Change • 96
Logout • 99
Lowercase Character Requirement • 477
Lua Scripts • 189, 288, 324

M

Main Menu • 60, 63
Maintenance • 105, 331
Managed vs Unmanaged Sensors/Actuators • 154, 161, 162

Managing an Outlet Group • 490
Managing External Authentication Settings • 239, 243, 245, 246
Managing Firewall Rules • 468
Managing One Sensor or Actuator • 156, 157, 167
Managing Role-Based Access Control Rules • 481
Manually Changing PXC's Zero U LCD Orientation • 59, 88
Manually Starting or Stopping a Script • 325, 326
Maximum Ambient Operating Temperature • 4, 569
Maximum Password History • 479
Maximum Password Length • 477
Menu • 101, 103, 117, 121, 123, 137, 147, 154, 176, 188, 326, 328, 329, 331, 358, 360, 361, 371, 376
Minimum Password Length • 477
Miscellaneous • 79, 189, 329
Mixing Diverse Sensor Types • 48, 49
Model List • 2
Modifying a Firewall Rule • 470
Modifying a Monitored Device's Settings • 539
Modifying a Role • 508
Modifying a Role-Based Access Control Rule • 482
Modifying a User Profile • 494
Modifying a User's Personal Data • 495
Modifying an Existing LDAP Server • 515
Modifying an Existing Radius Server • 519
Modifying an Outlet Group • 137, 142
Modifying Firewall Control Parameters • 466
Modifying or Deleting a Script • 324, 329
Modifying or Removing Bulk Profiles • 348
Modifying Role-Based Access Control Parameters • 479
Modifying SNMPv3 Settings • 496
Monitoring Server Accessibility • 189, 278, 316, 321
Mounting 1U or 2U Models • 9
Mounting Zero U Models Using Two Rear Buttons • 7
Mounting Zero U Models with Mount Buttons • 8
Multi-Command Syntax • 468, 475, 476, 477, 480, 490, 494, 495, 496, 499, 502, 525, 527, 529, 531, 533, 537, 539, 544

N

Network Configuration • 391
Network Configuration Commands • 430
Network Connections Diagnostic Log • 416
Network Diagnostics • 332, 351
Network Interface Settings • 394
Network Service Settings • 395
Network Troubleshooting • 351, 554
NPS Standard Attribute Illustration • 636
NPS VSA Illustration • 655
Numeric Character Requirement • 478

O

OCPs • 64, 70, 104, 112, 147, 149, 151
Off and Lock Icons for Outlets • 131, 132
Operating the Dot-Matrix LCD Display • 60, 62, 63, 65, 80, 94
Optional Parameters • 511, 512
Options for Outlet State on Startup • 118, 119, 134
Outlet Configuration Commands • 487
Outlet Group Configuration Commands • 489
Outlet Group Information • 397
Outlet Group Power Control • 137, 139
Outlet Groups • 74, 104, 118, 137, 278
Outlet Information • 396
Outlets • 56, 64, 71, 103, 123, 127, 130, 131, 133, 289
Overcurrent Protector Configuration Commands • 493
Overcurrent Protector Information • 399
Overcurrent Protector Sensor Threshold Information • 408
Overview of the Cascading Modes • 207, 209

P

Package Contents • 2, 4
Panel Components • 56
Password Aging • 475
Password Aging Interval • 476
PDU • 64, 67, 93, 102, 103, 117, 119, 136, 425
PDU Configuration • 395
PDU Configuration Commands • 422
Performing Bulk Configuration • 343, 346
Peripherals • 35, 38, 64, 79, 104, 154, 158, 160, 162, 164, 167, 169, 170, 171, 174, 175, 307, 323, 375
Placeholders for Custom Messages • 281, 282, 284, 299
Port Forwarding Examples • 98, 209, 212, 213
Port Number Syntax • 208, 210, 211, 213, 690

Possible Root Causes • 688
Power Control • 72, 323
Power Control Operations • 547
Power Cycling the Outlet(s) • 549
Power IQ Configuration • 710
Powering On/Off/Cycle Outlet Groups • 491
Power-Off Period Options for Individual Outlets • 135, 136
Preparing the Installation Site • 4
Push Out Sensor Readings • 275, 279
PXC • 2
PXC Rackmount Methods • 2, 6
PXC's Energy Pulse LED • 2, 67, 93
PXO • 3
PXO Rackmount Method • 3, 10

Q

Querying Available Parameters for a Command • 389, 390
Querying DNS Servers • 555
Quick Access to a Specific Page • 97, 105
Quitting Configuration Mode • 422, 474
Quitting Diagnostic Mode • 555

R

Rackmount and Locking Outlets • 6
Rackmount Safety Guidelines • 6
Rack-Mounting the PDU • 1, 6
RADIUS Configuration Illustration • 239, 636
Radius Settings • 518
Raritan Metered PDU • 57
Raritan Switched PDU • 56
Raw Configuration Upload and Download • 344, 348, 584, 590, 613
Rebooting the PXC/PXO • 332, 354
Record Snapshots to Webcam Storage • 275, 279
Reliability Data • 418
Reliability Error Log • 418
Reliability Hardware Failures • 418
Remembering User Names and Passwords • 99
Removing an Existing LDAP Server • 518
Removing an Existing Radius Server • 520
Removing the Uploaded Certificate or Private Key • 446
Reserving IP Addresses in DHCP Servers • 672, 673, 674
Reserving IP in Linux • 674
Reserving IP in Windows • 673
Reset Button • 93
Resetting All Settings to Factory Defaults • 332, 354, 619
Resetting the Button-Type Circuit Breaker • 94
Resetting the Handle-Type Circuit Breaker • 95
Resetting the PXC/PXO • 553
Resetting to Factory Defaults • 93, 355, 554, 619
Restarting the PDU • 553
Restricted Service Agreement • 472
Restrictions of Port-Forwarding Connections • 28, 31, 691
Retrieving Previous Commands • 390, 557
Retrieving Software Packages Information • 332, 355
Returning User Group Information • 629
RJ45-to-DB9 Cable Requirements for Computer Connections • 22, 58
Role Configuration Commands • 505
Role of a DNS Server • 623, 688
Role-Based Access Control • 479

S

Safety Guidelines • ii
Safety Instructions • iii, 4
Sample Environmental-Sensor-Level Event Rule • 131, 306
Sample Event Rules • 262, 303
Sample Inlet-Level Event Rule • 305
Sample Outlet-Level Event Rule • 304
Sample PDU-Level Event Rule • 303
Saving User Credentials for PDView's Automatic Login • 18, 19
Scheduling an Action • 260, 279, 291, 297
Security Configuration Commands • 466
Security Settings • 411
Send an SNMP Notification • 220, 275, 286
Send Email • 265, 275, 281, 293, 299
Send Sensor Report • 187, 275, 283, 296
Send Sensor Report Example • 283, 292, 293
Send Snapshots via Email • 275, 284
Sending Links to Snapshots or Videos • 357, 359, 361
Sensor Descriptors for Inlet Active Power • 313, 314
Sensor Log • 312, 313
Sensor RJ-45 Port Pinouts • 569
Sensor Threshold Configuration Commands • 527

Sensor Threshold Settings • 123, 149, 152, 159, 160, 170, 385, 676
Sensor/Actuator Location Example • 171, 174, 175
Sensor/Actuator States • 66, 80, 113, 155, 156, 162, 163
Serial Port Configuration Commands • 543
Serial Port Settings • 414
Serial RS-232 • 569
Server Reachability Configuration Commands • 538
Server Reachability Information • 416
Server Reachability Information for a Specific Server • 417
Server Status Checking or Power Control • 319
Setting an Outlet's Cycling Power-Off Period • 489
Setting Data Logging • 189, 310, 311, 426, 427
Setting Data Logging Measurements Per Entry • 427
Setting Default Measurement Units • 158, 176, 185, 186, 500, 502
Setting Ethernet EAP Parameters • 442
Setting IPv4 Static Routes • 433
Setting IPv6 Static Routes • 437
Setting LAN Interface Parameters • 439
Setting Network Service Parameters • 453
Setting Non-Critical Outlets • 125, 129, 130
Setting NTP Parameters • 463, 466
Setting Outlet Power-On Sequence and Delay • 125, 128, 548, 550
Setting the Alarmed to Normal Delay for DX-PIR • 524
Setting the Automatic Daylight Savings Time • 465
Setting the Baud Rates • 543
Setting the BSSID • 451
Setting the Cascading Mode • 3, 14, 24, 26, 27, 28, 30, 85, 190, 191, 193, 197, 207, 209, 215, 335
Setting the Date and Time • 189, 251, 281, 367, 385
Setting the Ethernet Authentication Method • 442
Setting the HTTP Port • 454
Setting the HTTPS Port • 455
Setting the Inrush Guard Delay Time • 425
Setting the IPv4 Address • 432
Setting the IPv4 Configuration Mode • 430
Setting the IPv4 Gateway • 432
Setting the IPv4 Preferred Host Name • 431
Setting the IPv6 Address • 436
Setting the IPv6 Configuration Mode • 434
Setting the IPv6 Gateway • 437
Setting the IPv6 Preferred Host Name • 435
Setting the LAN MTU • 441
Setting the Maximum Number of Active Powered Dry Contact Actuators • 429
Setting the Outlet Initialization Delay • 425
Setting the Outlet Power-On Sequence • 423
Setting the Outlet Power-On Sequence Delay • 423
Setting the PDU-Defined Cycling Power-Off Period • 425, 489
Setting the PDU-Defined Default Outlet State • 424, 488
Setting the Polling Interval • 543
Setting the PSK • 448
Setting the Registry to Permit Write Operations to the Schema • 630
Setting the SNMP Configuration • 457
Setting the SNMP Read Community • 458
Setting the SNMP Write Community • 458
Setting the SSID • 447
Setting the sysContact Value • 458
Setting the sysLocation Value • 459
Setting the sysName Value • 459
Setting the Time Zone • 385, 464
Setting the Wireless Authentication Method • 448
Setting the Wireless MTU • 451
Setting the X Coordinate • 522
Setting the Y Coordinate • 522
Setting the Z Coordinate • 428, 523
Setting the Z Coordinate Format for Environmental Sensors • 428, 523, 537
Setting Up a TLS Certificate • 189, 227, 234
Setting Up External Authentication • 189, 227, 239, 688
Setting Wireless EAP Parameters • 449
Setting Wireless Parameters • 447
Setting Your Preferred Measurement Units • 158, 176, 180, 185, 186
Showing an Outlet Group's Information • 74
Showing Information • 391
Showing Network Connections • 555
Showing Outlets Information • 71
Showing the Firmware Upgrade Progress • 92, 341
Shut down a Server and Control its Power • 275, 278
Single Login Limitation • 475
Slave Device Events in the Log • 691

SmartLock • 255, 370, 371, 376
SmartLock and Card Reader • 2, 104, 369
SNMP Gets and Sets • 383
SNMP Sets and Thresholds • 385
SNMPv2c Notifications • 220, 379
SNMPv3 Notifications • 220, 379, 380
Sorting a List • 106, 112, 124, 147, 155, 181, 184, 202, 299, 338, 342
Special Character Requirement • 479
Specifications • 6, 569
Specifying Non-Critical Outlets • 414, 426
Specifying the Agreement Contents • 474
Specifying the CC Sensor Type • 521
Specifying the Device Altitude • 427
Specifying the EnergyWise Domain • 542
Specifying the EnergyWise Secret • 542
Specifying the SSH Public Key • 457, 501
Standard Attributes • 636
Start or Stop a Lua Script • 275, 288, 325, 326
Static Route Examples • 190, 194, 203, 433, 437
Step A
  Add Your PXC/PXO as a RADIUS Client • 636, 637, 655, 656
Step A. Determine User Accounts and Roles • 621
Step B
  Configure Connection Policies and Standard Attributes • 637, 641
  Configure Connection Policies and Vendor-Specific Attributes • 655, 660
Step B. Configure User Groups on the AD Server • 622
Step C. Configure LDAP Authentication on the PXC/PXO • 623
Step D. Configure Roles on the PXC/PXO • 626
Strong Passwords • 477
Supported Maximum DPX Sensor Distances • 43, 47
Supported Web Browsers • 96
Supported Wireless LAN Configuration • 13, 689
Switch Outlet Group • 275, 288
Switch Outlets • 275, 289
Switch Peripheral Actuator • 275, 289
Switching Off an Actuator • 552
Switching On an Actuator • 552
Syslog Message • 276, 290
System and USB Requirements • 575, 576

T

Testing the Network Connectivity • 556, 692
TFTP Requirements • 591, 592
The ? Command for Showing Available Commands • 389
The Ping Tool • 691, 692
The PXC/PXO MIB • 384
Third Party Licenses • 713
Thresholds and Sensor States • 676
Time Configuration Commands • 461
Time Units • 117, 120, 136, 247, 248
TLS Certificate Chain • 199, 221, 242, 291, 311, 702
Tracing the Route • 557
Turning Off the Outlet(s) • 548
Turning On the Outlet(s) • 547

U

Unbalanced Current Calculation • 686
Unblocking a User • 247, 553
Unpacking the Product and Components • 4
Updating the LDAP Schema • 629
Updating the PXC/PXO Firmware • 331, 340, 559
Updating the Schema Cache • 633
Upload via Curl • 23, 615, 616, 617
Uploading or Downloading Raw Configuration Data • 23, 561, 564, 613, 615
Uploading Raw Configuration • 615
Uppercase Character Requirement • 478
USB Wireless LAN Adapters • 13, 27, 30, 689
User Blocking • 476
User Configuration Commands • 493
User Interfaces Showing Default Units • 186, 187
User Management • 104, 176
Using an Optional DPX3-ENVHUB4 Sensor Hub • 44, 48
Using an Optional DPX-ENVHUB2 cable • 45
Using an Optional DPX-ENVHUB4 Sensor Hub • 44
Using an Optional Sensor Hub • 36, 37
Using Default Thresholds • 524
Using SCP Commands • 559
Using SNMP • 341, 378
Using the CLI Command • 554, 620
Using the Command Line Interface • 217, 386, 620
Using the Reset Button • 619
Using the Web Interface • 96

V

Vendor-Specific Attributes • 636, 655
Viewing and Managing Locally-Saved Snapshots • 279, 354, 363, 366
Viewing Connected Users • 331, 338, 361
Viewing Firmware Update History • 331, 342
Viewing or Clearing the Local Event Log • 221, 239, 290, 331, 339
Visiting Other Pages from Current Group • 145

W

Ways to Probe Existing User Profiles • 688
Web Interface Overview • 100, 708
Webcam Management • 104, 339, 356
What is a Certificate Chain • 702, 708
Windows NTP Server Synchronization Solution • 252, 254
Wired Network Settings • 12, 14, 190, 191, 208, 226, 623
Wireless Network Settings • 190, 197, 208, 449
With HyperTerminal • 387, 553
With SSH or Telnet • 388, 692
Writing or Loading a Lua Script • 324, 328

Y

Yellow- or Red-Highlighted Sensors • 62, 65, 79, 89, 121, 147, 155, 160, 163, 169, 678

Z

Z Coordinate Format • 157, 174