PX3-3000/4000/5000 Series

User Guide
Release 3.2.10

Copyright © 2016 Raritan, Inc.

PX3-0F-v3.2.10-E

April 2016

255-80-0035-00

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.

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 2016 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.

CE c UL us LISTED 1F61 I.T.E.

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 xviii

What's New in the PX User Guide xx

Chapter 1 Introduction 1

Product Models 1
Package Contents 1
Zero U Products 1
1U Products 2
2U Products 2
APIPA and Link-Local Addressing 2

Chapter 2 Rack-Mounting the PDU 4

Rackmount Safety Guidelines 4
Circuit Breaker Orientation Limitation 4
Mounting Zero U Models Using L-Brackets 5
Mounting Zero U Models Using Button Mount 6
Mounting Zero U Models Using Claw-Foot Brackets 8
Mounting Zero U Models Using Two Rear Buttons 9
Mounting 1U or 2U Models 10

Chapter 3 Installation and Configuration 12

Before You Begin 12
Unpacking the Product and Components 12
Preparing the Installation Site 13

Checking the Branch Circuit Rating....13
Filling Out the Equipment Setup Worksheet....13
Installing Cable Retention Clips on the Inlet (Optional)....13
Connecting a Locking Line Cord....15
Disconnecting a Locking Line Cord....16
Connecting the PDU to a Power Source....17
Configuring the PX....17
Connecting the PX to a Computer....18
Installing the USB-to-Serial Driver (Optional)....20
Connecting the PX to Your Network....21
Initial Network Configuration via CLI....23
Cascading the PX via USB....29
Bulk Configuration Methods....32
Installing Cable Retention Clips on Outlets (Optional)....33

Chapter 4 Connecting External Equipment (Optional) 35

Connecting Environmental Sensor Packages....35
DPX Sensor Packages....36
DPX2 Sensor Packages....41
DPX3 Sensor Packages....43
DX Sensor Packages....45
Using an Optional DPX3-ENVHUB4 Sensor Hub....48
Mixing Diverse Sensor Types....50
Connecting Asset Management Sensors....54
Combining Regular Asset Sensors....54
Connecting Regular Asset Sensors to the PX....56
Connecting Blade Extension Strips....58
Connecting Composite Asset Sensors (AMS-Mx-Z)....61
Connecting a Logitech Webcam....63
Connecting a GSM Modem....64
Connecting an Analog Modem....64
Connecting an External Beeper....65
Connecting a Schroff LHX/SHX Heat Exchanger....65

Chapter 5 Using the PDU 67

Panel Components....67
Inlet....68
Outlets....69
Connection Ports....70
Dot-Matrix LCD Display....72
Reset Button....98
Circuit Breakers....99
Resetting the Button-Type Circuit Breaker....99
Resetting the Handle-Type Circuit Breaker....100
Fuse....101
Fuse Replacement on Zero U Models....101
Fuse Replacement on 1U Models....102

Beeper 104
Replaceable Controller 105

Chapter 6 Using the Web Interface 107

Supported Web Browsers 107
Logging in to the Web Interface 108
Login 108
Changing Your Password 111
Remembering User Names and Passwords 111
Logout 111
Introduction to the Web Interface 112
Menus 113
PX Explorer Pane 113
Setup Button 116
Status Bar 116
Add Page Icon 117
Data Pane 118
More Information 118
Viewing the Dashboard 122
Alerted Sensors 122
Alarms List 123
Device Management 124
Displaying PDU Information 125
Naming the PDU 130
Modifying the Network Configuration 130
Modifying Network Service Settings 140
Setting the Date and Time 146
Setting the LCD Display's Default View 150
Setting Default Measurement Units 150
Configuring the Feature Port 151
Configuring the Serial Port 153
Setting the Cascading Mode 154
Setting Data Logging 161
Configuring SMTP Settings 162
Configuring Data Push Settings 163
Specifying the Device Altitude 164
Rebooting the PX Device 165
Resetting All Active Energy Readings 165
Monitoring Total Active Energy or Power 166
Checking the Internal Beeper State 167
Setting the EnergyWise Configuration 167
User Management 168
Creating a User Profile 168
Modifying a User Profile 172
Deleting a User Profile 172
Setting Up Your Preferred Measurement Units 173
Setting Up Roles 174
Creating a Role 174
Modifying a Role 175

Deleting a Role 176
Access Security Control 177
Forcing HTTPS Encryption 177
Configuring the Firewall 177
Setting Up User Login Controls 184
Setting Up Role-Based Access Control Rules 188
Setting Up a TLS Certificate 192
Certificate Signing Request 193
Creating a Self-Signed Certificate 195
Installing Existing Key and Certificate Files 197
Downloading Key and Certificate Files 197
Setting Up External Authentication 198
Gathering the External Authentication Information 198
Adding Authentication Servers 200
Sorting the Access Order 204
Testing the Server Connection 204
Editing Authentication Server Settings 205
Deleting Authentication Server Settings 205
Disabling External Authentication 205
Enabling External and Local Authentication Services 206
Outlet Management 206
PX3 Latching Relay Behavior 206
Naming Outlets 208
Outlet Monitoring 208
Outlet Switching 210
Setting the Default Outlet State 213
Changing the Cycling Power-Off Period 215
Setting the Initialization Delay 217
Setting the Inrush Guard Delay 218
Setting the Outlet Power-On Sequence 219
Setting the Outlet-Specific Power-On Delay 220
Setting Non-Critical Outlets and Load Shedding Mode 220
Resetting Outlet Active Energy Readings 223
Enabling Front Panel Outlet Switching 224
Inlet and Overcurrent Protector Management 224
Naming the Inlet 225
Naming Overcurrent Protectors 225
Monitoring the Inlet 225
Monitoring Overcurrent Protectors 226
Resetting Inlet Active Energy Readings 227
Disabling an Inlet (for Multi-Inlet PDUs) 228
Setting Power Thresholds 229
Setting an Outlet's Thresholds 229
Bulk Configuration for Outlet Thresholds 230
Setting Inlet Thresholds 232
Setting an Overcurrent Protector's Thresholds 232
Bulk Configuration for Overcurrent Protector Thresholds 233
Setting Thresholds for Total Active Energy or Power 234
Event Rules and Actions 236
Components of an Event Rule 236
Creating an Event Rule 236
Sample Event Rules 280

A Note about Infinite Loop 283
Modifying an Event Rule 285
Modifying an Action 286
Deleting an Event Rule or Action 287
A Note about Untriggered Rules 287
Managing Event Logging 287
Viewing the Local Event Log 288
Viewing the Wireless LAN Diagnostic Log 289
Viewing Connected Users 290
Monitoring Server Accessibility 291
Adding IT Devices for Ping Monitoring 291
Editing Ping Monitoring Settings 294
Deleting Ping Monitoring Settings 294
Checking Server Monitoring States 295
Environmental Sensors and Actuators 295
Identifying Environmental Sensors and Actuators 296
Managing Environmental Sensors or Actuators 300
Configuring Environmental Sensors or Actuators 302
Viewing Sensor or Actuator Data 307
Unmanaging Environmental Sensors or Actuators 311
Disabling the Automatic Management Function 312
Controlling Actuators 313
Enabling the Front Panel Actuator Control 313
Asset Management 314
Configuring the Asset Sensor 314
Setting Asset Sensor LED Colors 315
Configuring a Specific Rack Unit 316
Expanding a Blade Extension Strip 317
Displaying the Asset Sensor Information 318
Bulk Configuration 319
Saving the PX Configuration 320
Copying the PX Configuration 321
Backup and Restore of PX Device Settings 322
Webcam Management 323
Configuring Webcams 323
Adjusting Image Properties 324
Viewing Webcam Snapshots or Videos 325
Sending Snapshots or Videos in an Email or Instant Message 327
Snapshot Storage 329
Network Diagnostics 332
Pinging a Host 332
Tracing the Network Route 332
Listing TCP Connections 333
Downloading Diagnostic Information 333
Managing the Schroff LHX/SHX Heat Exchanger 334
Enabling and Disabling Schroff LHX/SHX Heat Exchanger Support 335
Configuring the LHX/SHX 335
Monitoring the LHX/SHX 337
Turning the LHX/SHX On or Off 340
Requesting Maximum Cooling for an SHX-30 341
Firmware Upgrade 341
Updating the PX Firmware 342

Viewing Firmware Update History 344
Full Disaster Recovery 345
Updating the Asset Sensor Firmware 345
Accessing the Help 345
Retrieving Software Packages Information 345
Browsing through the Online Help 346

Chapter 7 Using SNMP 348

Enabling SNMP 348
Configuring Users for Encrypted SNMP v3 349
Configuring SNMP Notifications 350
SNMPv2c Notifications 351
SNMPv3 Notifications 353
SNMP Gets and Sets 355
The PX MIB 356
Retrieving Energy Usage 358
A Note about Enabling Thresholds 358

Chapter 8 Using the Command Line Interface 359

About the Interface 359
Logging in to CLI 360
With HyperTerminal 360
With SSH or Telnet 361
With an Analog Modem 362
Different CLI Modes and Prompts 363
Closing a Local Connection 363
Help Command 364
Querying Available Parameters for a Command 365
Showing Information 365
Network Configuration 366
PDU Configuration 368
Outlet Information 369
Inlet Information 370
Overcurrent Protector Information 371
Date and Time Settings 372
Default Measurement Units 372
Environmental Sensor Information 373
Environmental Sensor Package Information 375
Actuator Information 376
Outlet Sensor Threshold Information 377
Outlet Pole Sensor Threshold Information 378
Inlet Sensor Threshold Information 379
Inlet Pole Sensor Threshold Information 380
Overcurrent Protector Sensor Threshold Information 381
Environmental Sensor Threshold Information 382
Environmental Sensor Default Thresholds 383
Security Settings 384

Existing User Profiles 385
Existing Roles 386
Load Shedding Settings 386
Serial Port Settings 387
EnergyWise Settings 387
USB-Cascading Configuration Information 387
Asset Sensor Settings 387
Rack Unit Settings of an Asset Sensor 388
Blade Extension Strip Settings 389
Event Log 390
Wireless LAN Diagnostic Log 391
Server Reachability Information 391
Command History 393
History Buffer Length 393
Reliability Data 393
Reliability Error Log 393
Examples 394
Clearing Information 396
Clearing Event Log 396
Clearing WLAN Log 397
Configuring the PX Device and Network 397
Entering Configuration Mode 397
Quitting Configuration Mode 398
PDU Configuration Commands 398
Network Configuration Commands 406
Time Configuration Commands 430
Checking the Accessibility of NTP Servers 434
Security Configuration Commands 435
Outlet Configuration Commands 455
Inlet Configuration Commands 457
Overcurrent Protector Configuration Commands 459
User Configuration Commands 459
Role Configuration Commands 473
Environmental Sensor Configuration Commands 478
Configuring Environmental Sensors' Default Thresholds 483
Sensor Threshold Configuration Commands 485
Actuator Configuration Commands 495
Server Reachability Configuration Commands 496
EnergyWise Configuration Commands 500
USB-Cascading Configuration Commands 502
Asset Management Commands 502
Serial Port Configuration Commands 509
Setting the History Buffer Length 511
Multi-Command Syntax 511
Load Shedding Configuration Commands 513
Enabling or Disabling Load Shedding 514
Power Control Operations 515
Turning On the Outlet(s) 515
Turning Off the Outlet(s) 516
Power Cycling the Outlet(s) 517
Canceling the Power-On Process 518
Example - Power Cycling Specific Outlets 518

Actuator Control Operations 518
Switching On an Actuator 519
Switching Off an Actuator 519
Example - Turning On a Specific Actuator 520
Unblocking a User 520
Resetting the PX 520
Restarting the PDU 521
Resetting Active Energy Readings 521
Resetting to Factory Defaults 522
Network Troubleshooting 522
Entering Diagnostic Mode 522
Quitting Diagnostic Mode 523
Diagnostic Commands 523
Retrieving Previous Commands 525
Automatically Completing a Command 525
Logging out of CLI 526

Chapter 9 In-Line Monitors 527

Overview 527
Safety Instructions 527
Flexible Cord Installation Instructions 528
Flexible Cord Selection 528
Plug Selection 529
Receptacle Selection 529
Derating a Raritan Product 529
Wiring of 3-Phase In-Line Monitors 530
In-Line Monitor Unused Channels 530
Step by Step Flexible Cord Installation 530
In-Line Monitor's Web Interface 536
Dashboard Page 537
Outlet Page 537

Appendix A Specifications 539

Maximum Ambient Operating Temperature 539
Serial RS-232 Port Pinouts 539
Sensor RJ-45 Port Pinouts 539
Feature RJ-45 Port Pinouts 540

Appendix B Equipment Setup Worksheet 542

Appendix C Configuration or Firmware Upgrade with a USB Drive 546

System and USB Requirements 547
Configuration Files 547
fwupdate.cfg 549
config.txt 552
devices.csv 554
Creating Configuration Files via Mass Deployment Utility 555

Firmware Upgrade via USB 556

Appendix D Bulk Configuration or Firmware Upgrade via DHCP/TFTP 557

Bulk Configuration/Upgrade Procedure 557
TFTP Requirements 558
DHCP IPv4 Configuration in Windows 559
DHCP IPv6 Configuration in Windows 569
DHCP IPv4 Configuration in Linux 576
DHCP IPv6 Configuration in Linux 578

Appendix E Resetting to Factory Defaults 580

Using the Reset Button 580
Using the CLI Command 581

Appendix F Available SCP Commands 583

Firmware Update via SCP 583
Bulk Configuration via SCP 584
Backup and Restore via SCP 585

Appendix G PX Models with Residual Current Monitoring 587

RCM Current Sensor 587
RCM State Sensor 588
Compliance with IEC 62020 589
RCM Self-Test 590
Web Interface Operations for RCM 590
- Checking RCM State and Current 590
- Setting RCM Current Thresholds 592
- Scheduling RCM Self-Test 592
- Disabling or Enabling Front Panel RCM Self-Test 593

Front Panel Operations for RCM 593
- LCD Message for RCM Critical State 593
- Checking RCM States on Phase II Models 594
- Displaying the RCM Current 595
- Running RCM Self-Test 595

RCM SNMP Operations 597
- RCM Trap 597
- RCM Residual Current and State Objects 597
- Setting RCM Thresholds 597
- Running RCM Self-Test 597

CLI Operations for RCM 598
- Showing Residual Current Monitor Information 598
- Setting RCM Current Thresholds 598

Setting Front Panel RCM Self-Test 600
Running RCM Self-Test 600

Appendix H PX3 Phase I LCD Display 601

Overview of the Character LCD Display 601
Control Buttons 602
Operating the Character LCD Display 603
Outlet Information 603
Inlet Information 605
Overcurrent Protector Information 606
IPv4 Address 607
MAC Address 608
Outlet Switching 609
Environmental Sensor Information 611
Asset Sensor Information 614
USB-Cascaded Device's Position 615
RCM Information 617

Appendix I LDAP Configuration Illustration 620

Step A. Determine User Accounts and Roles 620
Step B. Configure User Groups on the AD Server 621
Step C. Configure LDAP Authentication on the PX Device 622
Step D. Configure Roles on the PX Device 624

Appendix J Updating the LDAP Schema 628

Returning User Group Information 628
From LDAP/LDAPS 628
From Microsoft Active Directory 628
Setting the Registry to Permit Write Operations to the Schema 629
Creating a New Attribute 629
Adding Attributes to the Class 630
Updating the Schema Cache 632
Editing rciusergroup Attributes for User Members 632

Appendix K RADIUS Configuration Illustration 635

Microsoft Network Policy Server 635
Step A: Add Your PX as a RADIUS Client 636
Step B: Configure Connection Request Policies 639
Step C: Configure a Vendor-Specific Attribute 654
AD-Related Configuration 656
Non-Windows RADIUS Server 659
Dictionary File 659

Format of the "string" 660

Appendix L Additional PX Information 662

Locking Outlets and Cords 662
SecureLock™ Outlets and Cords 662
Button-Type Locking Outlets 664
Unbalanced Current Calculation 664
Reserving IP Addresses in Windows DHCP Servers 665
Sensor Threshold Settings 667
Thresholds and Sensor States 668
"To Assert" and Assertion Timeout 670
"To De-assert" and Deassertion Hysteresis 672
PDView App for Viewing the PX 674
Altitude Correction Factors 677
Data for BTU Calculation 677
Ways to Probe Existing User Profiles 678
Truncated Data in the Web Interface 678
Raritan Training Website 679

Appendix M Integration 680

Dominion KX II / III Configuration 680
Configuring Rack PDU Targets 681
Turning Outlets On/Off and Cycling Power 684
Dominion KSX II, SX or SX II Configuration 685
Dominion KSX II 685
Dominion SX and SX II 687
Power IQ Configuration 690
dcTrack 691
dcTrack Overview 692
Asset Management Sensors and dcTrack 693

Index 695

Applicable Models

This User Guide is applicable to the following PDUs (*n* indicated below represents a number).

- PX3-3nnn series
- PX3-4nnn series
- PX3-5nnn series

In this User Guide, PX3-3nnn is called PX3-3000, PX3-4nnn is called PX3-4000, and PX3-5nnn is called PX3-5000 for convenience.

Note: For information on other PX2 or PX3 models, see their respective Online Help or User Guide on the 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
PX2-1000 **PX3-1000**	✔			
PX2-2000 **PX3-2000**	✔		✔	✔
PX2-3000 **PX3-3000**		✔		
PX2-4000 **PX3-4000**	✔	✔		
PX2-5000 **PX3-5000**	✔	✔	✔	✔

Comparison between PX2 and PX3 series:

Features	Front panel display	Outlet latching relays	Number of USB-A ports	SENSOR port type	Replaceable controller
PX2 series	LED display		1	RJ-12	
PX3 phase I series	Character LCD display	✔ *	2	RJ-45	***
PX3 phase II series	Dot-matrix LCD display	✔ *	2	RJ-45	✔ **

* Only PX3 models with outlet switching (phase I and phase II models) have outlet latching relays.

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

*** PX3 phase I models do NOT support a replaceable controller.

What's New in the PX User Guide

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

APIPA and Link-Local Addressing (on page 2)

Configuring the PX (on page 17)

Connecting the PX to a Computer (on page 18)

Bulk Configuration Methods (on page 32)

Connecting Environmental Sensor Packages (on page 35)

DPX Sensor Packages (on page 36)

DPX3 Sensor Packages (on page 43)

Connecting a DPX2 Sensor Package to DPX3 (on page 44)

Using an Optional DPX3-ENVHUB4 Sensor Hub (on page 48)

Mixing Diverse Sensor Types (on page 50)

Connecting Regular Asset Sensors to the PX (on page 56)

Daisy-Chain Limitations of Composite Asset Sensors (on page 62)

Connecting an External Beeper (on page 65)

Automatic and Manual Modes (on page 73)

Operating the Dot-Matrix LCD Display (on page 75)

Alerts (on page 77)

PDU (on page 79)

Alerts Notice in a Yellow or Red Screen (on page 97)

Replaceable Controller (on page 105)

Supported Web Browsers (on page 107)

Login (on page 108)

Configuring the Serial Port (on page 153)

Overview of the Cascading Modes (on page 156)

Adding LDAP Server Settings (on page 200)

Send Sensor Report Example (on page 264)

Default Log Messages (on page 267)

Email and SMS Message Placeholders (on page 277)

Matching the Position (on page 298)

States of Unmanaged Sensors or Actuators (on page 311)

Unmanaging Environmental Sensors or Actuators (on page 311)

Downloading Diagnostic Information (on page 333)

Clearing WLAN Log (on page 397)

Enabling or Disabling Peripheral Device Auto Management (on page 405)

Determining the SSH Authentication Method (on page 426)

Customizing the Date and Time (on page 433)

All Privileges (on page 474)

Setting the Baud Rates (on page 510)

Forcing the Device Detection Mode (on page 510)

Configuration or Firmware Upgrade with a USB Drive (on page 546)

Bulk Configuration/Upgrade Procedure (on page 557)

RCM Information (on page 617)

Updating the LDAP Schema (on page 628)

PDView App for Viewing the PX (on page 674)

Dominion KX II / III Configuration (on page 680)

Dominion KSX II, SX or SX II Configuration (on page 685)

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

Chapter 1 Introduction

Raritan PX 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 the Raritan PX is distribution of power to information technology equipment such as computers and communication equipment where such equipment is typically mounted in an equipment rack located in an information technology equipment room.

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

In This Chapter

Product Models.....1
Package Contents 1
APIPA and Link-Local Addressing 2

Product Models

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

Package Contents

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

Zero U Products

- The PX device
- Screws, brackets and/or buttons for Zero U
- A null-modem cable with DB9 connectors on both ends (Raritan number: 254-01-0006-00) (optional)
- Cable retention clips for the inlet (for some models only)
- Cable retention clips for outlets (for some models only)

1U Products

- The PX device
- 1U bracket pack and screws
- A null-modem cable with DB9 connectors on both ends (Raritan number: 254-01-0006-00) (optional)
- Cable retention clips for the inlet (for some models only)

2U Products

- The PX device
- 2U bracket pack and screws
- A null-modem cable with DB9 connectors on both ends (Raritan number: 254-01-0006-00) (optional)
- Cable retention clips for the inlet (for some models only)

APIPA and Link-Local Addressing

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

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

Exception: The PX in the Port Forwarding mode does not support APIPA. See **Setting the Cascading Mode** *(on page 154).*

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

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

  Note: Configuration by connecting the PX to a computer using a network cable is an application of this scenario. See **Connecting the PX to a Computer** *(on page 18).*

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

Link-local addressing:

- IPv4 address:

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

- IPv6 address:

  A link-local IPv6 address is available only after IPv6 is enabled on the PX. See ***Selecting the Internet Protocol*** (on page 134).

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

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

Retrieval of the link-local address:

- For PX3 phase II models, see ***Device Info*** (on page 93).
- For PX3 phase I models, see ***IPv4 Address*** (on page 607).

Chapter 2 Rack-Mounting the PDU

This chapter describes how to rack mount a PX device. Only the most common rackmount method is displayed. Follow the procedure suitable for your model.

In This Chapter

Rackmount Safety Guidelines 4
Circuit Breaker Orientation Limitation....4
Mounting Zero U Models Using L-Brackets....5
Mounting Zero U Models Using Button Mount 6
Mounting Zero U Models Using Claw-Foot Brackets 8
Mounting Zero U Models Using Two Rear Buttons....9
Mounting 1U or 2U Models....10

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 539) 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.

Circuit Breaker Orientation Limitation

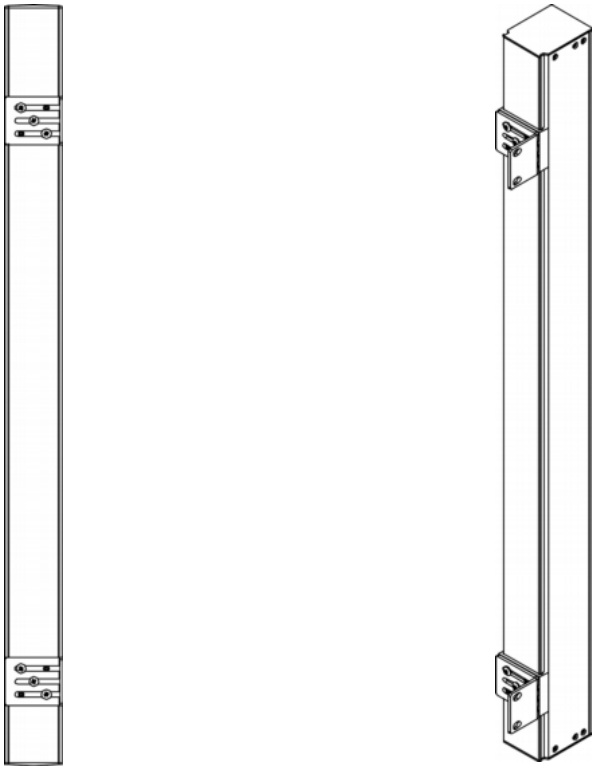
Usually a PDU can be mounted in any orientation. However, when mounting a PDU with circuit breakers, you must obey these rules:

- 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.

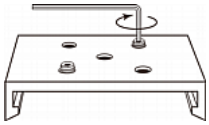
Mounting Zero U Models Using L-Brackets

If your PDU has circuit breakers implemented, read ***Circuit Breaker Orientation Limitation*** (on page 4) before mounting it.

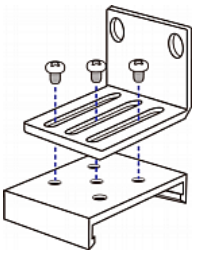


To mount Zero U models using L-brackets:

1. Align the baseplates on the rear of the PX device.
2. Secure the baseplates in place. Use the included L-shaped hex key to loosen the hex socket screws until the baseplate is "slightly" fastened.



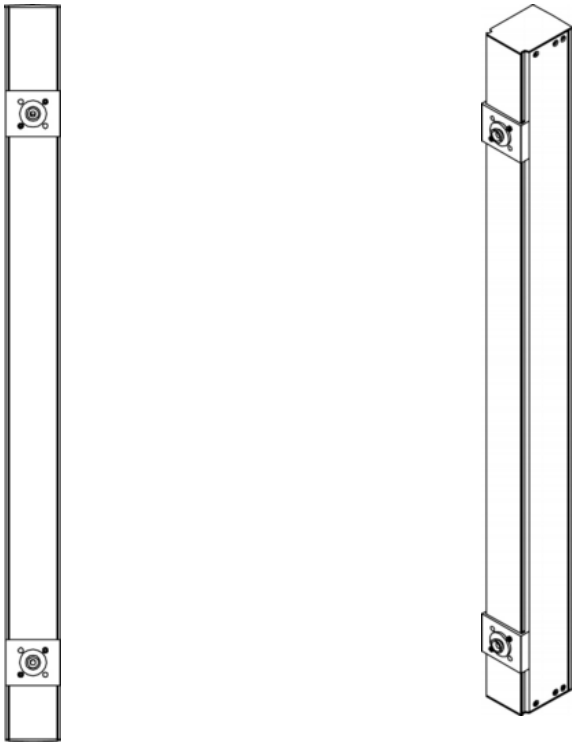
3. Align the L-brackets with the baseplates so that the five screw-holes on the baseplates line up through the L-bracket's slots. The rackmount side of brackets should face either the left or right side of the PX device.
4. Fasten the brackets in place with at least three screws (one through each slot). Use additional screws as desired.



5. Using rack screws, fasten the PX device to the rack through the L-brackets.

Mounting Zero U Models Using Button Mount

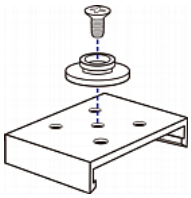
If your PDU has circuit breakers implemented, read ***Circuit Breaker Orientation Limitation*** (on page 4) before mounting it.



To mount Zero-U models using button mount:

1. Align the baseplates on the rear of the PX device. Leave at least 24 inches between the baseplates for stability.
2. Make the baseplates grasp the PX device lightly. Use the included L-shaped hex key to loosen the hex socket screws until the baseplate is "slightly" fastened.

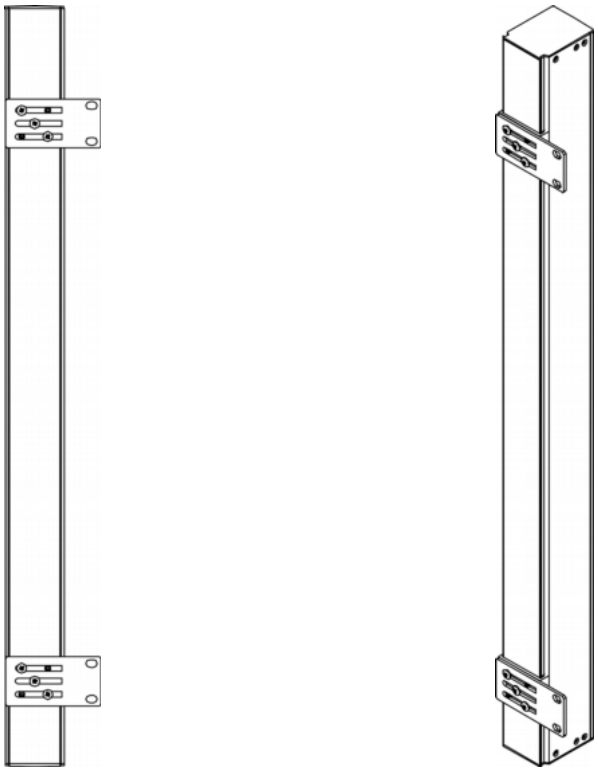
3. Screw each mounting button in the center of each baseplate. The recommended torque for the button is 1.96 N·m (20 kgf·cm).



4. Align the large mounting buttons with the mounting holes in the cabinet, fixing one in place and adjusting the other.
5. Loosen the hex socket screws until the mounting buttons are secured in their position.
6. Ensure that both buttons can engage their mounting holes simultaneously.
7. Press the PX device forward, pushing the mounting buttons through the mounting holes, then letting the device drop about 5/8". This secures the PX device in place and completes the installation.

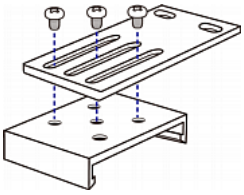
Mounting Zero U Models Using Claw-Foot Brackets

If your PDU has circuit breakers implemented, read ***Circuit Breaker Orientation Limitation*** (on page 4) before mounting it.



To mount Zero U models using claw-foot brackets:

1. Align the baseplates on the rear of the PX device.
2. Secure the baseplates in place. Use the included L-shaped hex key to loosen the hex socket screws until the baseplate is "slightly" fastened.
3. Align the claw-foot brackets with the baseplates so that the five screw-holes on the baseplates line up through the bracket's slots. The rackmount side of brackets should face either the left or right side of the PX device.
4. Fasten the brackets in place with at least three screws (one through each slot). Use additional screws as desired.



5. Using rack screws, fasten the PX device to the rack through the claw-foot brackets.

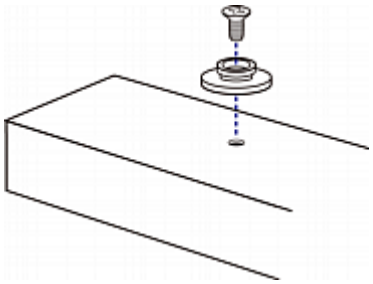
Mounting Zero U Models Using Two Rear Buttons

The following describes how to mount a PDU using two buttons only. If your PDU has circuit breakers implemented, read ***Circuit Breaker Orientation Limitation*** (on page 4) before mounting it.

To mount Zero U models using two buttons:

1. Turn to the rear of the PDU.
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).



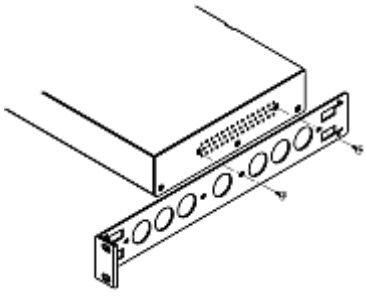
4. Screw a button in the screw hole near the top. The recommended torque for the button is 1.96 N·m (20 kgf·cm).
5. Ensure that the two buttons can engage their mounting holes in the rack or cabinet simultaneously.
6. Press the PX device forward, pushing the mounting buttons through the mounting holes,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

Mounting 1U or 2U Models

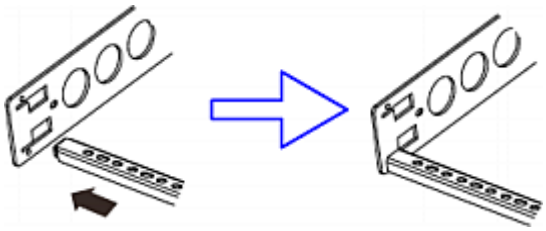
Using the appropriate brackets and tools, fasten the 1U or 2U PX device to the rack or cabinet.

To mount the PX device:

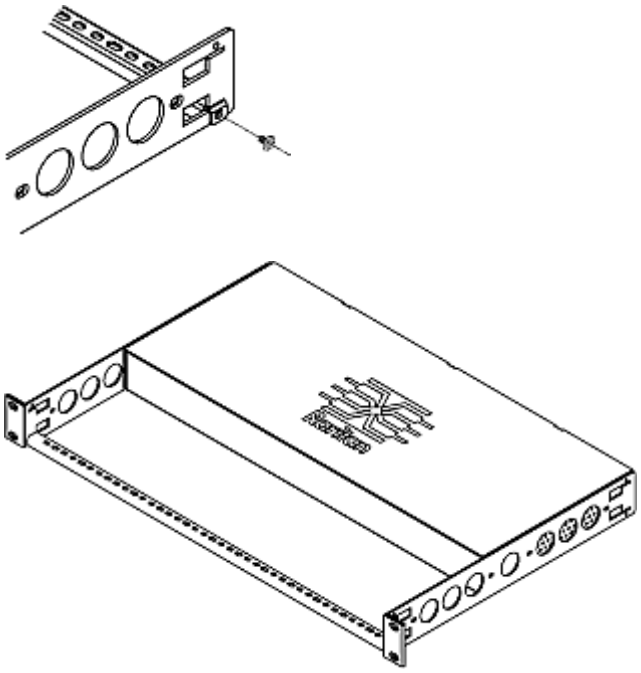
1. Attach a rackmount bracket to both sides of the PX with the provided screws.



2. Insert the cable-support bar into rackmount brackets.



3. Secure with the provided end cap screws.



4. Fasten the rackmount brackets' ears to the rack using your own fasteners.

Chapter 3 Installation and Configuration

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

In This Chapter

Before You Begin 12
Installing Cable Retention Clips on the Inlet (Optional).....13
Connecting a Locking Line Cord 15
Connecting the PDU to a Power Source.....17
Configuring the PX 17
Cascading the PX via USB.....29
Bulk Configuration Methods 32
Installing Cable Retention Clips on Outlets (Optional).....33

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 PX device and other equipment from the box in which they were shipped. See ***Package Contents*** (on page 1) 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's Technical Support Department for assistance.
4. Verify that all circuit breakers on the PX device 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 PX devices have overcurrent protection mechanisms.

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 539).*

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

Checking the Branch Circuit Rating

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

Filling Out the Equipment Setup Worksheet

An Equipment Setup Worksheet is provided in this User Guide. See ***Equipment Setup Worksheet*** (on page 542). 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.

Installing Cable Retention Clips on the Inlet (Optional)

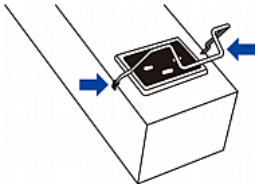
If your PX device is designed to use a cable retention clip, install the clip before connecting a power cord. A cable retention clip prevents the connected power cord from coming loose or falling off.

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

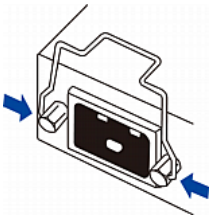
To install and use a cable retention clip on the inlet:

1. Locate two tiny holes adjacent to the inlet.
2. Install the cable retention clip by inserting two ends of the clip into the tiny holes.

Zero U models

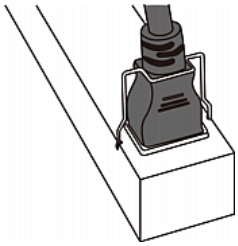


1U/2U models

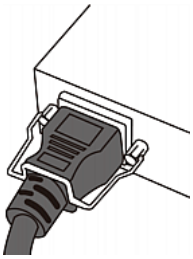


3. Connect the power cord to the inlet, and press the clip toward the power cord until it holds the cord firmly.

Zero U models



1U/2U models



Connecting a Locking Line Cord

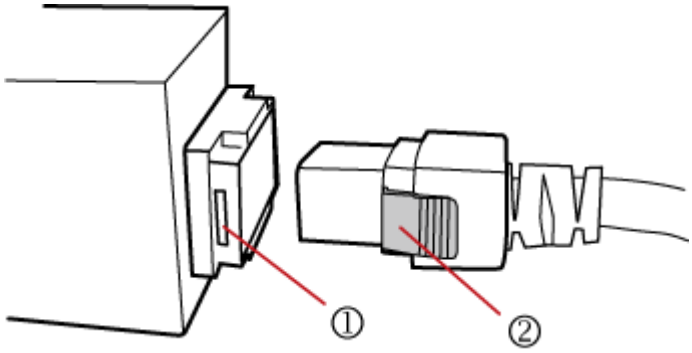
If your PDU is a PX3 *Phase II* model, it is shipped with either of the following locking line cords.

- A line cord with locking clips: A locking inlet on the PDU is required for this cord.
- A line cord with slide release buttons: This line cord automatically locks after being connected to the inlet. A locking inlet is not required for this cord.

A locking inlet and/or locking line cord ensure that the line cord is securely fastened to the inlet.

To connect a cord with locking clips:

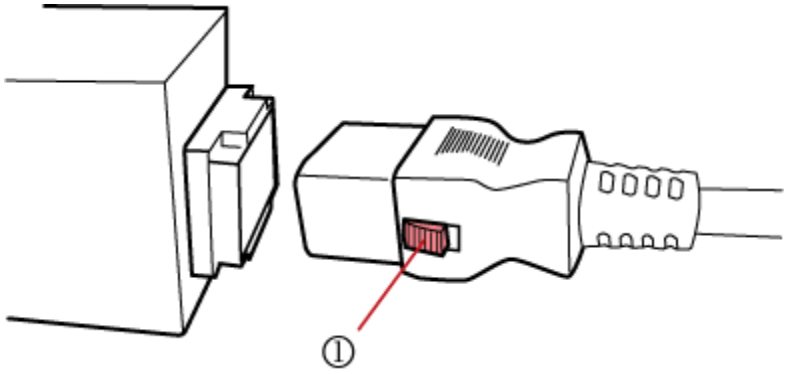
Make sure the line cord's locking clips fit into the locking holes at two sides of the inlet when plugging the cord's connector into the PDU's locking inlet.



Number	Item
1	Locking holes on the inlet
2	Locking clips of the line cord

To connect a cord with slide release buttons:

Simply plug the cord's connector into the PDU's inlet.



Number	Item
1	Slide release buttons

For information on removing the locking line cord, see ***Disconnecting a Locking Line Cord*** (on page 16).

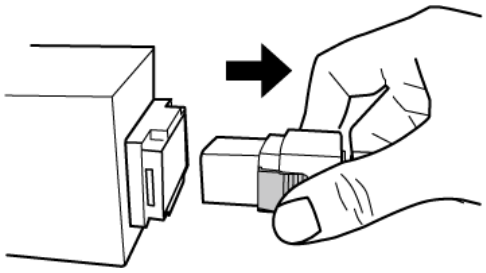
Disconnecting a Locking Line Cord

The ways to disconnect a locking line cord vary according to the cord type.

To disconnect a line cord with locking clips:

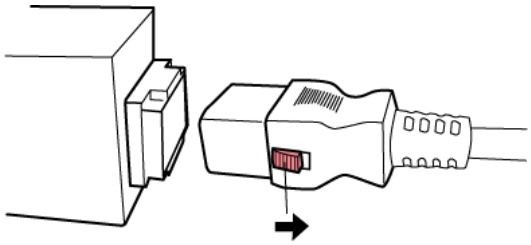
Press both locking clips of the line cord while unplugging the cord.

Tip: You can slightly move the line cord's plug horizontally while pulling it out to facilitate the disconnection process.



To disconnect a line cord with slide release buttons:

Push both slide release buttons toward the cord while unplugging this cord.



Connecting the PDU to a Power Source

1. Verify that all circuit breakers on the PX device 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 PX devices have overcurrent protection mechanisms.

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

   Note: When a PX device powers up, it proceeds with the power-on self test and software loading for a few moments. At this time, the outlet LEDs cycle through different colors. Note that outlet LEDs are only available on some PDU models.

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

Configuring the PX

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

Configuration over a DHCP-enabled network:

1. Connect the PX to a DHCP network. See ***Connecting the PX to Your Network*** (on page 21).
2. Retrieve the DHCP-assigned IPv4 address. Use the front panel LCD display to retrieve it.
   - PX3 Phase II models, see ***Device Info*** (on page 93).
   - PX3 Phase I models, see ***IPv4 Address*** (on page 607).

3. Launch a web browser to configure the PX. See ***Login*** (on page 108).

Configuration using a connected computer:

1. Connect the PX to a computer. See ***Connecting the PX to a Computer*** (on page 18).
2. Use the connected computer to configure the PX via the command line or web interface.
   - Command line interface: See ***Initial Network Configuration via CLI*** (on page 23).
   - Web interface: Launch the web browser on the computer, and type the link-local IP address or *pdu.local* to access the PX. See ***Login*** (on page 108).

     For IP address retrieval, see ***Device Info*** (on page 93) or ***IPv4 Address*** (on page 607).

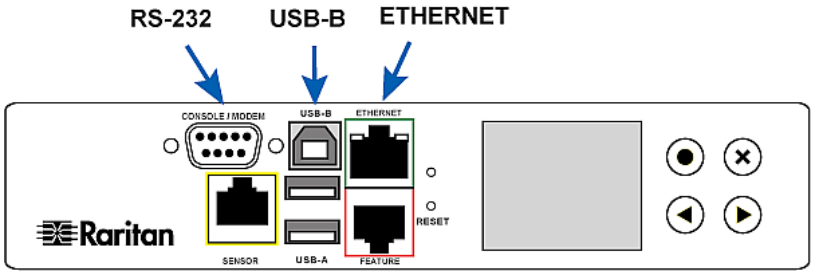
Tip: To configure a number of PX devices quickly, see **Bulk Configuration Methods** *(on page 32).*

Connecting the PX to a Computer

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

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

PX3 "Phase II" Zero U models:



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 PX is automatically configured with the following link-local addressing in any network without DHCP available:

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

Establish one of the following connections to a computer.

Serial RS-232 connection:

1. Connect one end of the null-modem cable to the male RS-232 port labeled CONSOLE / MODEM on the PX.
2. Connect the other end to your computer's RS-232 port (COM).
3. Perform ***Initial Network Configuration via CLI*** (on page 23).

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 20).
2. Connect a USB cable between the PX device's USB-B port and a computer's USB-A port.
3. Perform ***Initial Network Configuration via CLI*** (on page 23).

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

Direct network connection:

1. Connect one end of a standard network patch cable to the ETHERNET port of the PX.
2. Connect the other end to a computer's Ethernet port.
3. On the connected computer, launch a web browser to access the PX, using either link-local addressing: *pdu.local* or *169.254.x.x*. See ***Login*** (on page 108).

Installing the USB-to-Serial Driver (Optional)

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

Note: <n> in the filename of "dominion-serial-setup-<n>.exe" represents the file's version number.

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

Automatic driver installation in Windows®:

1. Make sure the PX 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 PX to the computer via a USB cable. The driver is automatically installed.

Manual driver installation in Windows®:

1. Make sure the PX 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 PX 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 PX to the computer. Usually the tty device is "/dev/ttyACM#" or "/dev/ttyUSB#," where # is an integer number.

For example, if you are using the kermit terminal program, and the tty device is "/dev/ttyACM0," perform the following commands:

> set line /dev/ttyACM0

> Connect

Connecting the PX to Your Network

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

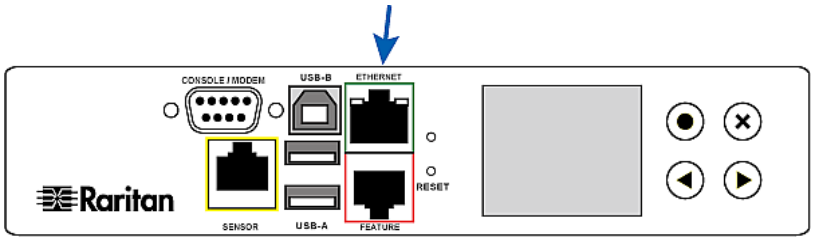
Note: If your PX will be used as a master device in the USB-cascading configuration where the bridging mode applies, make a wired connection. See **Cascading the PX via USB** *(on page 29).*

To make a wired connection:

1. Connect a standard network patch cable to the ETHERNET port on the PX.
2. Connect the other end of the cable to your LAN.

Below indicates the ETHERNET port on Zero U models:

PX3 Phase II models:



Warning: Accidentally plugging an RS-232 RJ-45 connector into the ETHERNET port can cause permanent damages 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 PX.
- Connect a USB docking station to the USB-A port on the PX. Then plug the supported USB wireless LAN adapter into the appropriate USB port on the docking station.

See ***USB Wireless LAN Adapters*** (on page 22) for a list of supported wireless LAN adapters.

USB Wireless LAN Adapters

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

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

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

Supported Wireless LAN Configuration

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

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

Important: Supported 802.11 network protocols vary according to the wireless LAN adapter being used with the PX. See *USB Wireless LAN Adapters* (on page 22).

Initial Network Configuration via CLI

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

This section describes the initial network configuration via a serial RS-232 or USB connection. To configure the network settings using the web interface, see ***Modifying the Network Configuration*** (on page 130).

To configure the PX device:

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

   Tip: For a USB connection, you can determine the COM port by choosing Control Panel > System > Hardware > Device Manager, and locating the "Dominion PX2 Serial Console" under the Ports group.
3. In the communications program, press Enter to send a carriage return to the PX.
4. The PX prompts you to log in. Both user name and password are case sensitive.

a. Username: `admin`

b. Password: `raritan` (or a new password if you have changed it).

5. If prompted to change the default password, change or ignore it.
   - To change it, follow onscreen instructions to type your new password.
   - To ignore it, simply press Enter.
6. The # prompt appears.
7. Type `config` and press Enter.
8. To configure network settings, type appropriate commands and press Enter. All commands are case sensitive.

   a. To set the networking mode, type this command:

   ```
   network mode <mode>
   ```

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

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

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

Tip: You can combine multiple commands to configure multiple parameters at a time. For example,
`network interface LANInterfaceSpeed <option> LANInterfaceDuplexMode <mode>`

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

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

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

To set	Use this command
BSSID	`network wireless BSSID <bssid>` <bssid> = AP MAC address or *none*
Authentication method	`network wireless authMethod <method>` <method> = *psk* or *eap*
PSK	`network wireless PSK <psk>` <psk> = PSK string
EAP outer authentication	`network wireless eapOuterAuthentication <outer_auth>` <outer_auth> = *PEAP*
EAP inner authentication	`network wireless eapInnerAuthentication <inner_auth>` <inner_auth> = *MSCHAPv2*
EAP identity	`network wireless eapIdentity <identity>` <identity> = your user name for EAP authentication
EAP passord	`network wireless eapPassword` When prompted to enter the password for EAP authentication, type the password.
EAP CA certificate	`network wireless eapCACertificate` When prompted to enter the CA certificate, open the certificate with a text editor, copy and paste the content into the communications program.

The content to be copied from the CA certificate does NOT include the first line containing "BEGIN CERTIFICATE" and the final line containing "END CERTIFICATE." If a certificate is installed, configure the following:

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

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

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

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

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

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

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

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

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

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

`network <version> overrideDNS <option>`

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

- For static IP configuration, configure these parameters.

To set	Use this command
Static IPv4 or IPv6 address	`network <version> ipAddress <ip address>` <ip address> = static IP address
IPv4 subnet mask	`network ipv4 subnetMask <netmask>` <netmask> = subnet mask
IPv4 or IPv6 gateway	`network <version> gateway <ip address>` <ip address> = gateway's IP address

To set	Use this command
IPv4 or IPv6 primary DNS server	`network <version> primaryDNSServer <ip address>` <ip address> = IP address of the primary DNS server
IPv4 or IPv6 secondary DNS server (optional)	`network <version> secondaryDNSServer <ip address>` <ip address> = IP address of the secondary DNS server

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

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

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

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

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

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

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

The IP address configured may take seconds to take effect.

Cascading the PX via USB

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

The first device in the chain is the master device and all the other are slave devices. All devices in the chain are accessible over the network, with the bridging or port-forwarding cascading mode activated on the master device. See ***Setting the Cascading Mode*** (on page 154).

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

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

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

To cascade the PX devices via USB:

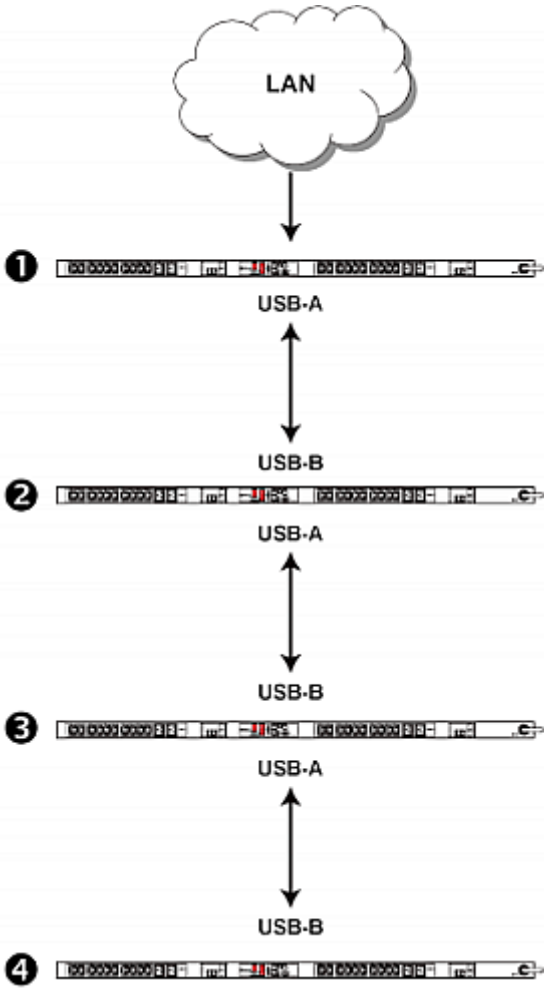
1. Verify that the PDUs to be cascaded are running the following firmware versions by choosing Maintenance > Device Information. If not, upgrade these devices. See ***Updating the PX Firmware*** (on page 342).
   - PX2 series: version 2.3.1 or later
   - PX3 series: version 2.5.10 or later

   Note: Port forwarding mode over wireless LAN is supported as of release 3.1.0. You must upgrade all devices in the chain to version 3.1.0 or higher if wireless networking is preferred.
2. Select one of the devices as the master device.
   - When the port forwarding mode over wireless LAN is intended, the master device must be a Raritan product with two USB-A ports, such as PX3, EMX2-888, PX3TS or BCM2.
3. Connect the master device to the LAN via:
   - A standard network patch cable (CAT5e or higher) if the bridging mode is intended.
   - A standard network patch cable or a Raritan USB WIFI wireless LAN adapter if the port forwarding mode is intended.

     For information on the Raritan USB WIFI adapter, see ***USB Wireless LAN Adapters*** (on page 22).

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

   Do NOT connect any slave device to the LAN. That is, there is no connection of a standard network cable or USB wireless LAN adapter to the slave devices.
7. Log in to the master device to configure the cascading mode. See ***Setting the Cascading Mode*** (on page 154) or ***Configuring the Cascading Mode*** (on page 502).
8. Configure the master and/or each slave device's networking settings.
   - Bridging mode: You need to configure each cascaded device's network settings respectively.
   - Port forwarding mode: Only the mater device's network settings must be configured.



Number	Device role
1	Master device
2	Slave 1
3	Slave 2
4	Slave 3

Note: To remotely identify the master and slave devices and their positions in the USB-cascading configuration, see **Identifying Cascaded Devices** *(on page 126).*

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

Bulk Configuration Methods

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

Use a bulk configuration file:

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

See ***Bulk Configuration*** (on page 319).

Use a TFTP server:

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

See ***Bulk Configuration or Firmware Upgrade via DHCP/TFTP*** (on page 557).

Use a USB flash drive:

- Requirement: A FAT32-formatted USB flash drive containing special configuration files is required.
- Procedure: Plug this USB drive into the PX. 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 546).

Installing Cable Retention Clips on Outlets (Optional)

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

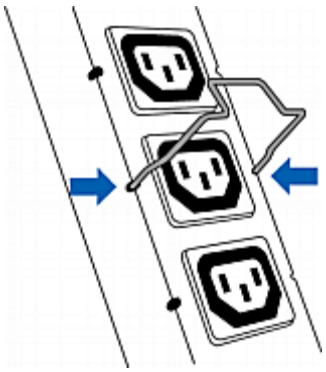
The use of cable retention clips is highly recommended for regions with high seismic activities, and environments where shocks and vibrations are expected.

These optional clips come in various sizes to accommodate diverse power cords used on IT equipment, which are connected to C13 or C19 outlets. You can request a cable retention kit containing different sizes of clips from you reseller. Make sure you use a clip that fits the power cord snugly to facilitate the installation or removal operation (for servicing).

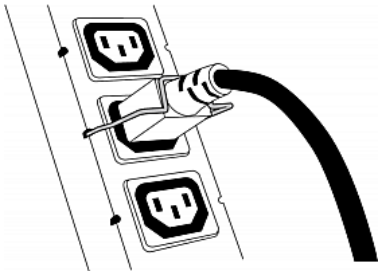
Note: Some NEMA sockets on PSE-certified PDUs for Japan have integral locking capability and do not need cable retention clips. See **Locking Outlets and Cords** *(on page 662).*

To install and use a cable retention clip on the outlet:

1. Locate two tiny holes at two sides of an outlet.
2. Install the cable retention clip by inserting two ends of the clip into the tiny holes.



3. Plug the power cord into the outlet, and press the clip toward the power cord until it holds the cord firmly. The clip's central part holding the plug should face downwards toward the ground, like an inverted "U". This allows gravity to keep the clip in place.



4. Repeat the same steps to install clips and power cords on the other outlets.

Chapter 4 Connecting External Equipment (Optional)

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

In This Chapter

Connecting Environmental Sensor Packages 35
Connecting Asset Management Sensors 54
Connecting a Logitech Webcam 63
Connecting a GSM Modem 64
Connecting an Analog Modem 64
Connecting an External Beeper 65
Connecting a Schroff LHX/SHX Heat Exchanger 65

Connecting Environmental Sensor Packages

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

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

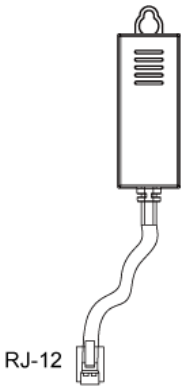
The PX can manage a maximum of 32 sensors and/or actuators. The supported maximum cabling distance is 98 feet (30 m), except for DPX sensor packages.

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

- ***DPX Sensor Packages*** (on page 36)
- ***DPX2 Sensor Packages*** (on page 41)
- ***DPX3 Sensor Packages*** (on page 43)
- ***DX Sensor Packages*** (on page 45)

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 40).

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 the PX3.

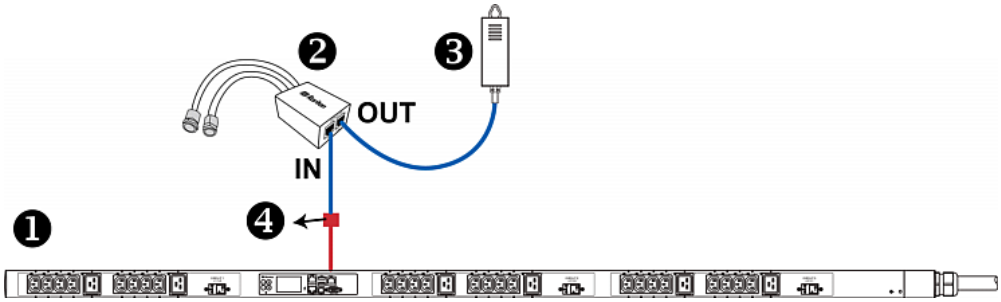
a. Connect the adapter's RJ-12 connector to the DPX sensor cable.

b. Connect the adapter's RJ-45 connector to the RJ-45 SENSOR port of the PX3.

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 PX3.

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 PX device
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 PX. This allows you to connect up to four DPX sensor packages to the PX via the hub.

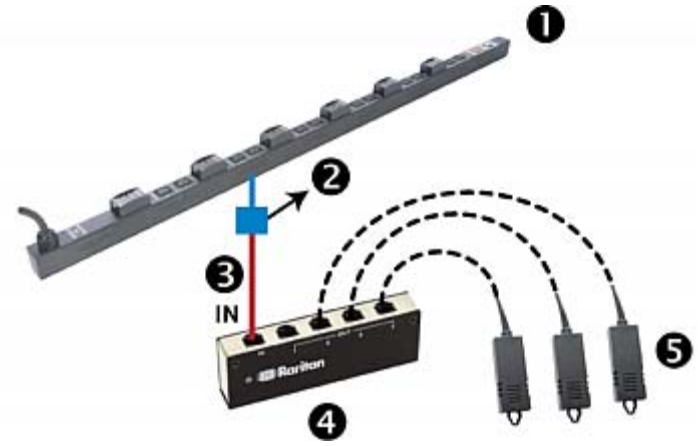
The DPX-ENVHUB4 sensor hub supports DPX sensor packages only. Do NOT connect DPX2, DPX3 or DX sensor packages to this hub.

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

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

1. Connect the DPX-ENVHUB4 sensor hub to the PX.
   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	The PX device
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

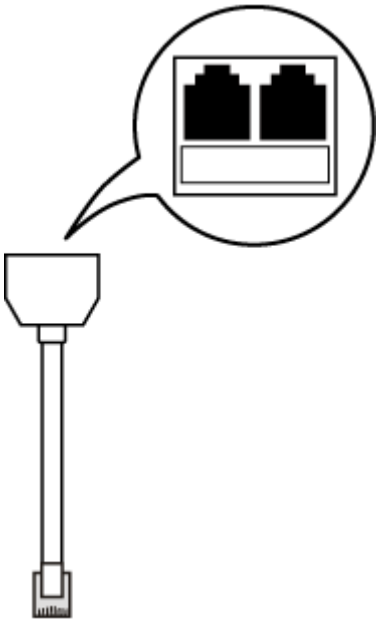
A Raritan *DPX-ENVHUB2* cable doubles the number of connected environmental sensors per SENSOR port.

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

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

1. Use an RJ-12 to RJ-45 adapter to connect the DPX-ENVHUB2 cable to the PX3.
   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 PX3.

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 PX.

Supported Maximum DPX Sensor Distances

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

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

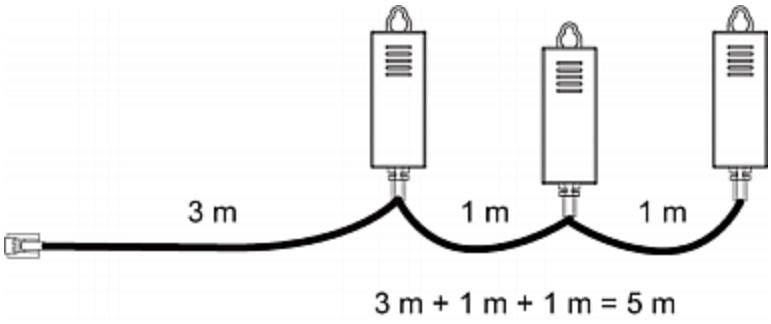
Sensor Connection Restrictions:

- Connect a DPX sensor package to the PX 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 PX 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 a PX via a sensor hub.

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



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

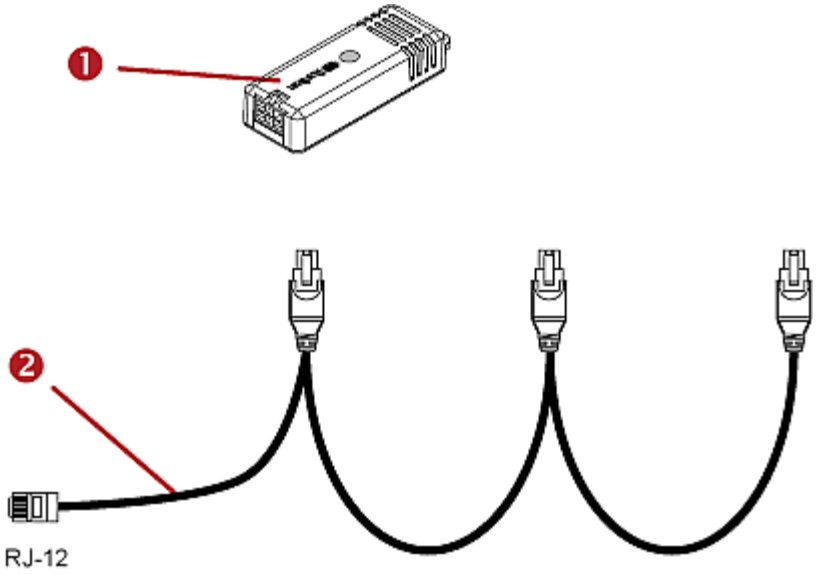
  Note that the length 16' (5 m) is the length of each DPX-T3H1 sensor cable, which is defined in the above diagram.

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

DPX2 Sensor Packages

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

For more information on DPX2 sensor packages, access the Environmental Sensors Guide or Online Help on Raritan website's ***Support page*** (***http://www.raritan.com/support/***).



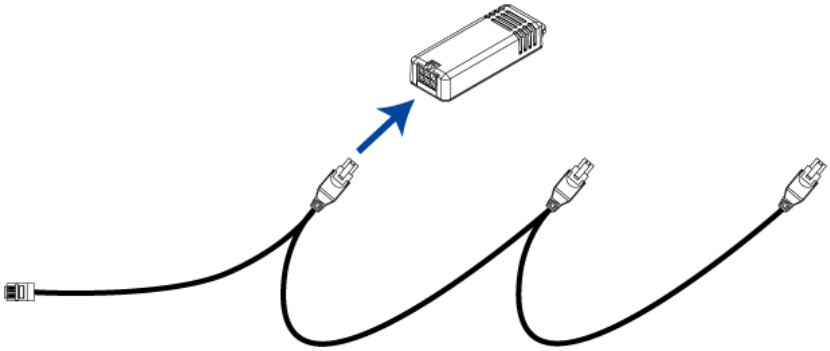
Item	
1	DPX2 sensor package
2	DPX2 sensor cable with one RJ-12 connector and three head connectors

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

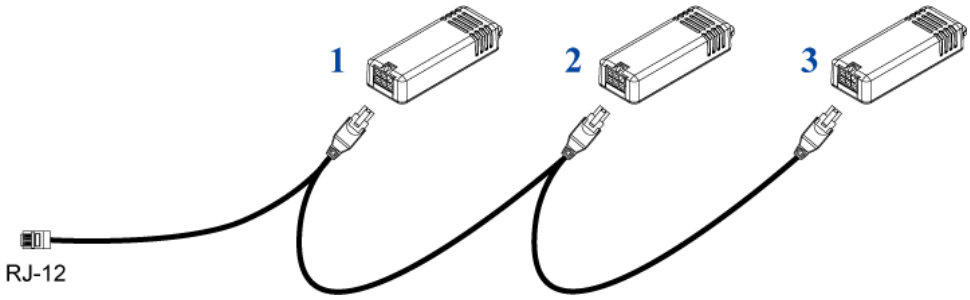
Warning: If there are free head connectors between a DPX2 sensor cable's RJ-12 connector and the final attached DPX2 sensor package, the sensor packages following the free head connector(s) on the same cable do NOT work properly. Therefore, always occupy all head connectors prior to the final sensor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

To connect DPX2 sensor packages to the PX:

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 PX3.
   a. Connect the adapter's RJ-12 connector to the DPX2 sensor cable.

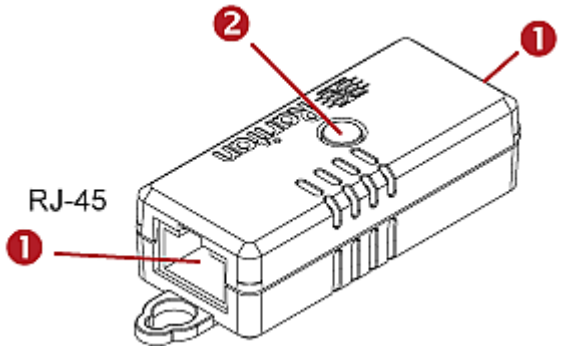
b. Connect the adapter's RJ-45 connector to the RJ-45 SENSOR port of the PX3.

OR you can directly connect the DPX2 sensor package to a DX sensor chain without using any RJ-12 to RJ-45 adapter. See ***Connecting a DPX2 Sensor Package to DX*** (on page 47).

DPX3 Sensor Packages

A DPX3 sensor package features the following:

- Its connection interface is RJ-45.
- You can cascade a maximum of 12 DPX3 sensor packages.

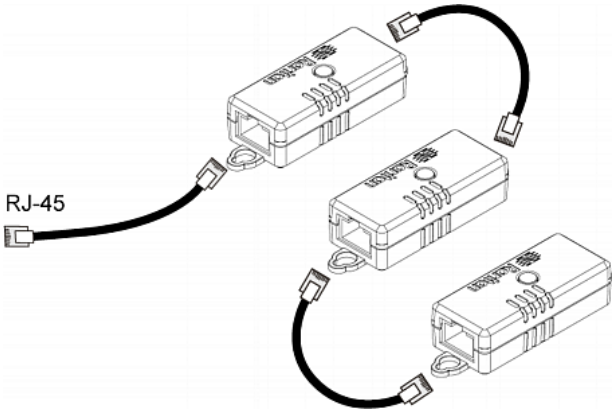


Numbers	Components
❶	RJ-45 ports, each of which is located on either end of a DPX3 sensor package.
❷	LED for indicating the sensor status.

To connect DPX3 sensor packages to the PX:

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 PX3 by plugging its cable's connector into the RJ-45 SENSOR port of the PX3.

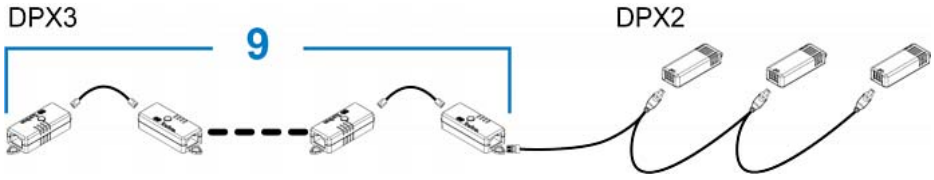
Connecting a DPX2 Sensor Package to DPX3

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

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

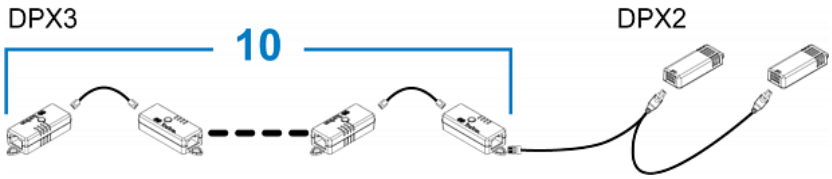
- **When connecting a DPX2 sensor package containing three DPX2 sensors:**

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



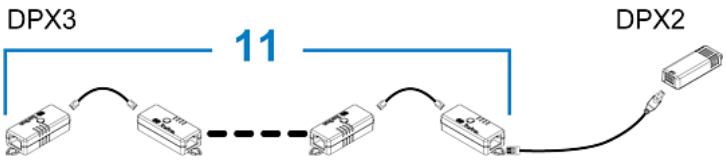
- **When connecting a DPX2 sensor package containing two DPX2 sensors:**

  A maximum of ten DPX3 sensor packages can be cascaded because 12-2=10.



When connecting a DPX2 sensor package containing one DPX2 sensor:

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



DX Sensor Packages

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

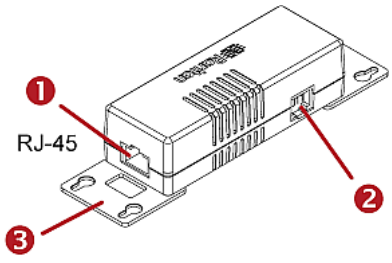
You can cascade up to 12 DX sensor packages.

When cascading DX, remember that the PX 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 PX.

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

Tip: To manage the last 4 functions, you can release 4 sensors or actuators that have been under management, and then manually bring the last 4 functions into management. See **Unmanaging Environmental Sensors or Actuators** *(on page 311) and* **Managing Environmental Sensors or Actuators** *(on page 300).*



Numbers	Components
1	RJ-45 ports, each of which is located on either end of a DX sensor package.

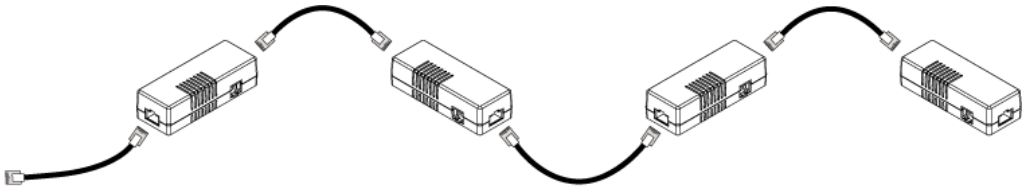
Numbers	Components
❷	RJ-12 port, which is reserved for future use and now blocked.
❸	Removable rackmount brackets.

Connect DX sensor packages to the PX:

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

   Repeat the same steps to cascade more DX packages.

Exception: You CANNOT cascade DX-PD2C5 sensor packages. A PX device supports only one DX-PD2C5.



3. Connect the first DX sensor package to the PX3 by plugging its cable's connector into the RJ-45 SENSOR port of the PX3.
4. If needed, connect a DPX2 sensor package to the end of the DX chain. See ***Connecting a DPX2 Sensor Package to DX*** (on page 47).

Warning: The PX3 does NOT support simultaneous connection of both DX-PD2C5 and asset management sensor(s) so do NOT connect both of them to the PX3 device.

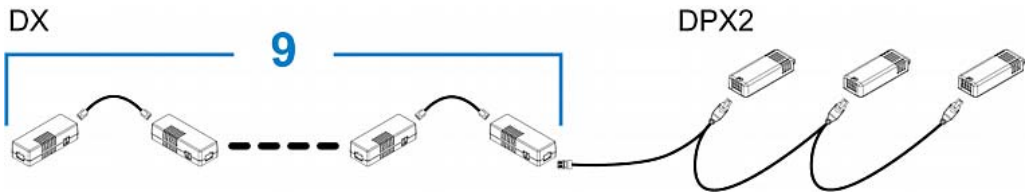
Connecting a DPX2 Sensor Package to DX

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

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

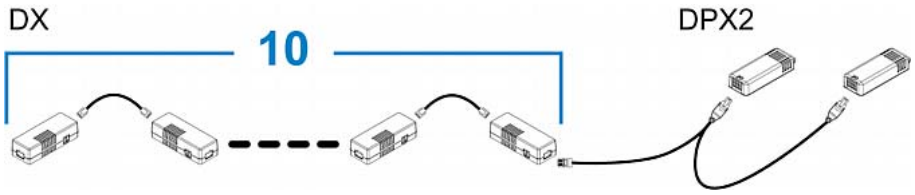
- **When connecting a DPX2 sensor package containing three DPX2 sensors:**

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



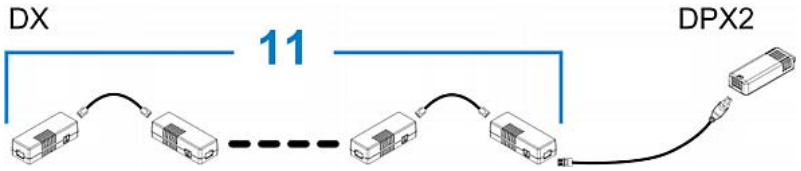
- **When connecting a DPX2 sensor package containing two DPX2 sensors:**

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



- **When connecting a DPX2 sensor package containing one DPX2 sensor:**

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



Using an Optional DPX3-ENVHUB4 Sensor Hub

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

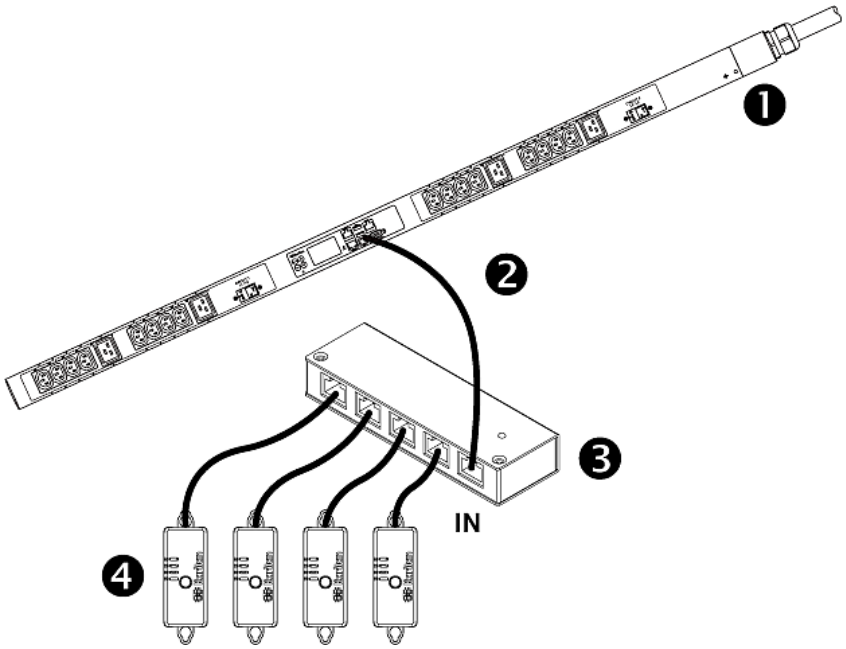
- All ports on the DPX3-ENVHUB4 sensor hub are RJ-45 instead of RJ-12 as the DPX-ENVHUB4 sensor hub.
- The DPX3-ENVHUB4 sensor hub supports all Raritan environmental sensor packages, including DPX, DPX2, DPX3 and DX sensor packages.

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

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

1. Connect the DPX3-ENVHUB4 sensor hub to the PX 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 PX.
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.



1	The PX
2	A standard network cable
3	DPX3-ENVHUB4 sensor hub
4	Any Raritan sensor packages

Mixing Diverse Sensor Types

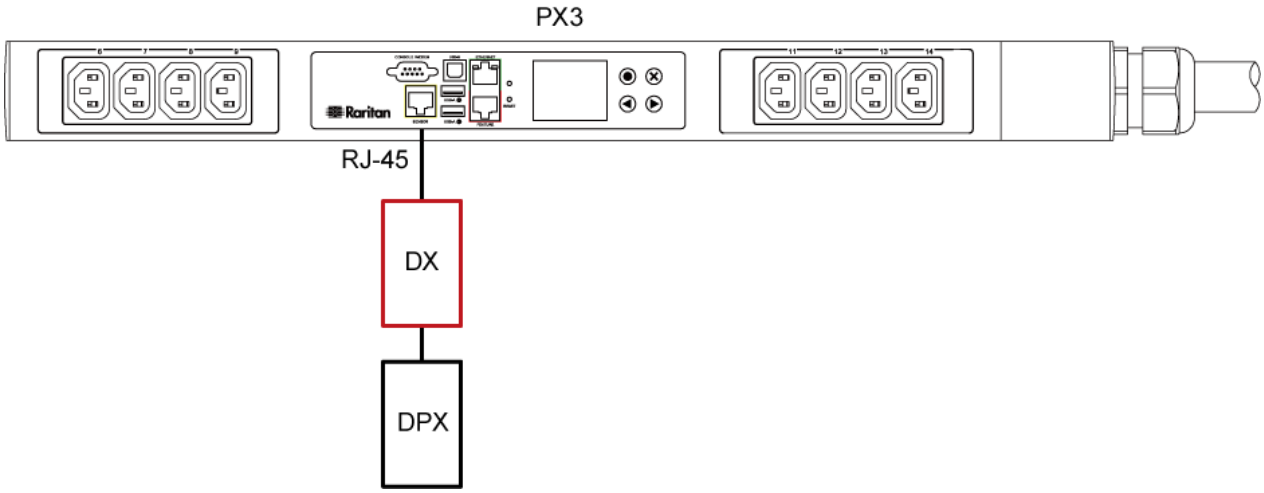
You can mix DPX, DPX2, DPX3 and DX sensor packages on one PX according to the following sensor combinations. In some scenarios, the DPX3-ENVHUB4 sensor hub is required.

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

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

1 DX + 1 DPX:

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

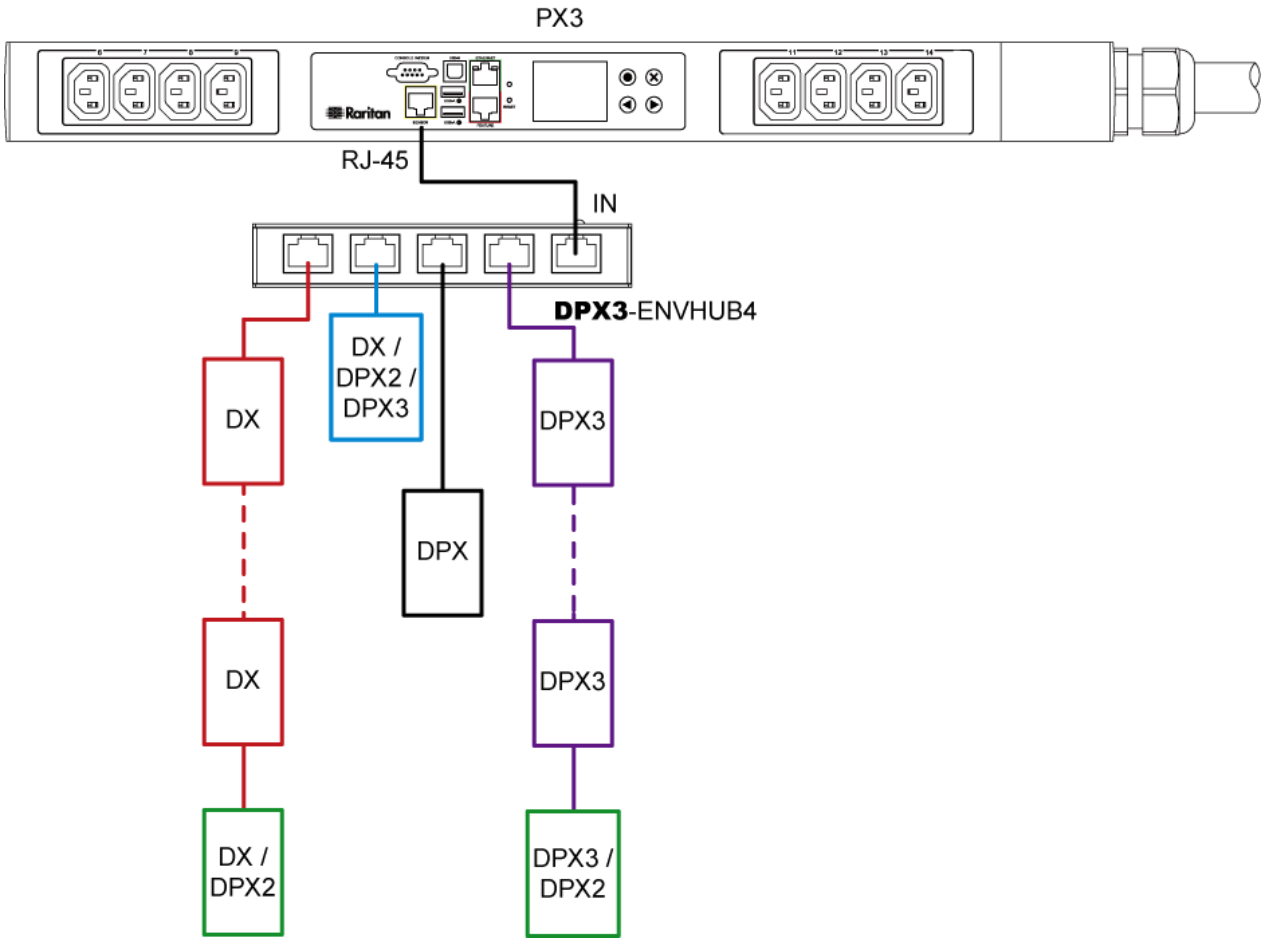


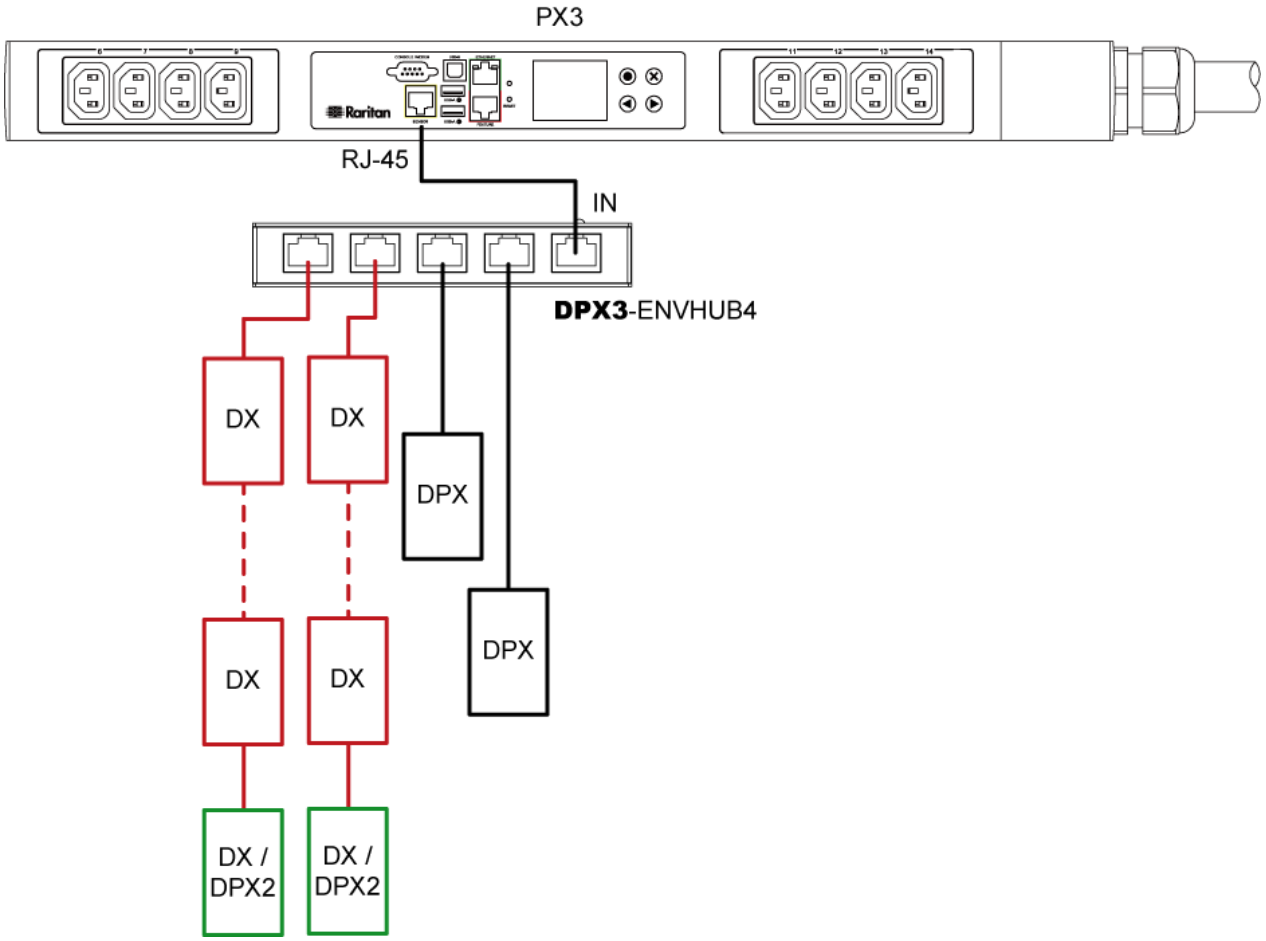
Diverse combinations via the DPX3-ENVHUB4 sensor hub:

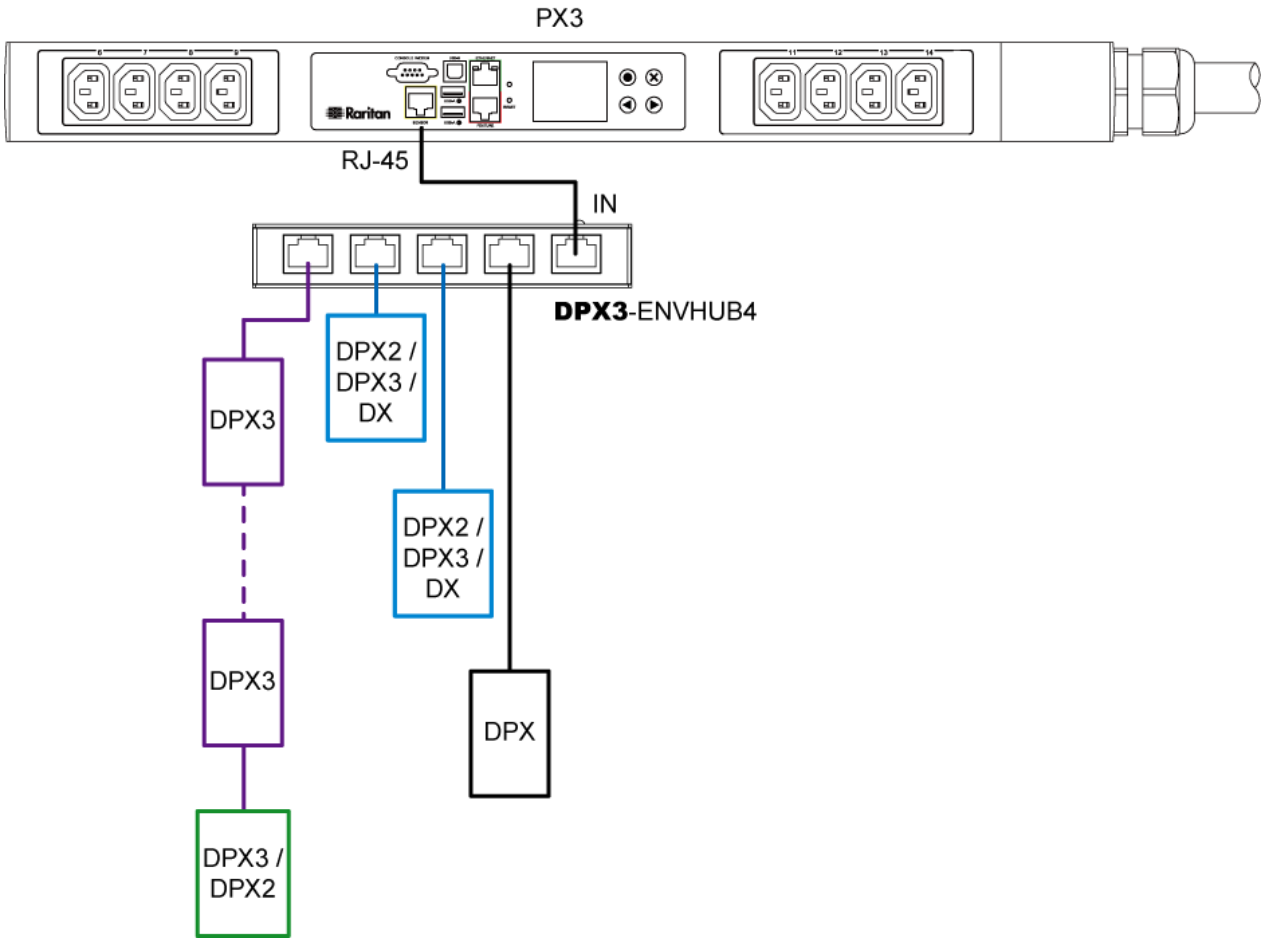
- You must use the **DPX3**-ENVHUB4 sensor hub instead of the old DPX-ENVHUB4 sensor hub. Each port on the hub supports any of the following:
  - A DX sensor package
  - A chain of DX sensor packages
  - A DPX3 sensor package
  - A chain of DPX3 sensor packages
  - A DPX2 sensor package
  - A DPX sensor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

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

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

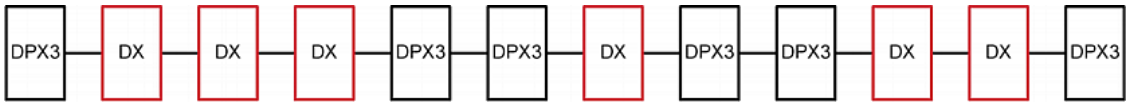



PX3
RJ-45
IN
DPX3-ENVHUB4
DX
DX
DPX
DX
DX
DPX
DX / DPX2
DX / DPX2



Mix DPX3 and DX in a sensor chain:

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



You can add a DPX2 sensor package to the end of such a sensor-mixing chain if intended. See ***Connecting a DPX2 Sensor Package to DPX3*** (on page 44) or ***Connecting a DPX2 Sensor Package to DX*** (on page 47).

Connecting Asset Management Sensors

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

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

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

Warning: The PX3 does NOT support simultaneous connection of both DX-PD2C5 and asset management sensor(s) so do NOT connect both of them to the PX3 device.

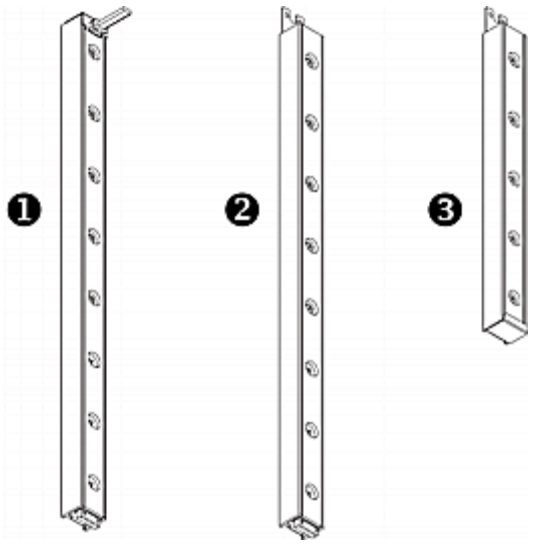
Combining Regular Asset Sensors

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

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

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

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



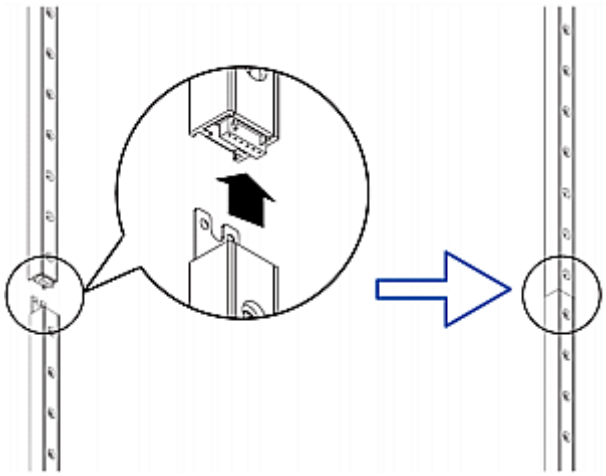
1	8U MASTER asset sensor with 8 tag ports

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

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

To assemble asset sensors:

1. Connect a MASTER asset sensor to an 8U SLAVE asset sensor.
   - Plug the white male DIN connector of the slave asset sensor into the white female DIN connector of the master asset sensor.
   - Make sure that the U-shaped sheet metal adjacent to the male DIN connector is inserted into the rear slot of the master asset sensor. Screw up the U-shaped sheet metal to reinforce the connection.



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

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

Connecting Regular Asset Sensors to the PX

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

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

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

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

The following diagram illustrates an asset tag.

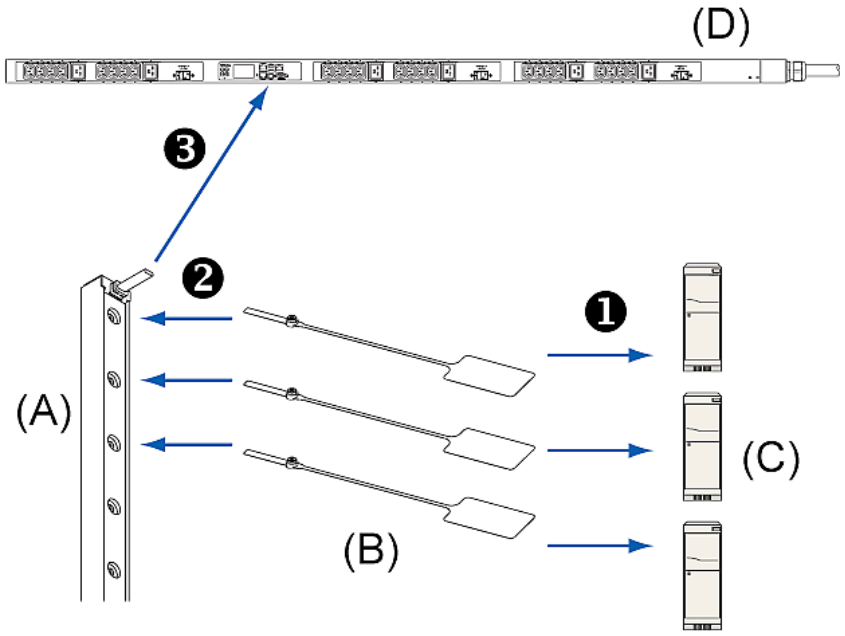
A	Barcode (ID number), which is available on either end of the asset tag
B	Tag connector
C	Adhesive area with the tape

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

To connect regular asset sensors to the PX device:

1. Affix the adhesive end of an asset tag to each IT device through the tag's tape.
2. Plug the connector of each asset tag into the corresponding tag port on the asset sensor.
3. Connect the asset sensor assembly to the PX device, using a network patch cable (CAT5e or higher).
   a. Connect one end of the cable to the RJ-45 connector on the MASTER asset sensor.
   b. Connect the other end of the cable to the FEATURE port on the PX device.

The PX device supplies power to the connected asset sensor assembly. All LEDs on the asset sensor assembly may cycle through different colors during the power-on process if the asset sensor's firmware is being upgraded by the PX device. After the power-on or firmware upgrade process completes, the LEDs show solid colors. Note that the LED color of the tag ports with asset tags connected will be different from the LED color of the tag ports without asset tags connected.



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

Note: The PX cannot detect how many rack units the connected asset sensor(s) has. You must provide the information to it manually. See **Configuring the Asset Sensor** *(on page 314).*

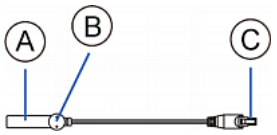
Connecting Blade Extension Strips

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

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

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

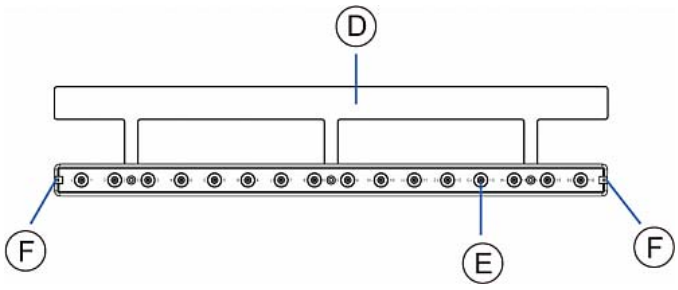
Tag connector cable



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

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

Blade extension strip with 16 tag ports



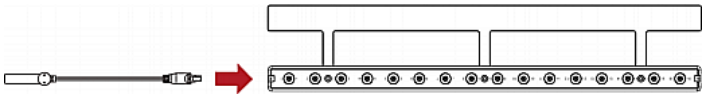
D	Mylar section with the adhesive tape

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

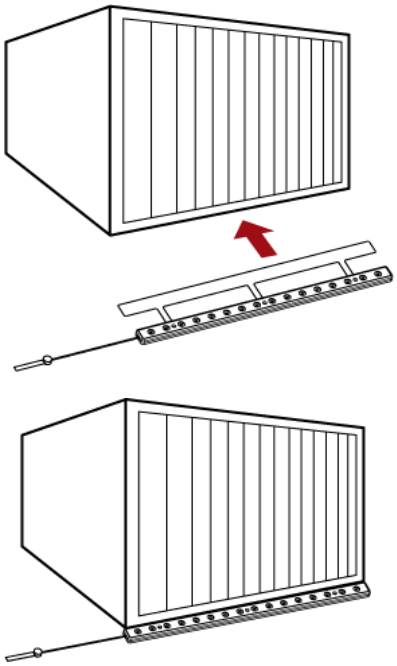
Note: Each tag port on the blade extension strip is labeled a number, which is displayed as the slot number in the PX device's web interface.

To install a blade extension strip:

1. Connect the tag connector cable to the blade extension strip.
   - Plug the cable's connector into the socket at either end of the blade extension strip.



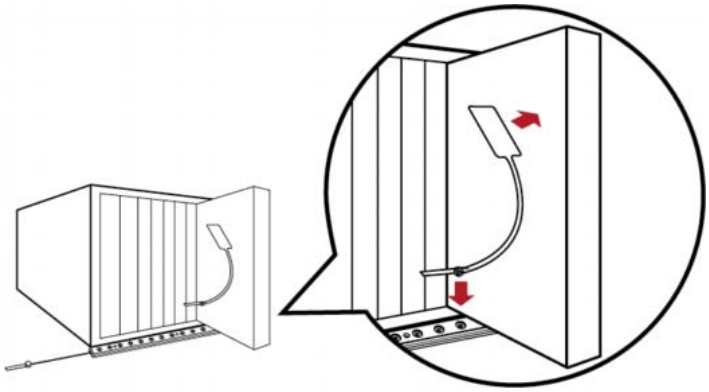
2. Move the blade extension strip toward the bottom of the blade chassis until its mylar section is fully under the chassis, and verify that the blade extension strip does not fall off easily. If necessary, you may use the adhesive tape in the back of the mylar section to help fix the strip in place.



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

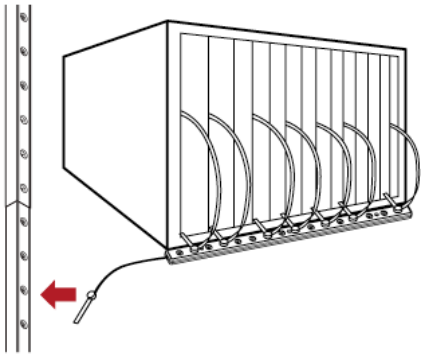
a. Affix the adhesive part of the asset tag to one side of a blade server through the tag's tape.

b. Plug the tag connector of the asset tag into a tag port on the blade extension strip.



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

5. Plug the tag connector of the blade extension strip into the closest tag port of the regular or composite asset sensor on the rack.



6. Repeat the above steps to connect additional blade extension strips. Up to 128 asset tags on blade extension strips are supported per FEATURE port.

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

Connecting Composite Asset Sensors (AMS-Mx-Z)

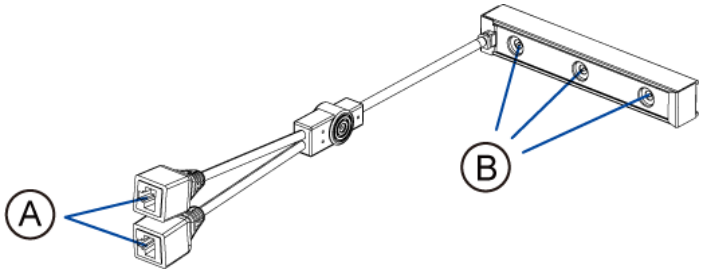
A composite asset sensor is named AMS-Mx-Z, where x is a number, such as AMS-M2-Z or AMS-M3-Z. It is a type of asset sensor that functions the same as regular MASTER asset sensors except for the following differences:

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

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

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

The following diagram illustrates AMS-M3-Z.

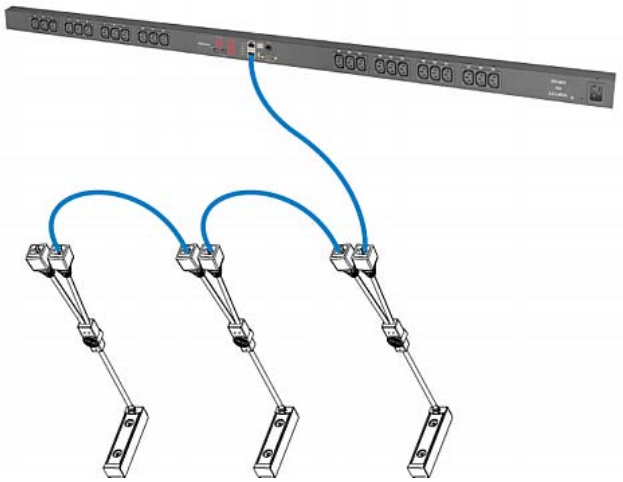


A	Two RJ-45 connectors
B	Tag ports

To connect composite asset sensors to the PX device:

1. Connect a composite asset sensor to the PX device via a standard network patch cable (CAT5e or higher).
   a. Connect one end of the cable to the RJ-45 port labeled "Input" on the composite asset sensor.
   b. Connect the other end of the cable to the FEATURE port on the PX device.
2. Affix an asset tag to the IT device. Then connect this asset tag to the composite asset sensor by plugging the tag connector into the tag port on the composite asset sensor. For details, see ***Connecting Regular Asset Sensors to the PX*** (on page 56).

3. If necessary, daisy chain *the same* type of composite asset sensors to track more IT devices.
   a. Get a standard network patch cable that is within 2 meters.
   b. Connect one end of the network cable to the RJ-45 connector labeled "Output" on the previous composite asset sensor.
   c. Connect the other end of the cable to the RJ-45 connector labeled "Input" on the subsequent composite asset sensor.
   d. Repeat the above steps to connect more composite asset sensors. See ***Daisy-Chain Limitations of Composite Asset Sensors*** (on page 62) for the maximum number of composite asset sensors supported per chain.
   e. It is highly recommended using the cable ties to help hold the weight of all connecting cables.



4. Repeat Step 2 to connect IT devices to the other composite asset sensors in the chain.

Important: Do NOT mix AMS-M2-Z and AMS-M3-Z in a chain.

Daisy-Chain Limitations of Composite Asset Sensors

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

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

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

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

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

Connecting a Logitech Webcam

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

The following UVC-compliant webcams are supported:

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

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

The PX supports up to two webcams. After connecting a webcam, you can retrieve visual information from anywhere through the PX web interface. If your webcam supports audio, audio is available with videos.

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

To connect a webcam:

1. Connect the webcam to the USB-A port on the PX device. The PX 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 PX web interface after the connection is complete. See ***Viewing Webcam Snapshots or Videos*** (on page 325).

Connecting a GSM Modem

A Cinterion® MC52iT or MC55iT GSM modem can be connected to the PX in order to send SMS messages containing event information. See ***Creating Actions*** (on page 237) for more information on SMS messages.

Note: PX cannot receive SMS messages.

To connect the GSM modem:

1. Connect the GSM modem to the serial port labeled CONSOLE / MODEM on the PX.
2. Configure the GSM modem as needed. See the supporting GSM modem help for information on configuring the GSM modem.
3. Configure the GSM modem settings in PX.
   a. Click Device Settings > Serial Port Settings. The Serial Port Configuration dialog opens.
   b. If needed, enter the GSM modem SIM PIN.

Connecting an Analog Modem

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

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

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

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

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

To connect an analog modem:

1. Plug a telephone cord into the phone jack of the supported modem.

2. Plug the modem's RS-232 cable into the serial port labeled CONSOLE / MODEM on the PX.

You need to enable the modem dial-in support to take advantage of this feature, see ***Configuring the Serial Port*** (on page 153).

Connecting an External Beeper

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

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

- Mallory Sonalert MODEL SNP2R

After having an external beeper connected, you can create event rules for the PX to switch on or off the external beeper when specific events occur. See ***Creating an Event Rule*** (on page 236).

To connect an external beeper:

1. Connect a standard network patch cable to the FEATURE port of the PX.
2. Plug the other end of the cable into the external beeper's RJ-45 socket.

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

Connecting a Schroff LHX/SHX Heat Exchanger

Note: Only the PDUs whose model names begin with PX2 or PX3 support the LHX/SHX heat exchangers.

To remotely monitor and administer the Schroff® LHX-20, LHX-40 and SHX-30 heat exchangers through the PX device, you must establish a connection between the heat exchanger and the PX device.

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

To establish a connection between the PDU and LHX/SHX heat exchanger, an RJ-45 to RS-232 adapter cable provided by Schroff is required.

To connect an LHX or SHX heat exchanger:

1. Plug the RS-232 DB9 end of the adapter cable into the RS-232 port on the Schroff LHX/SHX heat exchanger.
2. Plug the RJ-45 end of the cable into the port labeled FEATURE on your PX device.

See ***Managing the Schroff LHX/SHX Heat Exchanger*** (on page 334) for enabling the support of the LHX/SHX heat exchanger.

Chapter 5 Using the PDU

This chapter explains how to use the PX device. It describes the LEDs and ports on the PDU, and explains how to use the front panel display. It also explains how the overcurrent protector works and when the beeper sounds.

In This Chapter

Panel Components 67
Circuit Breakers 99
Fuse 101
Beeper 104
Replaceable Controller 105

Panel Components

The PX 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 (PX3 phase II models)

  Note: PX3 phase I models contain a character LCD display instead of a dot-matrix LCD display. For information on the character LCD display, see **PX3 Phase I LCD Display** *(on page 601).*

- Reset button

Connection ports, LCD display and reset button are located on a replaceable controller of the PX3 phase II model. See ***Replaceable Controller*** (on page 105).

Note: An older PX3 phase I model does not support a replaceable controller.

Inlet

Most of PX3 PDUs are shipped with a locking line cord, which is ready to be plugged into the PDU's inlet and an appropriate receptacle for electricity reception. Such devices cannot be rewired by the user.

A locking line cord helps secure the cord connection. For details, see ***Connecting a Locking Line Cord*** (on page 15).

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

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

Besides, a PX3 "Zero U" model supports a relocatable inlet. See ***Zero U Models' Relocatable Inlet*** (on page 68).

Zero U Models' Relocatable Inlet

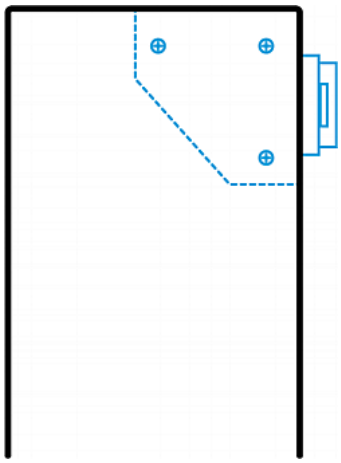
You can easily change the inlet's location from the side to the top or from the top to the side on a Zero U model.

Note: A PX3 phase I model does not support a relocatable inlet at the time of writing, but may support it later.

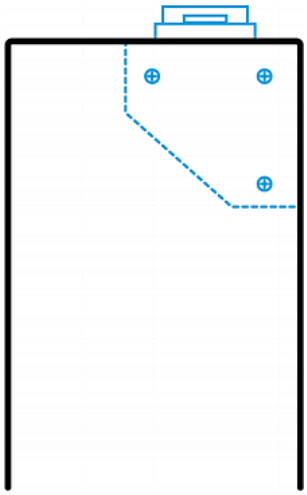
To change a PX3 inlet's position:

1. Power OFF the PDU.
2. Remove the screws at two sides of the inlet to uninstall the inlet module.
3. Re-install the inlet module in a manner that the inlet is located at the desired position.

Inlet on the side



Inlet on the top



Outlets

The total number of outlets varies from model to model.

PX3-3000 Series

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

Outlet LEDs are not available.

PX3-4000 Series

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

A small LED adjacent to each outlet indicates the outlet state. Outlet LEDs always light red, indicating that the outlet power is ON.

PX3-5000 Series

These models are outlet-switching capable. A small LED adjacent to each outlet indicates the outlet or PDU state. The PDU is shipped from the factory with all outlets turned ON. The table below explains how to interpret different outlet LED states.

LED state	Outlet status	What it means
Not lit	Powered OFF	The outlet is not connected to power, or the control circuitry's power supply is broken.

LED state	Outlet status	What it means
Red	ON and LIVE	LIVE power. The outlet is on and power is available.
Red flashing	ON and LIVE	The current flowing through the outlet is greater than the upper warning (non-critical) threshold.
Green	OFF and LIVE	The outlet is turned off and power is available when the outlet is turned on.
Green flashing	OFF and NOT LIVE	The outlet is turned off and power is not available because the circuit breaker has tripped.
Red and Green flashing alternatively	ON and NOT LIVE	The outlet is turned on but power is not available because a circuit breaker has tripped.
Cycling through Red, Green and Yellow	n/a	The PX device has just been plugged in and its management software is loading. LED color cycling does not interrupt power to outlets. It is an indication of firmware loading.

Note: When a PX device powers up, it proceeds with the power-on self test and software loading for a few moments. At this time, the outlet LEDs cycle through different colors. When the software has completed loading, the outlet LEDs show a steady color and the front panel display illuminates.

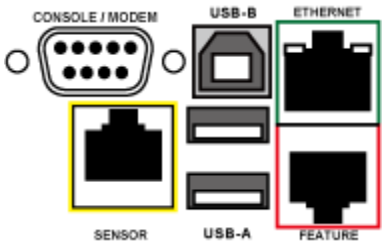
Connection Ports

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

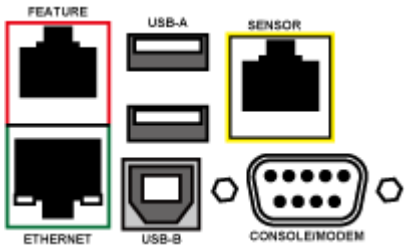
Zero U Connection Ports

For most of PX3 series Zero U models, there are 7 ports on the front panel. The PX3 PDU has two USB-A ports.

- PX3 Phase II models:



- PX3 Phase I models:



1U and 2U Port Locations

The difference between Zero U, 1U and 2U models is that Zero U models have all the connection ports located on the front panel while 1U and 2U models have the ports located respectively on the front and back panels.

Connection Port Functions

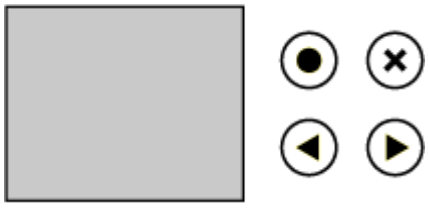
The table below explains the function of each port.

Port	Used for...
USB-B	• Cascading the PX devices for sharing a network connection. See ***Cascading the PX via USB*** (on page 29). • Establishing a USB connection between a computer and the PX for using the command line interface or performing the disaster recovery. For disaster recovery instructions, contact Raritan Technical Support.
USB-A	**This is a "host" port, which is powered, per USB 2.0 specifications.** • Connecting a USB device, such as a Logitech® webcam or wireless LAN adapter. • Cascading the PX devices for sharing a network connection.
FEATURE	Connection to one of the following devices: ▪ A Raritan access product, such as Dominion KX III KVM switch, with the use of a power CIM. ▪ A Schroff® LHX-20, SHX-30 or LHX-40 device, using an RJ-45 to RS-232 cable provided by Schroff. ▪ An external beeper with the RJ-45 socket. ▪ A Raritan asset management sensor, which allows you to track the locations of IT devices on the rack. See ***Connecting External Equipment (Optional)*** (on page 35). Warning: This is not an RS-232 port so do NOT plug in an RS-232 device, or damages can be caused to the device.

Port	Used for...
CONSOLE/ MODEM	Establishing a serial connection between the PX and a computer or modem. This is a standard DTE RS-232 port. You can use a null-modem cable with two DB9 connectors on both ends to connect the PX to the computer.
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.
ETHERNET	Connecting the PX to your company's network. Connect a standard Cat5e/6 UTP cable to this port and connect the other end to your network. This connection is necessary to administer or access the PX device remotely using the web interface. There are two small LEDs adjacent to the port: ▪ Green indicates a physical link and activity. ▪ Yellow indicates communications at 10/100 BaseT speeds. *Note: Connection to this port is not required if wireless connection is preferred, or if the PX is a slave device in the USB-cascading configuration. See* **Cascading the PX via USB** *(on page 29).*

Dot-Matrix LCD Display

The following diagram shows the dot-matrix LCD display panel on a Zero U PX3 **Phase II** model.



You can use the LCD display to view the PX information and even switch an outlet. It consists of:

- A dot-matrix LCD display
- Four control buttons

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

Zero U models automatically adjust the orientation of the content shown on the dot-matrix LCD display after detecting the direction in which the PX is installed.

1U and 2U models do NOT adjust the content's orientation.

Automatic and Manual Modes

After powering on or resetting the PX, the front panel LCD display first shows the Raritan logo and name, and then 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 PX, the display cycles between both the inlet and overcurrent protector information.

Note: You can make a PX with overcurrent protectors only show the inlet information in the automatic mode. See **Setting the LCD Display's Default View** *(on page 150).*

Manual mode:

To view more information or control outlets if your PX 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 76).

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

When an alert exists:

- In the automatic mode, when an alert occurs, the LCD display stops cycling through the inlet information, and warns you by showing the alerts notice in a yellow or red background. See ***Alerts Notice in a Yellow or Red Screen*** (on page 97).

  To enter the manual mode then, press ⊗ only.

- In the manual mode, both the top and bottom bars in a menu's screen will turn yellow or red to indicate the presence of any alert. See ***Operating the Dot-Matrix LCD Display*** (on page 75).

Control Buttons

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

Button	Function
	Up
	Down
	OK
	Back Switch between Automatic and Manual modes

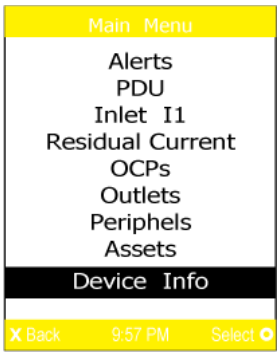
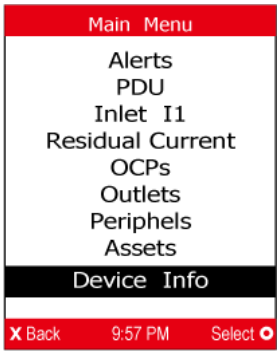
Operating the Dot-Matrix LCD Display

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

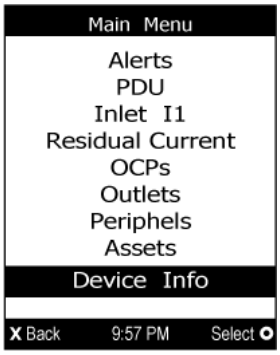
- Show information of the PDU, built-in components, or connected peripheral devices
- Control outlets if your model supports outlet-switching

Color changes of the menu's top and bottom bars:

- In the manual mode, both the top and bottom bars in a menu's screen will turn yellow or red to indicate the presence of any alert. See ***The Yellow- or Red-Highlighted Sensors*** (on page 119) for the definition of yellow and red colors.

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

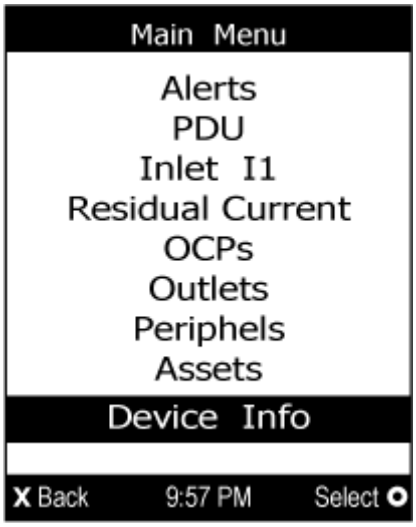
- Both bars turn black when there are NO alerts.

Screen with black bars


Main Menu

The Main Menu contains 6 to 9 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.



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 75).

Menu command	Function
Alerts	Indicates all alerted sensors, if any. See ***Alerts*** (on page 77).
PDU	Shows the internal beeper's state, and, if it is on, the reason for turning on. If your PX has multiple inlets, this menu item also shows the total active power and total active energy. See ***PDU*** (on page 79).
Inlet I1	Shows the inlet I1's information. See ***Inlet*** (on page 81).
Residual Current	Available only on PX models with residual current monitoring. See ***Front Panel Operations for RCM*** (on page 593).
OCPs	Shows a list of overcurrent protector information. See ***OCPs*** (on page 83). Only PX models with overcurrent protectors have this menu item.
Outlets	Shows each outlet's information. If your PX supports outlet-switching, you can turn on, off or power cycle an outlet. See ***Outlets*** (on page 84).
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 89).
Assets	Shows the asset management information if Raritan asset management equipment is connected to your PX. See ***Assets*** (on page 92).
Device Info	Shows the PX device's information, such as IP and MAC address. See ***Device Info*** (on page 93).

Note: To return to the automatic mode, press ⊗*. See* **Automatic and Manual Modes** *(on page 73).*

Alerts

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

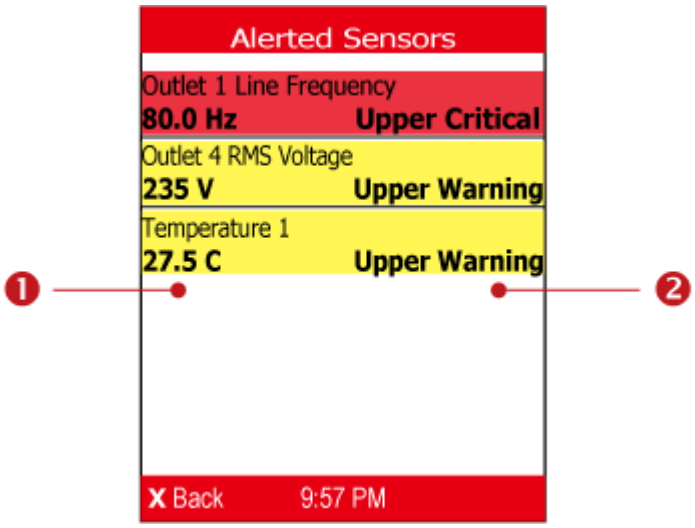
- Any sensor that enters the warning or critical range if the thresholds have been enabled
- Discrete (on/off) sensors that enter the alarmed state
- Any tripped circuit breakers or blown fuses

Tip: The same information is available in the PX web interface's Dashboard. See **Alerted Sensors** *(on page 122).*

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 available, are highlighted in either red or yellow. See ***The Yellow- or Red-Highlighted Sensors*** (on page 119) for color meanings.
   - 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 75).



Number	Description
1	Sensor names. For a numeric sensor, its reading is displayed right below the sensor name. For a discrete sensor, no reading is displayed.

Number	Description
❷	Sensor states as listed below. For further information, see ***States of Managed Sensors*** (on page 308). ▪ Alarmed ▪ Lower Critical = below lower critical ▪ Lower Warning = below lower warning ▪ Upper Warning = above upper warning ▪ Upper Critical = above upper critical ▪ Open (for overcurrent protectors)

3. Press ▲ or ▼ to view additional pages. When there are multiple pages, page numbers show in the top-right corner of the display.

PDU

Depending on the model you purchased, the "PDU" menu command may contain one or all of the following data.

- Internal beeper states - On or Off
- Total active power of the PX - available on a multi-inlet model only
- Total active energy of the PX - available on a multi-inlet model only
- Energy pulse output settings - available on PX3-4000 and PX3-5000 models only

Tip: The internal beeper state information is also available in the PX web interface. See **Checking the Internal Beeper State** *(on page 167).*

To view or configure PDU information:

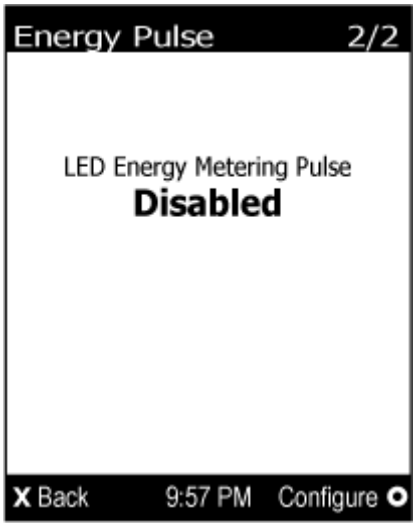
1. Press ▲ or ▼ to select "PDU" in the Main Menu, and press ●.
2. The internal beeper state is shown: Active or Off.

- For the Active state, the reason of turning on the beeper is indicated below the beeper state.

3. If your PX is a PX3-4000 or PX3-5000 model, it supports the active energy pulse output. Press ▼ to enter the Energy Pulse page.

   By default the energy pulsing is turned off. DO NOT enable this feature unless you want to verify a power meter's accuracy.

   Note: For more information, refer to the PX3 energy pulse setup guide on the Raritan website's **Support page** *(***http://www.raritan.com/support/***).*



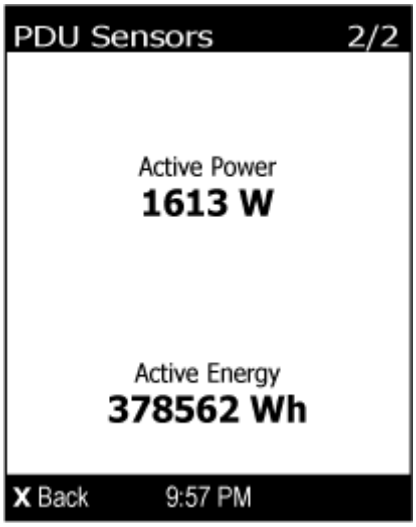
   a. To change the energy pulse settings, press ◉.

b. Press ▲ or ▼ to select an option.

c. Press ● to confirm the selection, or ✕ to cancel.

Note: All outlet LEDs on the PX turn OFF after enabling the energy pulsing. You still can turn on or off outlets during the pulsing period though outlet LEDs do not change their status.

4. If your PX has more than one inlet, press ▼ to show the information of total active power (W) and total active energy (Wh).



5. To return to the Main Menu, press ✕.

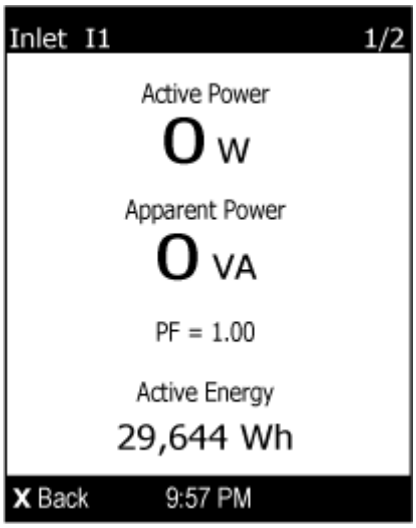
Inlet

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

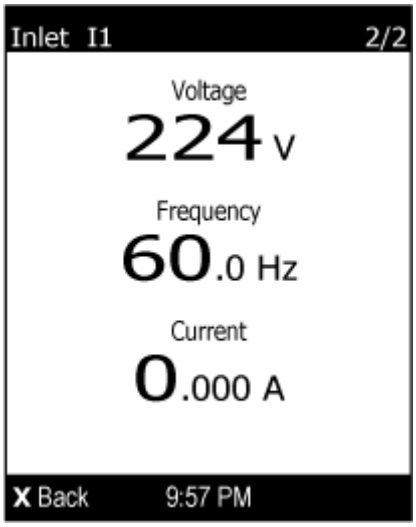
To show the inlet information:

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

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



3. To go to the next page, press ▲ or ▼.
   - For a single-phase model, the second page shows the inlet's voltage (V), frequency (Hz) and current (A) from top to down.



   - For a three-phase model, the next several pages respectively show the current value of each line, unbalanced current's percentage, line frequency, and voltage value of each line.

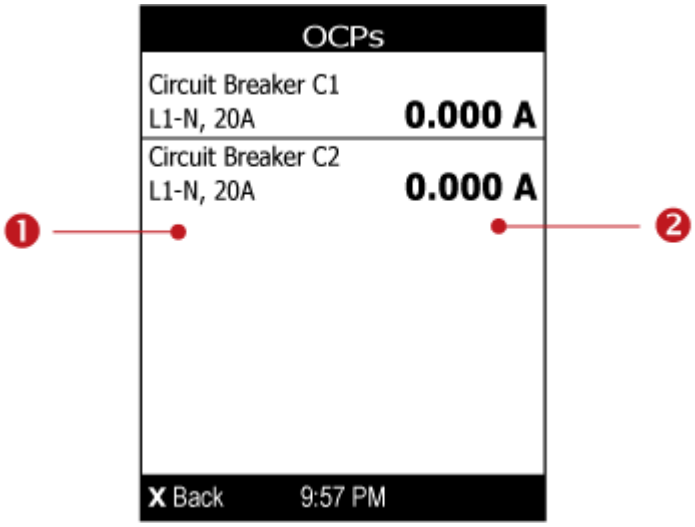
4. To return to the Main Menu, press ✕.

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
❶	Overcurrent protector names. Associated lines and rated current are displayed below each overcurrent protector's name.
❷	Current reading of the corresponding overcurrent protector.

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

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

Outlets

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 PX is outlet-switching capable. To do this, you must first enable the front panel outlet control function. See ***Enabling Front Panel Outlet Switching*** (on page 224).

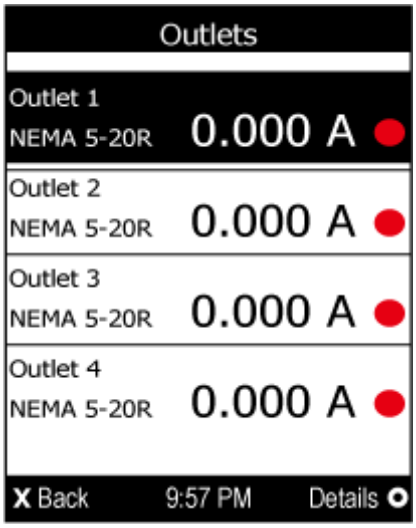
Showing an Outlet's Information

Multiple outlet information can be displayed on the LCD display. Page numbers are indicated in the top-right corner of the LCD display.

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

To show an outlet's information:

1. Press ▲ or ▼ to select "Outlets" in the Main Menu, and press ●.
2. The LCD display shows a list of outlets with their receptacle types, current values (A), and power states which are indicated by the colors of circles.
   - A red circle indicates that this outlet is powered on.
   - A green circle indicates that this outlet is powered off. If so, the word "Off" replaces the current value.

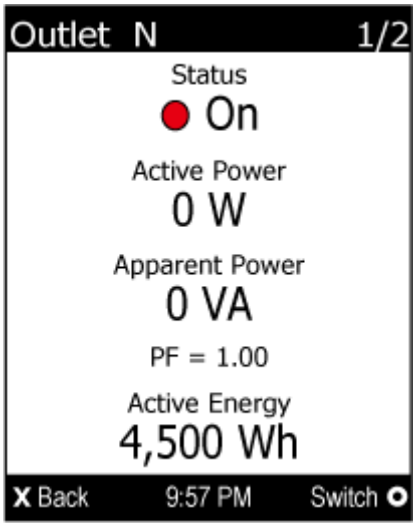


3. Press ▲ or ▼ to select an outlet, and press ●.

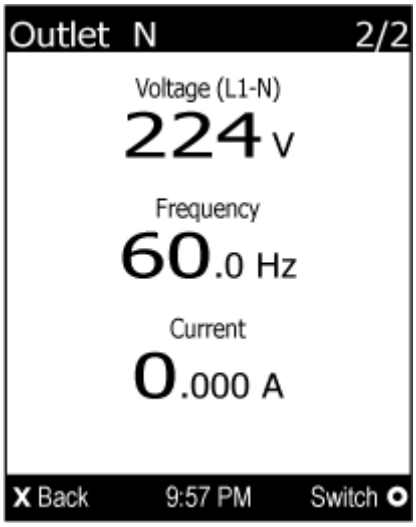
- If the desired outlet is not visible, press ▲ or ▼ to scroll up or down.

4. The LCD display shows the selected outlet's power state, active power (W), apparent power (VA), power factor (PF) and active energy (Wh) from top to down.

Note: In the following diagrams, N represents the selected outlet's number.



5. To go to the next page which shows the outlet's voltage (V), frequency (Hz) and current (A), press ▲ or ▼.



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

Power Control

This section applies to outlet-switching capable models only.

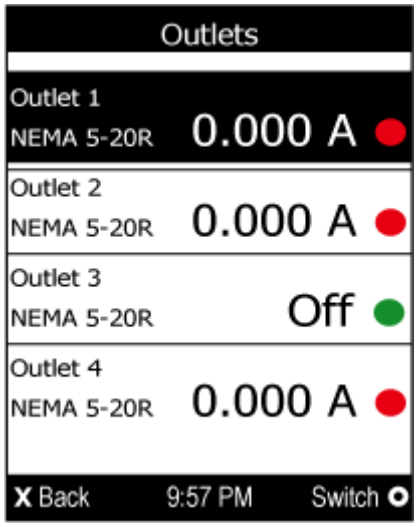
The front panel outlet control must be enabled for performing this power control function. The default is to disable this function. See ***Enabling Front Panel Outlet Switching*** (on page 224).

Available options for power control vary based on the power state of the selected outlet. For an outlet which has been turned on, the 'Switch On' option is unavailable. For an outlet which has been turned off, the "Switch Off" option is unavailable.

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

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

1. Press ▲ or ▼ to select "Outlets" in the Main Menu, and press ●.
2. The LCD display shows a list of outlets with their receptacle types, current values (A), and power states which are indicated by the colors of circles.
   - A red circle indicates that this outlet is powered on.
   - A green circle indicates that this outlet is powered off. If so, the word "Off" replaces the current value.

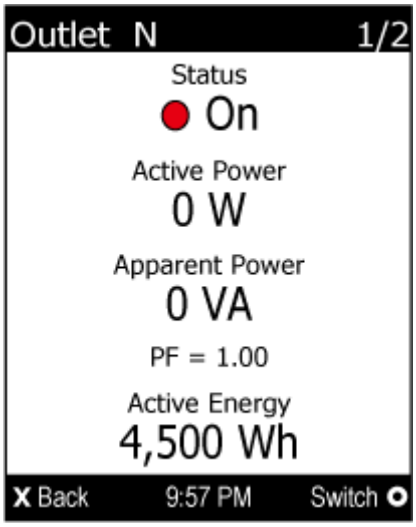


3. Press ▲ or ▼ to select an outlet, and press ●.

If the desired outlet is not visible, press ▲ or ▼ to scroll up or down.

4. The LCD display shows the selected outlet's information. For details, see ***Showing an Outlet's Information*** (on page 84).

Note: In the following diagrams, N represents the selected outlet's number.



5. 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, and 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'.

6. 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.
7. A confirmation message appears. Press ▲ or ▼ to select Yes or No, and then press ●.
   - Yes: Confirm the operation.
   - No: Abort the operation.
8. 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. See step 4.
   - 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.
9. To return to the Main Menu, press ✕ several times until the Main Menu is shown.

Peripherals

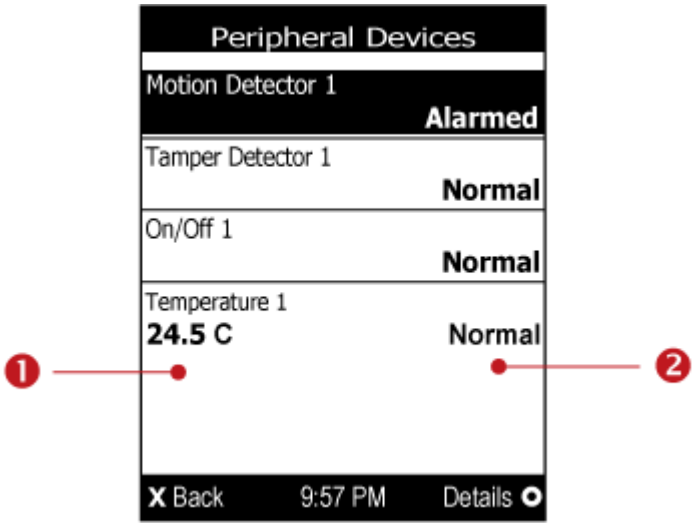
If there are no Raritan environmental sensor packages connected to your PX, the LCD display shows the message "No managed devices" for the "Peripherals" menu command.

If any connected sensor is highlighted in red or yellow, that sensor has entered an alarmed, warning or critical state. See ***The Yellow- or Red-Highlighted Sensors*** (on page 119) for color meanings.

If you have enabled the front panel actuator control function, you can switch on or off a connected actuator using the LCD display. See ***Enabling the Front Panel Actuator Control*** (on page 313).

To show environmental sensor or actuator information:

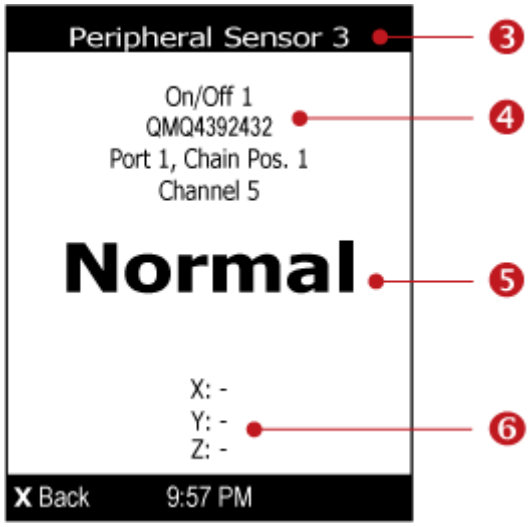
1. Press ▲ or ▼ to select "Peripherals" in the Main Menu, and press ●.
2. The display shows a list of environmental sensors similar to the following diagram.
   - If the desired sensor or actuator is not visible, press ▲ or ▼ to scroll up or down. Page numbers are indicated in the top-right corner of the LCD display.



Number	Description
1	Sensor or actuator names. For a numeric sensor, its reading is displayed right below the sensor name. For a discrete sensor, no reading is displayed.

Number	Description
❷	Sensor or actuator states as listed below. For further information, see ***States of Managed Sensors*** (on page 308) and ***States of Managed Actuators*** (on page 311). ▪ 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

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



Number	Description
❸	The ID number assigned to this sensor or actuator. ▪ A sensor is shows as "Peripheral Sensor x," where x is the ID number. ▪ An actuator is shown as "Peripheral Actuator x," where x is the ID number.

Number	Description
❹	Three pieces of sensor or actuator information are listed from top to down. ▪ Sensor or actuator name ▪ 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. Chain Pos. <n>: <n> is the sensor or actuator's position in a sensor daisy chain. *Note: Only DX and DPX2 sensor packages provide the chain position information.* ▪ If this sensor or actuator is on a sensor package with multiple channels, such as DX-D2C6, its channel number is indicated as "Channel x", where x is a number.
❺	Depending on the sensor type, any of the following information is displayed: ▪ State of a discrete (on/off) sensor: Normal or Alarmed. ▪ State of an actuator: On or Off. ▪ Reading of a numeric sensor.
❻	X, Y, and Z coordinates which you specify for this sensor or actuator. See ***Configuring Environmental Sensors or Actuators*** (on page 302).

To switch on or off an actuator:

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

Assets

If there are no Raritan asset management sensors connected, the LCD display shows the message "Asset strip not connected" for the "Assets" menu command.

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

To show asset sensor information:

1. Press ▲ or ▼ to select "Assets" in the Main Menu, and press ⊙.

2. The LCD display shows a list of rack unit numbers as well as their information similar to the following diagram.

Number	Description
1	Three pieces of information are displayed from left to right. ▪ A color box: This represents the asset sensor's LED color when an asset tag is detected. The default is green. You can customize the color. See ***Setting Asset Sensor LED Colors*** (on page 315). ▪ Rack unit number: The numerical order can be either ascending or descending, depending on the numbering mode you set. See ***Configuring the Asset Sensor*** (on page 314). ▪ The connected asset tag's ID number (barcode)
2	The asset tag's name if you have specified one. This field does not show up if no name is available.

3. If the desired rack unit is not visible, press ▲ or ▼ to scroll up or down. Page numbers are indicated in the top-right corner of the LCD display.

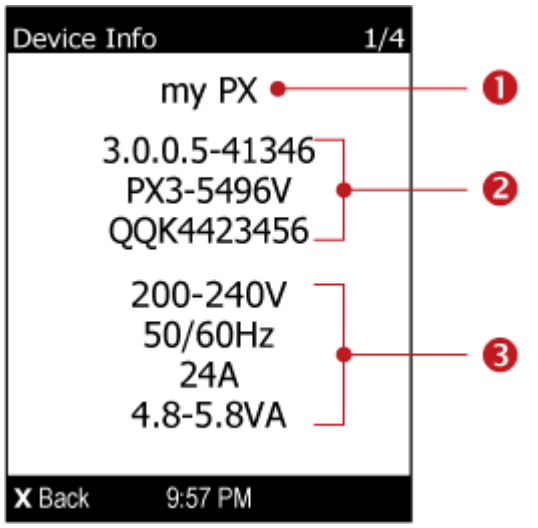
Device Info

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

To show the device information:

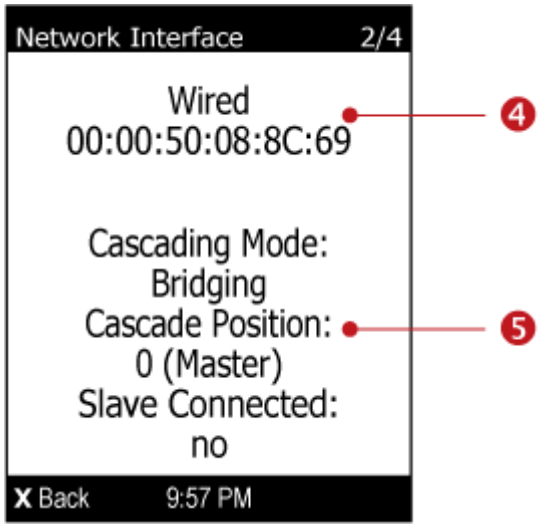
1. Press ▲ or ▼ to select "Device Info" in the Main Menu, and press ●.

2. The display shows device information similar to the following diagram.



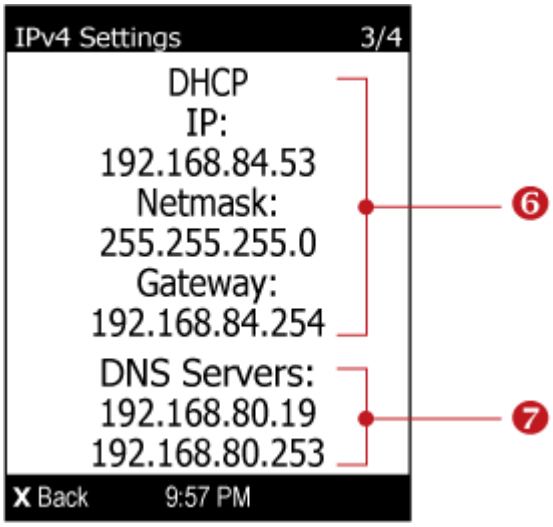
Number	Description
❶	The PX device's name.
❷	Firmware version, model name and serial number.
❸	Device ratings, including rated voltage, frequency, current and power.

3. To go to the next page which shows the networking mode and USB-cascading status, press ▼.



Number	Description
❹	Networking information, including: ▪ Network mode: Wired or Wireless. ▪ MAC address of the PX. ▪ If the networking mode is wireless, the following additional information is available: - SSID - MAC address of the access point being used
❺	USB-cascading status, including: ▪ Cascading mode: Bridging or Port Forwarding. See ***Setting the Cascading Mode*** (on page 154). ▪ Cascade position: The position information is available only when the PX is in a USB-cascading configuration. The information comprises a number and a noun enclosed in parentheses: - The number represents the device's position. For example, 0 represents the master device, 1 represents Slave 1, 2 represents Slave 2, and so on. - The noun in parentheses indicates whether it is a master or slave device. ▪ Slave connected: Indicates whether the presence of a slave device is detected on the USB-A port - *yes* or *no*.

4. To go to the next page which shows IPv4 settings, press ▼.



Number	Description
❻	IPv4 network information, including: ▪ Network configuration: DHCP or Static. Static represents Static IP. ▪ IP address. ▪ Netmask. ▪ Gateway.
❼	DNS server addresses, including the primary and secondary ones.

If you do not enable IPv4 settings, a message is displayed to indicate IPv4 is disabled.

5. To show IPv6 settings, press ▼. If IPv6 settings have been enabled, the following IPv6 information is available:
   - Network configuration: Automatic or Static.
   - IP address(es).
   - DNS server address(es).

   If you do not enable IPv6 settings, the following message is displayed instead.

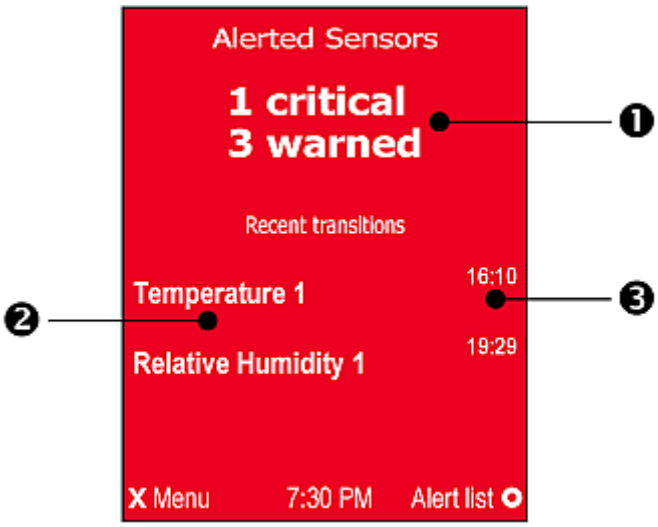
6. To return to the Main Menu, press ⊗.

Alerts Notice in a Yellow or Red Screen

In the automatic mode, if an alerts 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 is yellow. When any alerted sensor enters the critical level, the screen's background turns red. For additional information on colors, see ***The Yellow- or Red-Highlighted Sensors*** (on page 119).

The following illustrates the alerts notice in the red screen.



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

Next steps:

- To view details of all alerted sensors, press .
- To enter the manual mode, press .

Showing the Firmware Upgrade Progress

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

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

Reset Button

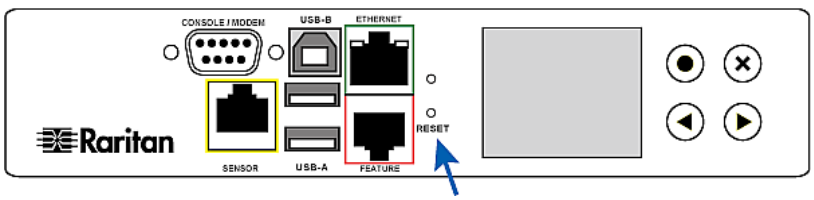
The reset button is located inside the small hole near the display panel on the PDU.

The PX device can be reset to its factory default values using this button when a serial connection is available. See ***Resetting to Factory Defaults*** (on page 580).

Without the serial connection, pressing this reset button restarts the PX device's software without any loss of power to outlets.

The following images illustrate the locations of the reset button on Zero U models only.

- **PX3 phase II models:**



Circuit Breakers

PX 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:

- A PX3 **phase I** model's LCD display shows CbE, which means "circuit breaker error." See ***Overcurrent Protector Information*** (on page 606).
- A PX3 **phase II** model's 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 75).

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.

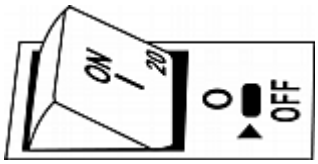
Depending on the model you purchased, the circuit breaker may use a button- or handle-reset mechanism.

Resetting the Button-Type Circuit Breaker

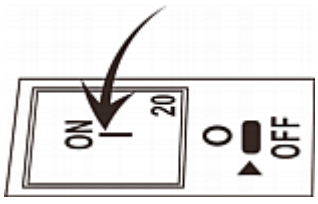
Your button-type circuit breakers may look slightly different from the images shown in this section, but the reset procedure remains the same.

To reset the button-type breakers:

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



2. Examine your PX and the connected equipment to remove or resolve the cause that results in the overload or short circuit. **This step is required, or you cannot proceed with the next step.**
3. Press the ON button until it is completely down.

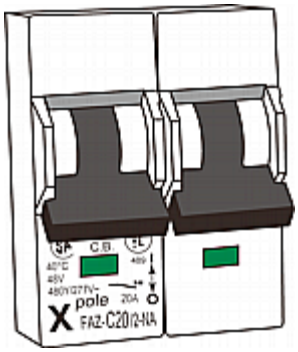


Resetting the Handle-Type Circuit Breaker

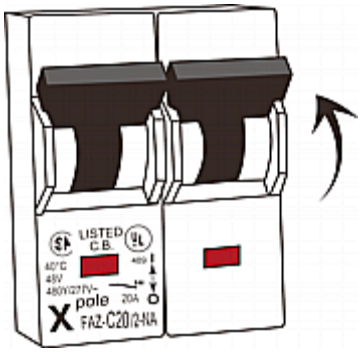
Your handle-type circuit breakers may look slightly different from the images shown in this section, but the reset procedure remains the same.

To reset the handle-type breakers:

1. Lift the hinged cover over the breaker.
2. Check if the colorful rectangle or triangle below the operating handle is GREEN, indicating that the breaker has tripped.



3. Examine your PX 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.



Fuse

Some PX devices may be implemented with fuses instead of circuit breakers. A fuse blows to protect associated outlets if it detects the overload.

If your PDU uses fuses, you must replace it with a new one when it blows or malfunctions. The rating of the new fuse must be the same as the original one.

Use of inappropriately rated fuse results in damage to the PDU and connected equipment, electric shock, fire, personal injury or death.

Depending on the design of your PDU, the fuse replacement methods differ.

Fuse Replacement on Zero U Models

This section only applies to a Zero U PDU with "replaceable" fuses.

To replace a fuse on the Zero U model:

1. Lift the hinged cover over the fuse.

2. Verify the new fuse's rating against the rating specified in the fuse holder's cover.

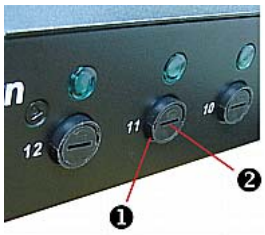
3. Push the cover of the fuse holder to expose the fuse.

4. Take the fuse out of the holder.

5. Insert a new fuse into the holder. There is no orientation limit for fuse insertion.
6. Close the fuse holder and the hinged cover in a reverse order.

Fuse Replacement on 1U Models

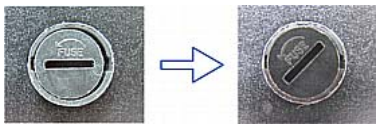
On the 1U model, a fuse is installed in a fuse knob, which fits into the PDU's fuse carrier.



Number	Description
❶	Fuse carrier
❷	Fuse knob where a fuse is installed

To replace a fuse on the 1U PDUs:

1. Disconnect the PDU's power cord from the power source.
2. Remove the desired fuse from the PDU's fuse carrier using a flat screwdriver.
   a. Rotate the fuse knob counterclockwise until its slot is inclined to 45 degrees.



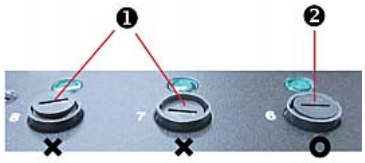
   b. Take this knob out of the fuse carrier.
3. Remove the original fuse from this knob, and insert either end of a new one into the knob. Make sure the new fuse's rating is the same as the original one.

Number	Description
1	Fuse knob
2	Fuse

4. Install this knob along with the new fuse into the fuse carrier using a flat screwdriver.
   a. Have this knob's slot inclined 45 degrees when inserting the knob into the fuse carrier.

   b. Gently push this knob into the fuse carrier and then rotate it clockwise until its slot is horizontal.

5. Verify whether this knob's head is aligned with the fuse carrier. If its head is higher or lower than the fuse carrier, re-install it.



Number	Description
❶	INAPPROPRIATE installations
❷	Appropriate installation

6. Connect the PDU's power cord to the power source and verify that the corresponding fuse LED is lit, indicating that the fuse works properly.

Beeper

The PX includes an internal beeper to issue an audible alarm for an overcurrent protector which is open.

- The beeper sounds an alarm within 3 seconds of a circuit breaker trip.
- The beeper stops as soon as all circuit breakers have been reset.

Tip: You can remotely check this beeper's state via the web interface. See **Checking the Internal Beeper State** *(on page 167).*

Replaceable Controller

A PX3 phase II *Zero U* model provides flexibility for replacement of its controller. The controller, which contains the dot-matrix LCD display and connection ports, is usually located in the middle of the PDU.

If the controller is broken, you can simply send the controller back to Raritan for repair, or purchase a new controller from Raritan.

1U and 2U models do NOT support this feature.

Note: PX3 phase I models do NOT support a replaceable controller.

To request a new PX3 controller:

Contact tech@raritan.com to request a new PX3 controller.

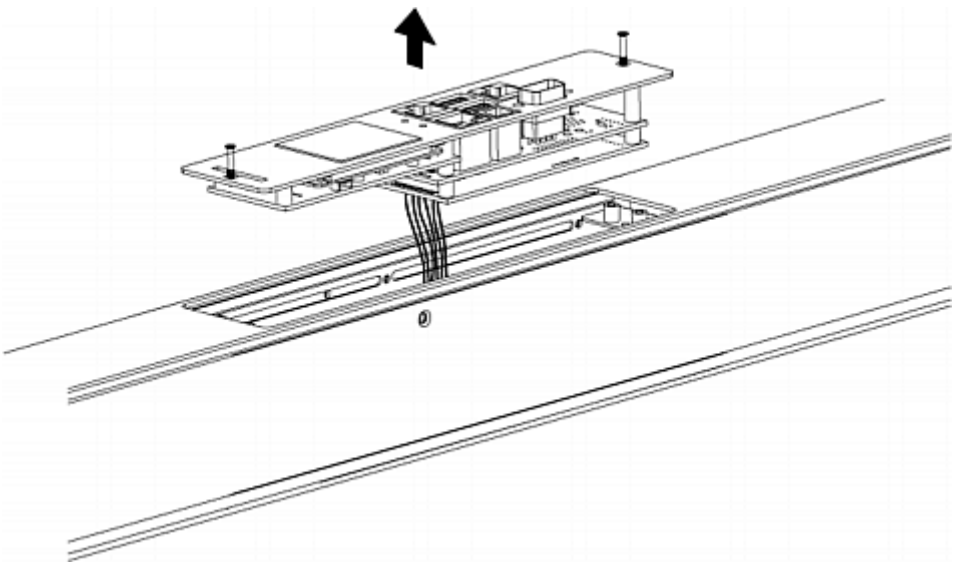
Include these details with your request:

- The serial number of the PDU
- The serial number of the controller board
- The full model number of the PDU
- The firmware version that the PDU is running (if known).

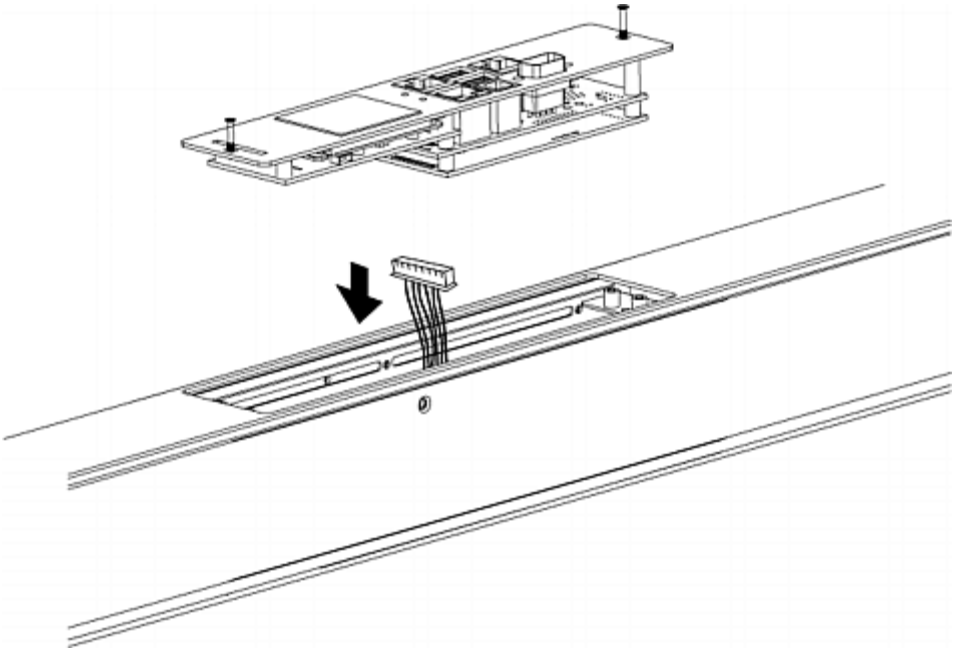
To replace a PX3 controller:

1. PDU is NOT required to be powered off.
2. Loosen the screws at two sides of the PX3 controller, and lift it up.

Note: Loosen the screws instead of removing them.



3. Disconnect the PDU's controller cable from the controller.



4. Get a new PX3 controller and install it back into the PDU in the reverse order.

Chapter 6 Using the Web Interface

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

In This Chapter

Supported Web Browsers....107
Logging in to the Web Interface....108
Logout....111
Introduction to the Web Interface....112
Viewing the Dashboard....122
Device Management....124
User Management....168
Setting Up Roles....174
Access Security Control....177
Setting Up a TLS Certificate....192
Setting Up External Authentication....198
Outlet Management....206
Inlet and Overcurrent Protector Management....224
Setting Power Thresholds....229
Event Rules and Actions....236
Managing Event Logging....287
Viewing Connected Users....290
Monitoring Server Accessibility....291
Environmental Sensors and Actuators....295
Asset Management....314
Bulk Configuration....319
Backup and Restore of PX Device Settings....322
Webcam Management....323
Network Diagnostics....332
Downloading Diagnostic Information....333
Managing the Schroff LHX/SHX Heat Exchanger....334
Firmware Upgrade....341
Accessing the Help....345

Supported Web Browsers

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

Logging in to the Web Interface

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

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

After successfully logging in, you can create user profiles for your other users. These profiles define their login names and passwords. See ***Creating a User Profile*** (on page 168).

Login

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

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

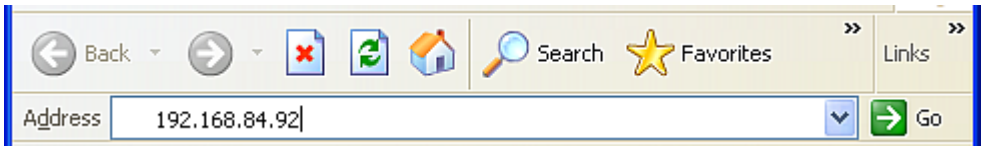
To log in to the web interface:

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

   http(s)://<ip address>

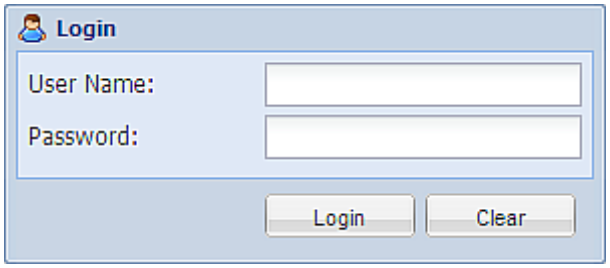
   where *<ip address>* is the IP address of the PX.

   Tip: If the link-local addressing has been enabled, you can type pdu.local *instead of an IP address. See* **APIPA and Link-Local Addressing** *(on page 2).*



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

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



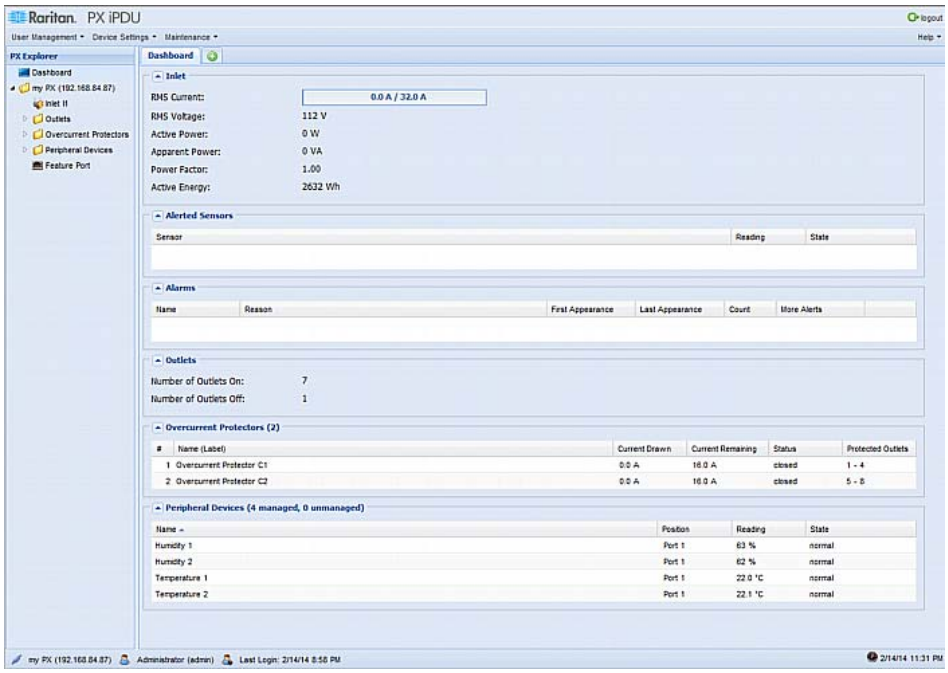
Note: If needed, click Clear to clear either the inputs or any error message that appears.

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

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

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

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

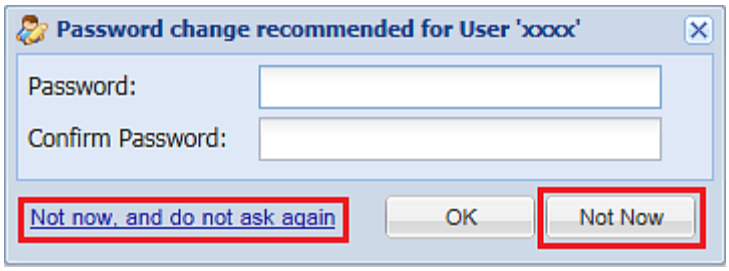


Note: The IP address to access a slave device in the USB-cascading configuration where the port forwarding mode is applied is a combination of the IP address and the port number. See **Port Forwarding Examples** *(on page 159).*

Password change request for first login:

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

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



Users without permissions listed must change password.

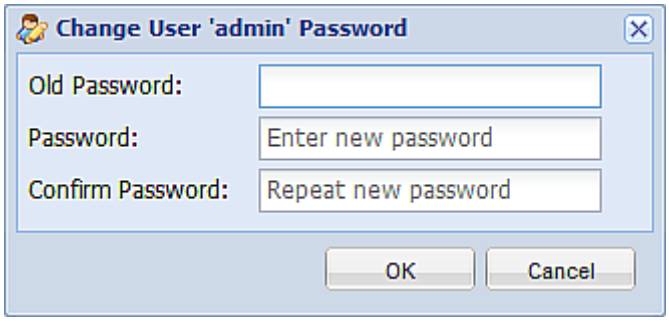
Changing Your Password

You must have the Change Own Password permission to change your own password. See ***Setting Up Roles*** (on page 174).

You must have Administrator Privileges to change other users' passwords. See ***Modifying a User Profile*** (on page 172).

To change your password:

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



Remembering User Names and Passwords

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

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

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

The PX does NOT support other browser password managers.

Logout

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

To log out of the web interface:

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

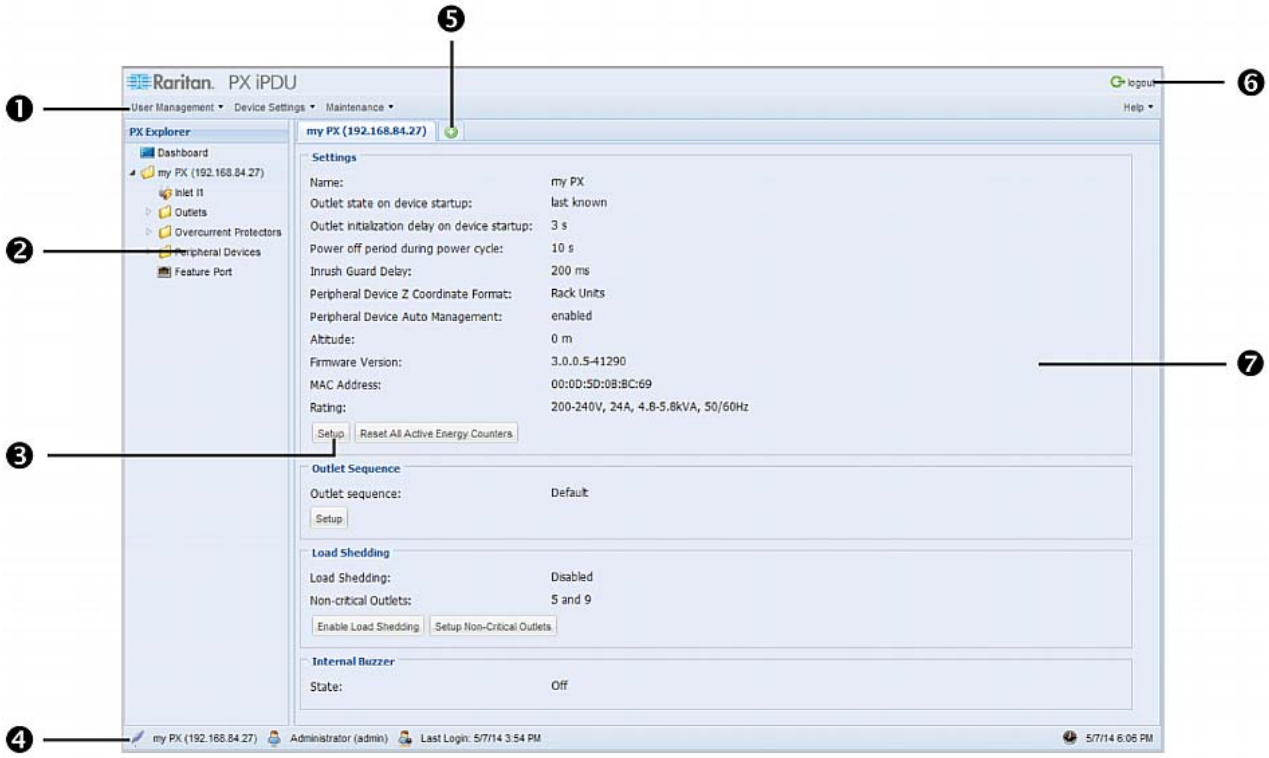
logout

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

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

Introduction to the Web Interface

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



Number	Web interface element
1	Menus
2	PX Explorer pane

Number	Web interface element
❸	Setup button*
❹	Status bar
❺	Add Page icon
❻	Logout button
❼	Data pane

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

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

Menus

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

PX Explorer Pane

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

The tree structure comprises three hierarchical levels.

First level	Second level	Third level
Dashboard	None	None
PDU folder*	Inlet I1	None
	Outlets folder	1 to n**
	Overcurrent Protectors folder	• Circuit breakers - C1 to Cn** • Fuses - F1 to Fn**

First level	Second level	Third level
	Peripheral Devices folder	A list of connected environmental sensors
	Feature Port folder	One of the following is displayed, depending on your configuration: • None • Asset Strip • Power CIM • External Beeper • LHX-20 • SHX-30 • LHX-40
	Webcam Management folder	• Snapshots • Webcam

* The folder is named "my PX" by default. The name can be customized. See ***Naming the PDU*** (on page 130).

** n represents the final number of that component.

Note: A Webcam icon appears only when a supported Logitech® webcam is connected to the PX. See **Connecting a Logitech Webcam** *(on page 63).*

To navigate through the tree:

1. To expand any folders, see ***Expanding the Tree*** (on page 114).
2. To show any tree item's data, click on that item. See ***Add Page Icon*** (on page 117).

Expanding the Tree

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

To expand the tree:

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

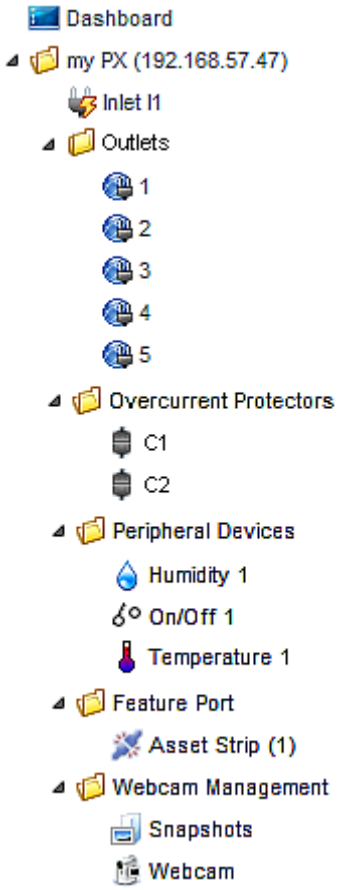
Note: This folder is named "my PX" by default. The name can be customized.

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

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

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

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



Collapsing the Tree

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

To collapse the whole tree:

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

  Note: This folder is named "my PX" by default. The name can be customized.

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

To hide some tree items:

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

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

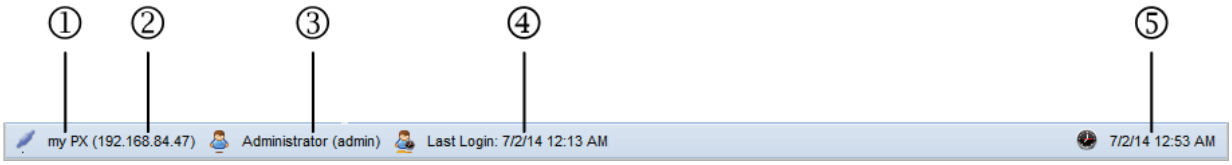
2. Repeat Step 1 for other component groups you want to collapse.

Setup Button

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

Status Bar

The status bar shows five pieces of information.



1. **Device name:**

   This is the name assigned to the PX device. The default is "my PX." See ***Naming the PDU*** (on page 130).

2. **IP address:**

   The numbers enclosed in parentheses is the IP address assigned to the PX device. See ***Initial Network Configuration via CLI*** (on page 23) or ***Modifying Network Settings*** (on page 134).

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

3. **Login name:**

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

4. **Last login time:**

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

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

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

   There are different types of access clients:

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

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

5. **System date and time:**

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

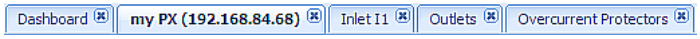
Add Page Icon

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

To open new data pages:

1. Click the Add Page icon . A new tab along with a blank data page appears.
2. Click a tree item whose data page you want to open. The data of the selected tree item is then displayed on the blank page.
3. To open more data pages, repeat the above steps. All tabs representing opened pages are shown across the top of the page.

The following diagram shows a multi-tab example.



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

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

Data Pane

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

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

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

To adjust the pane's width:

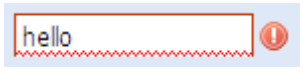
1. Move the mouse pointer to the left border of the right pane.
2. When the mouse pointer turns into a two-way arrow, drag the border horizontally to widen or shrink the pane.

More Information

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

Warning Icon

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



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

The Yellow- or Red-Highlighted Sensors

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

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

If any circuit breaker trips or any fuse blows, the circuit breaker or fuse's row is also highlighted in red.

See the table for the meaning of each color:

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

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

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

For information on threshold settings, see:

- ***Setting Power Thresholds*** (on page 229)
- ***Configuring Environmental Sensors or Actuators*** (on page 302)
- ***Configuring Temperature and Fan Thresholds*** (on page 336)

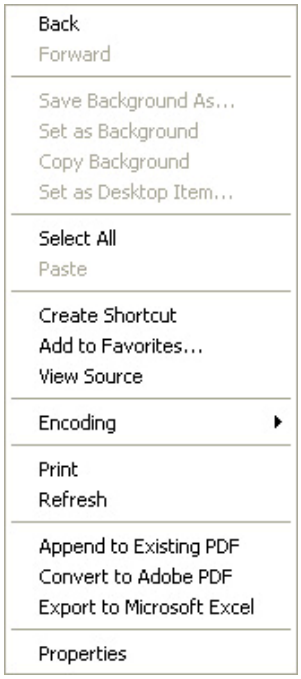
Browser-Defined Shortcut Menu

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

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

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

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



Viewing the Dashboard

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

The page is divided into various sections according to the component type, such as inlet(s), outlets, circuit breakers and alerted sensors.

Note: If a sensor row is colored, it means the sensor reading already crosses one of the thresholds, the sensor enters an alarmed state, or the overcurrent protector has tripped or blown. See **The Yellow- or Red-Highlighted Sensors** *(on page 119).*

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

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

To collapse any section:

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

To expand a collapsed section:

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

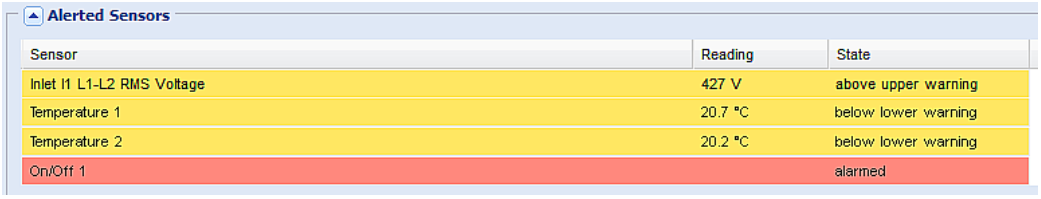
Alerted Sensors

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

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

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

- Any tripped circuit breakers or blown fuses



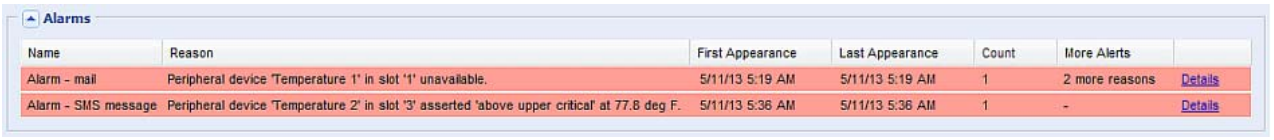
For the background color meanings in this section, see ***The Yellow- or Red-Highlighted Sensors*** (on page 119).

Alarms List

You can create event rules that request users to acknowledge certain alerts, and resend alert notifications if the acknowledgment action is not taken yet. See ***Creating Actions*** (on page 237).

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

Below is the illustration of the alarms list.



The following table explains each column of the alarms list.

Column	Description
Name	The customized name of the Alarm action.
Reason	The first event that triggers the alert.
First Appearance	The date and time when the event indicated in the Reason column occurred for the first time.
Last Appearance	The date and time when the event indicated in the Reason column occurred for the last time.
Count	The number of times the event indicated in the Reason column has occurred.
More Alerts	▪ A dash is displayed when there is only one event triggering this alert. ▪ If there are other types of events triggering the same alert, the total number of these additional reasons is displayed. You can double click that alarm to view a list of all events that have occurred.

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

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

To acknowledge an alarm:

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

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

Device Management

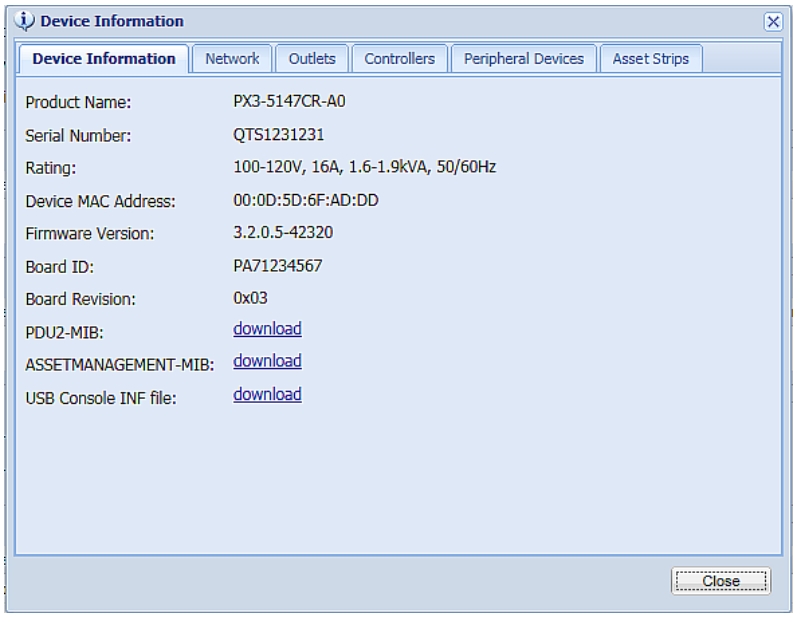
Using the web interface, you can retrieve basic hardware and software information, give the PX a new device name, set the system date and time, and modify network settings that were entered during the initial configuration process.

Displaying PDU Information

To display information specific to the PX device that you are using, such as inlet or outlet types, trigger the Device Information dialog.

To display PDU-specific information:

1. Choose Maintenance > Device Information.



2. Click a tab to view type-specific information. The number of available tabs varies according to the model you purchased.

Tab	Data
Device Information	General PDU information, such as model name, serial number, firmware version, hardware revision, and so on.
Network	The PDU specific network information, such as the current networking mode, IPv4 and/or IPv6 addresses and so on. This tab also indicates whether the PDU is part of an USB-cascading configuration. See ***Identifying Cascaded Devices*** (on page 126).
Outlets	Each outlet's receptacle type, operating voltage and rated current.
Controllers	Each outlet controller's serial number, board ID, firmware version and hardware version.

Tab	Data
Inlets	Each inlet's plug type, rated voltage and current.
Overcurrent Protectors	Each overcurrent protector's type, rated current and the outlets that it protects.
Peripheral Devices	Serial numbers, model names and firmware-related information of connected external devices, such as environmental sensor packages.
Asset Strips	Each asset sensor's ID, boot version, application version and protocol version.

3. Enlarge the dialog if necessary.
4. Click Close to quit the dialog.

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

Identifying Cascaded Devices

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

For information on how to cascade devices using USB cables, see ***Cascading the PX via USB*** (on page 29).

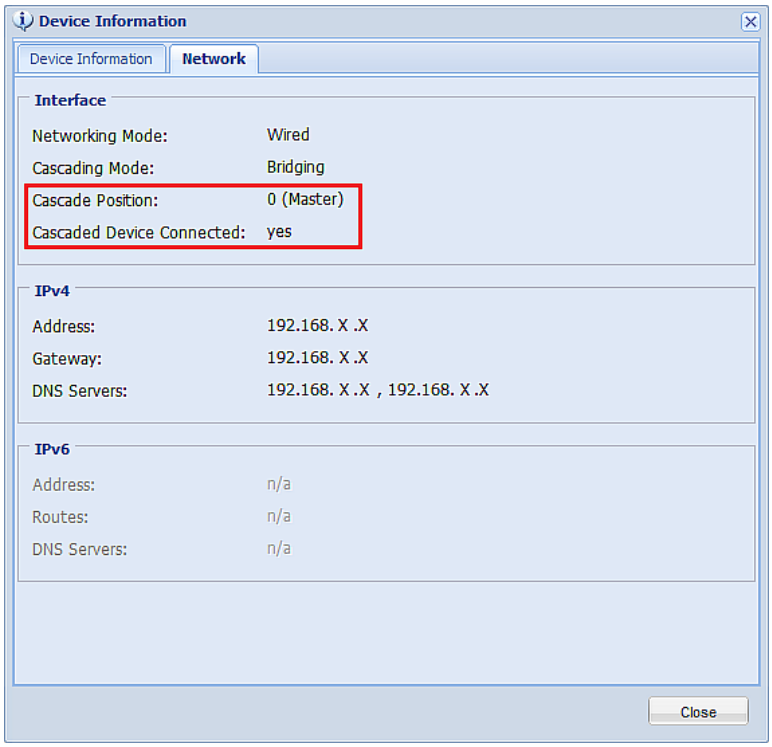
Note: For more information on the USB-cascading configuration, see the USB-Cascading Solution Guide*, which is available from Raritan website's* **Support page** *(***http://www.raritan.com/support/***).*

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

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

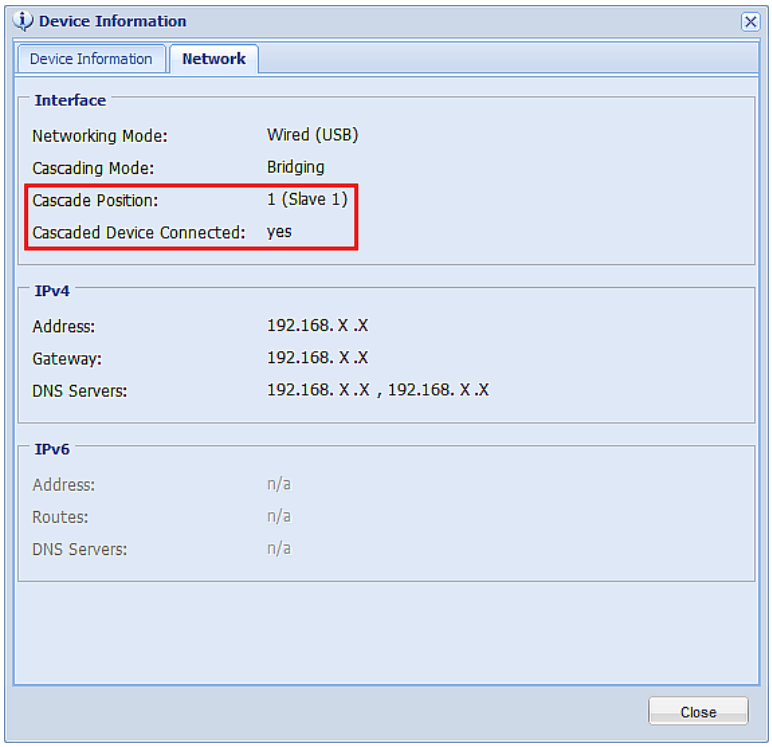
Fields	Description
Networking Mode	Indicates how the PX is connected to the LAN. ▪ Wired: The device is connected to the LAN through a standard network cable. ▪ Wireless: The device is connected to the LAN through a supported USB wireless LAN adapter. See ***USB Wireless LAN Adapters*** (on page 22). ▪ XXX (USB): XXX represents Wired or Wireless. The device is connected to the LAN through a USB-cascading configuration. That is, it is a slave device.
Cascading Mode	Shows the cascading mode applied. See ***Setting the Cascading Mode*** (on page 154).
Cascade Position	Indicates the position of the PX in the USB-cascading configuration. ▪ 0 (zero) represents the master device. ▪ A non-zero number represents a slave device. 1 is Slave 1, 2 is Slave 2, 3 is Slave 3 and so on. This field is NOT available on a standalone PX.
Cascaded Device Connected	Indicates whether the presence of a slave device is detected on the USB-A port. ▪ yes: Connection to a slave device is detected. ▪ no: NO connection to a slave device is detected.

- A master device shows *0* (zero) in the Cascade Position field and *yes* in the Cascaded Device Connected field.



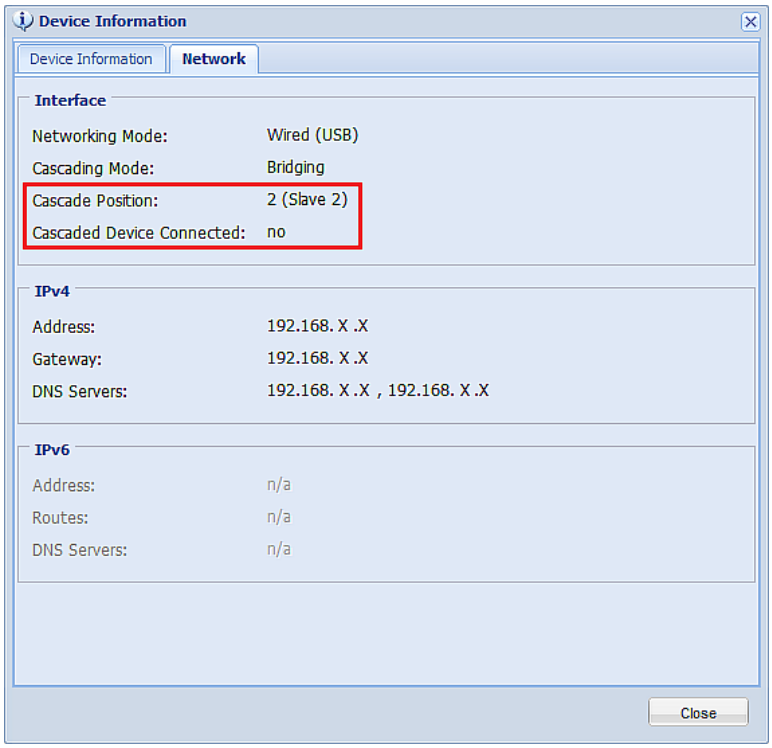
- A slave device in the middle position shows a non-zero number which indicates its exact position in the Cascade Position field and *yes* in the Cascaded Device Connected field.

The following diagram shows 1, indicating it is the first slave - Slave 1.



- The final slave device shows a non-zero number which indicates its position in the Cascade Position field and *no* in the Cascaded Device Connected field.

The following diagram shows 2, indicating it is the second slave - Slave 2. The Cascaded Device Connected field shows *no*, indicating that it is the final one in the chain.



Naming the PDU

The default name for PX root folder is *my PX*. You may give it a unique device name.

To change the device name:

1. Click the PDU folder in the PX Explorer pane to open the PDU page.
2. Click Setup in the Settings section. The Pdu Setup dialog appears.
3. Type a new name in the Device Name field.
4. Click OK.

Modifying the Network Configuration

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

Modifying Network Interface Settings

The PX supports two types of network interfaces: wired and wireless. You should configure the network interface settings according to the networking mode that applies. See ***Connecting the PX to Your Network*** (on page 21).

Wired Network Settings

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

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

To modify the network interface settings:

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

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

Wireless Network Settings

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

Note for USB-cascading configuration: Port forwarding mode over wireless LAN is supported as of release 3.1.0. You must upgrade all devices in the chain to version 3.1.0 or higher if wireless networking is preferred. See **Cascading the PX via USB** *(on page 29).*

To modify the wireless interface settings:

1. Choose Device Settings > Network. The Network Configuration dialog appears.
2. The Interface Settings tab should have been selected. If not, click the Interface Settings tab.
3. In the Network Interface field, click the drop-down arrow, and select Wireless from the list.
4. Check the Hardware State field to ensure that the PX device has detected a wireless USB LAN adapter. If not, verify whether the USB LAN adapter is firmly connected or whether it is supported. See ***Connecting the PX to Your Network*** (on page 21).
5. Type the name of the wireless access point (AP) in the SSID field.
6. If the BSSID is available, select the Force AP BSSID checkbox, and type the MAC address in the BSSID field.

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

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

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

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

8. When the PEAP authentication requires a CA certificate, do the following:
   a. Select the "Enable Verification of TLS Certificate Chain" checkbox for the PX to verify the validity of the TLS certificate that will be installed. For example, the PX will check the certificate's validity period against the system time.
   b. Click Browse to select a TLS certificate file. Then you can:
      - Click Show to view the certificate's contents.
      - Click Remove to delete the installed certificate if it is inappropriate.
   c. Select the "Allow expired and not yet valid certificates" checkbox if intending to make the wireless network connection successful even though the installed TLS certificate chain contains any certificate that is outdated or not valid yet.
   d. Select the "Allow wireless connection if system clock is incorrect" checkbox to make the wireless network connection successful when the PX system time is earlier than the firmware build before synchronizing with any NTP server. If the system time is incorrect, the installed TLS certificate is considered not valid yet and will cause the wireless network connection to fail while this checkbox is not selected.

      The incorrect system time issue may occur when the PX has once been powered off for a long time.
9. Click OK.

Modifying Network Settings

The PX was configured for network connectivity during the installation and configuration process. See ***Configuring the PX*** (on page 17). If necessary, you can modify any network settings later.

Selecting the Internet Protocol

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

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

To select the appropriate Internet Protocol:

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

Modifying IPv4 Settings

You must enable the IPv4 protocol before you can modify the IPv4 network settings. See ***Selecting the Internet Protocol*** (on page 134).

To modify IPv4 settings:

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

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

Option	Description
	mask using the format "IP address/subnet mask." ▪ Next Hop: IP address of the next hop router. See ***Static Route Examples*** (on page 138) for illustrations.

4. Click OK.

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

Modifying IPv6 Settings

You must enable the IPv6 protocol before you can modify the IPv6 network settings. See ***Selecting the Internet Protocol*** (on page 134).

To modify IPv6 settings:

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

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

Option	Description
	▪ IP address ▪ Default gateway ▪ Primary DNS server ▪ Secondary DNS server (optional) ▪ DNS Suffix (optional) If your local network contains two subnets and IP forwarding has been enabled, you can click Append to add static routes so that your PX can communicate with the other subnet. Each static route requires: ▪ Destination: IP address of the current subnet and prefix length using the format "IP address/prefix." ▪ Next Hop: IP address of the next hop router. See ***Static Route Examples*** (on page 138) for illustrations.

4. Click OK.

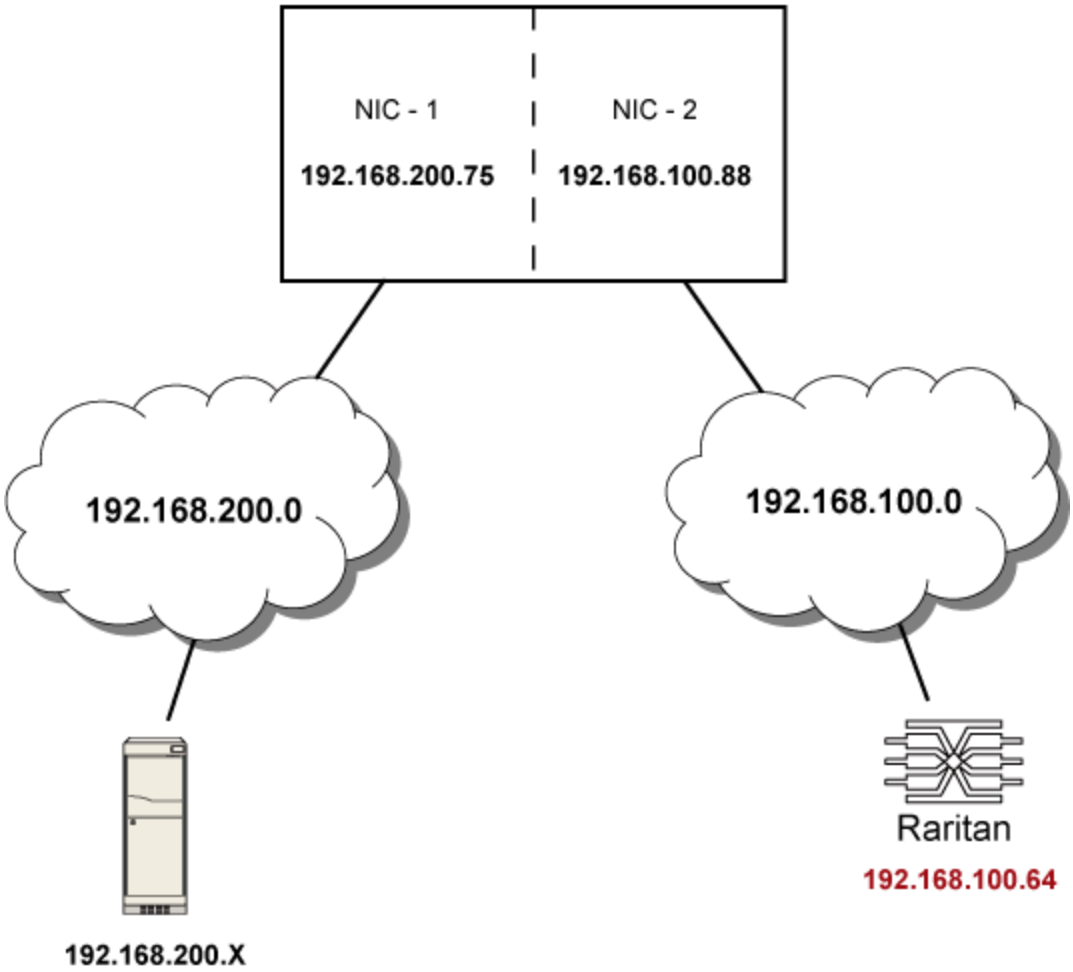
Note: The PX supports a maximum of 3 DNS servers. If two IPv4 DNS servers and two IPv6 DNS servers are available, the PX only uses the primary IPv4 and IPv6 DNS servers.

Static Route Examples

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

IPv4 example:

- Your PX: *192.168.100.64*
- Two NICs: *192.168.200.75* and *192.168.100.88*
- Two networks: *192.168.200.0* and *192.168.100.0*
- Subnet mask: *24*

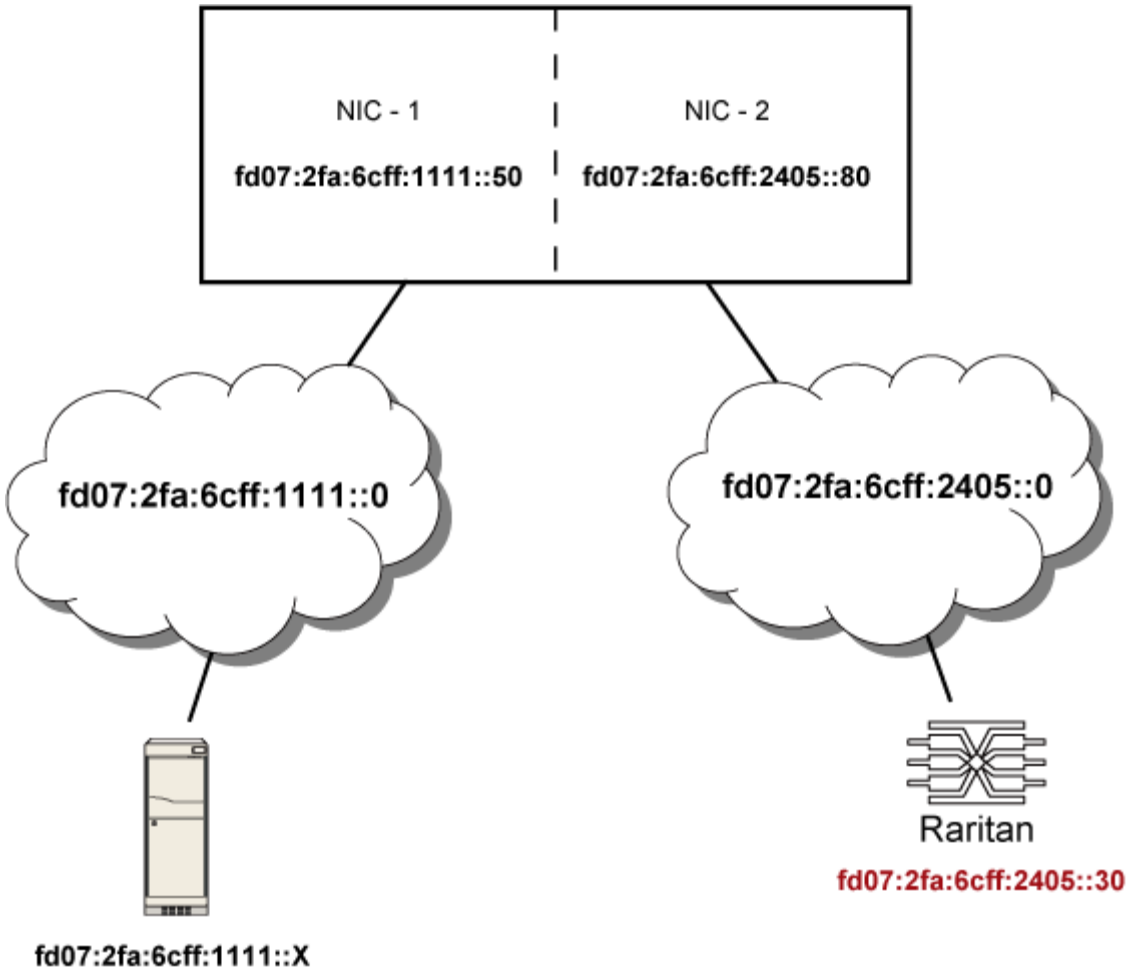


In this example, NIC-2 (192.168.100.88) is the next hop router for your PX to communicate with any device in the other subnet 192.168.200.0. In the IPv4 "Append new Route" dialog, you should specify:

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

IPv6 example:

- Your PX: *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 PX to communicate with any device in the other subnet fd07:2fa:6cff:1111::0. In the IPv6 "Append new Route" dialog, you should specify:

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

Role of a DNS Server

As Internet communications are carried out on the basis of IP addresses, appropriate DNS server settings are required for mapping domain names (host names) to corresponding IP addresses, or the PX may fail to connect to the given host.

Therefore, DNS server settings are important for external authentication. With appropriate DNS settings, the PX 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 198).

Modifying Network Service Settings

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

HTTPS and HTTP enable the access to the web interface, and Telnet and SSH enable the access to the command line interface. See ***Using the Command Line Interface*** (on page 359).

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

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

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

Changing HTTP(S) Settings

Important: Raritan disables SSL 3.0 and uses TLS for releases 3.0.4, 3.0.20 and later releases due to published security vulnerabilities in SSL 3.0. Make sure your network infrastructure, such as LDAP and mail services, uses TLS rather than SSL 3.0.

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

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

To change HTTP or HTTPS port settings:

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

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

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

To enable or disable HTTPS redirection:

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

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

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

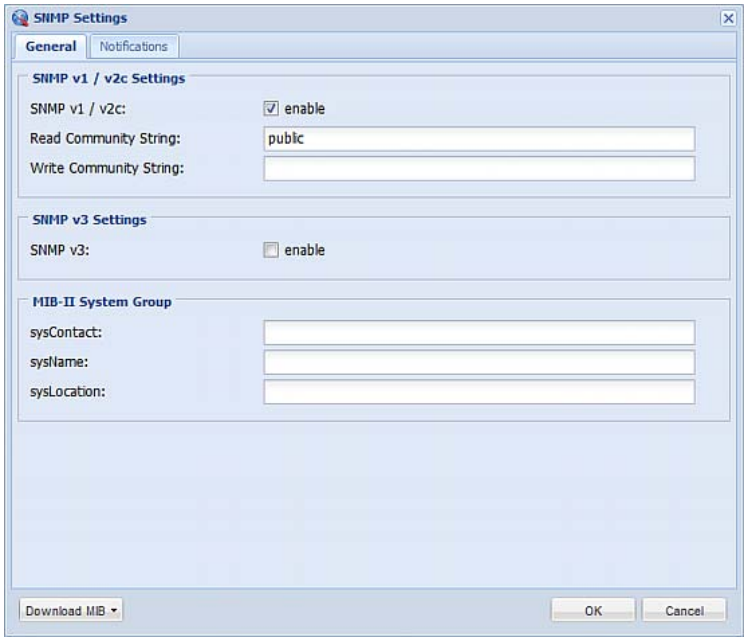
Configuring SNMP Settings

You can enable or disable SNMP communication between an SNMP manager and the PX device. Enabling SNMP communication allows the manager to retrieve and 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 236).

To configure SNMP communication:

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



2. Enable or disable "SNMP v1 / v2c" and/or "SNMP v3" by clicking the corresponding "enable" checkbox. For details, see ***Enabling SNMP*** (on page 348).
   - The SNMP v1/v2c read-only access is enabled by default.
3. Enter the MIB-II system group information, if applicable.

   Important: You must download the SNMP MIB for your PX to use with your SNMP manager. Click Download MIB in this dialog to download the desired MIB file. For details, see **Downloading SNMP MIB** *(on page 356).*

4. Click OK.

To configure SNMP notification destinations:

1. Click the Notifications tab in the same SNMP dialog.
2. Select the Enabled checkbox.
3. Select an SNMP notification type - SNMP v2c Trap, SNMP v2c Inform, SNMP v3 Trap, and SNMP v3 Inform.
4. Specify the SNMP notification destinations and enter necessary information. For details, refer to either of the following:
   - ***SNMPv2c Notifications*** (on page 351)
   - ***SNMPv3 Notifications*** (on page 353)
5. Click OK.

Tip: The SNMP notification destinations can be also set in the Event Rule Settings dialog. See **Modifying an Action** *(on page 286).*

Changing SSH Settings

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

To change SSH service settings:

1. Choose Device Settings > Network Services > SSH. The SSH Settings dialog appears.
2. To use a different port, type a new port number in the port field. Valid range is 1 to 65535.
3. To enable the SSH application, select the Enable SSH Access checkbox. To disable it, deselect the checkbox.
4. To select a different authentication method, select one of the checkboxes.
   - Password authentication only: Enables the password-based login only.
   - Public key authentication only: Enables the public key-based login only.
   - Password and public key authentication: Enables both the password- and public key-based login. This is the default.
5. Click OK.

If the public key authentication is selected, you must type a valid SSH public key for each user profile to log in over the SSH connection. See ***Creating a User Profile*** (on page 168).

Changing Telnet Settings

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

To change Telnet service settings:

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

Changing Modbus/TCP Settings

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

To change the Modbus service settings:

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

Enabling Service Advertisement

The PX advertises all enabled services that are reachable using the IP network. This feature uses DNS-SD (Domain Name System-Service Discovery) and mDNS (multicastDNS). The advertised services are discovered by clients that have implemented DNS-SD and mDNS.

The advertised services include the following:

- HTTP
- HTTPS
- Telnet
- SSH
- Modbus
- json-rpc
- SNMP

By default, this feature is enabled.

Enabling this feature also enables Link-local Multicast Name Resolution (LLMNR) and mDNS, which are required for resolving APIPA host names. See ***APIPA and Link-Local Addressing*** (on page 2).

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 PX. 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 **Modifying Network Settings** *(on page 134).*

To enable service advertisement:

1. Choose Device Settings > Network Services to select the Service Advertisement checkbox.
2. Click Yes on the confirmation message to switch to zero configuration advertising. The feature is enabled and the Service Advertisement checkbox is selected in the submenu.

To disable service advertisement:

1. Choose Device Settings > Network Services to deselect the Service Advertisement checkbox.

2. Click Yes on the confirmation message to switch off the zero configuration advertising. The feature is disabled and the Service Advertisement checkbox is deselected in the submenu.

Setting the Date and Time

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

To set the date and time:

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

   If the daylight saving time rules are not available for the selected time zone, the checkbox is not configurable.
4. Choose one of the methods to set the date and time:
   - To customize the date and time, select the User Specified Time radio button, and then enter the date and time in appropriate fields. Use the yyyy-mm-dd format for the date and the hh:mm:ss format for the time.
     - The time is measured in 24-hour format so enter 13 for 1:00pm, 14 for 2:00pm, and so on.
   - To let an NTP server set the date and time, select the "Synchronize with NTP Server" radio button. There are two ways to assign the NTP servers.
     - To use the DHCP-assigned NTP servers, make sure the "Always use the servers below and ignore DHCP-provided servers" checkbox is deselected. This method is usable only when either IPv4 or IPv6 DHCP is enabled.
     - To use the NTP servers that are manually specified, select the "Always use the servers below and ignore DHCP-provided servers" checkbox, and specify the primary NTP server in the First Time Server field. A secondary NTP server is optional.
       Click Check NTP Servers to verify the validity and accessibility of the specified NTP servers.

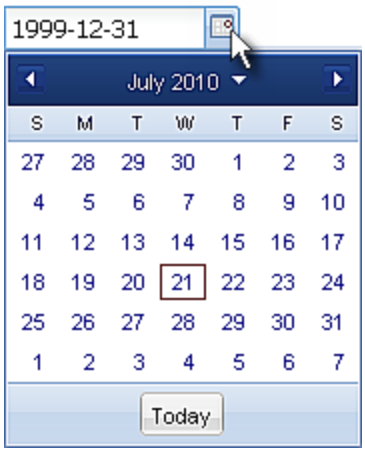
   Note: If the PX device's IP address is assigned through IPv4 or IPv6 DHCP, the NTP servers can be automatically discovered. When this occurs, the data you entered in the fields of First and Second Time Server will be overridden.
5. Click OK.

The PX follows the NTP server sanity check per the IETF RFC. If your PX has problems synchronizing with a Windows NTP server, see ***Windows NTP Server Synchronization Solution*** (on page 149).

Note: If you are using Sunbird's Power IQ to manage the PX, you must configure Power IQ and the PX to have the same date/time or NTP settings.

How to Use the Calendar

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



To select a date using the calendar:

1. To change the year shown in the calendar, do either of the following:
   - Press Ctrl+Up arrow or Ctrl+Down arrow to switch between years.

- Click , which is adjacent to the year, to show a list of years and months. Select the desired year from the list to the right and click OK. If the list does not show the desired year, click or to show additional years.

2. To change the month shown in the calendar, do one of the following:
   - Press Ctrl+Right arrow or Ctrl+Left arrow to switch between months.
   - Click or on the top of the calendar to switch between months.
   - Click , which is adjacent to the year, to show a list of years and months. Select the desired month from the list to the left and click OK.
3. To select a date, click that date on the calendar.
   - Click Today if you want to select today.

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

Windows NTP Server Synchronization Solution

The NTP client on the PX follows the NTP RFC so the PX 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 PX.

Note: For information on NTP RFC, visit **http://tools.ietf.org/html/rfc4330 http://tools.ietf.org/html/rfc4330** *to refer to the section 5.*

Windows NTP servers may have a root dispersion of more than one second, and therefore cannot synchronize with the PX. When the NTP synchronization issue occurs, change the dispersion settings to resolve it.

To change the Windows NTP's root dispersion settings:

1. Access the registry settings associated with the root dispersion on the Windows NTP server.

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config

2. *AnnounceFlags* must be set to 0x05 or 0x06.

   - 0x05 = 0x01 (Always time server) and 0x04 (Always reliable time server)
   - 0x06 = 0x02 (Automatic time server) and 0x04 (Always reliable time server)

   Note: Do NOT use 0x08 (Automatic reliable time server) because its dispersion starts at a high value and then gradually decreases to one second or lower.

   ---

3. *LocalClockDispersion* must be set to 0.

Setting the LCD Display's Default View

This setting is only available on PX3 phase II models except for PX3-3000 series, which does NOT provide inlet sensor information.

After powering on or resetting a PX, the dot-matrix LCD display enters the automatic mode by default, which cycles through the inlet information and, if available, overcurrent protector information. See ***Automatic and Manual Modes*** (on page 73).

If you want your PX which contains overcurrent protectors to cycle through the inlet information only in the default view, change its front panel default view settings.

To set the default view of the LCD display:

1. Choose Device Settings > Front Panel Settings. The Front Panel Default View dialog appears.
2. Select the default view you prefer.
   - Automatic mode: The LCD display cycles through both the inlet and overcurrent protector information. This is the default.
   - Inlet overview: The LCD display cycles through the inlet information only.
3. Click OK.

Setting Default Measurement Units

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

Note: To set preferred measurement units for your own, see **Setting Up Your Preferred Measurement Units** *(on page 173). If your preferences are different from the default measurement units, your preferences rather than the defaults apply to the PX user interfaces after you log in.*

To set up default user preferences:

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

- In the Pressure Unit field, select "Pascal" or "psi" as the measurement unit for pressure.

3. Click OK.

Configuring the Feature Port

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

- Raritan Computer Interface Module (CIM) for KVM access. See ***Dominion KX II / III Configuration*** (on page 680).
- Raritan serial access products, including Dominion KSX II, SX or SX II. See ***Dominion KSX II, SX or SX II Configuration*** (on page 685).
- Raritan asset management sensors (asset sensors). See ***Connecting Asset Management Sensors*** (on page 54).
- External beeper. See ***Connecting an External Beeper*** (on page 65).
- Schroff® LHX-20, SHX-30 or LHX-40 heat exchanger. See ***Connecting a Schroff LHX/SHX Heat Exchanger*** (on page 65).

By default, the FEATURE port can automatically detect and display the device connected to the FEATURE port. The only exception is the Schroff® LHX/SHX device, which requires enabling the LHX/SHX support before the PX can detect or display it. See ***Managing the Schroff LHX/SHX Heat Exchanger*** (on page 334).

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

To configure the FEATURE port:

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

Device type	Description
Asset Strip	Raritan asset sensors.
External Beeper	An external beeper with the RJ-45 socket.
LHX 20	Schroff® LHX-20 heat exchanger. All Schroff® SHX/LHX device types are available only after the LHX/SHX support is enabled. See ***Enabling and Disabling Schroff LHX/SHX Heat Exchanger Support*** (on page 335).
SHX 30	Schroff® SHX-30 heat exchanger.
LHX 40	Schroff® LHX-40 heat exchanger.
Power CIM	Select this type when connecting one of the following Raritan products: ▪ Raritan power CIM, D2CIM-PWR. This CIM is used to connect the PX to the Raritan digital KVM switch -- Dominion KX II. ▪ Dominion KSX II ▪ Dominion SX or SX II

4. Click OK.

Configuring the Serial Port

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

The PX supports the use of one of the following devices via the serial interface:

- A computer or Raritan KVM product for console management.
- An analog modem for remote dial-in and access to the CLI.
- A GSM modem for sending out SMS messages to a cellular phone.

Bit-rate adjustment may be necessary. Change the bit-rate before connecting the supported device to the PX through the serial port, or there are communication problems.

Note: The serial port bit-rate change is needed when the PX works in conjunction with Raritan's Dominion LX KVM switch. The Dominion LX only supports 19200 bps for communications over the serial interface.

You can set diverse bit-rate settings for console and modem operations. Usually the PX can detect the device type, and automatically apply the preset bit-rate.

To change the serial port baud rate settings:

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

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

3. In the Console Baud Rate field, select the baud rate intended for console management.

   Note: For a serial RS-232 or USB connection between a computer and the PX, leave it at the default (115200 bps).

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

To configure the analog modem settings:

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

To configure the GSM modem settings:

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

Setting the Cascading Mode

A maximum of eight PX devices can be cascaded using USB cables and therefore share only one Ethernet connection. See ***Cascading the PX via USB*** (on page 29).

The Ethernet sharing mode applied to the USB-cascading configuration is either network bridging or port forwarding. This mode is determined by the master device. See ***Overview of the Cascading Modes*** (on page 156).

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

To apply the "Port Forwarding" cascading mode, all cascaded PX devices must be upgraded to version 2.5.20 or later, or those devices not supporting the "Port Forwarding" mode cannot be accessed over the network. See ***Updating the PX Firmware*** (on page 342).

Note: The PX in the Port Forwarding mode does not support APIPA. See **APIPA and Link-Local Addressing** *(on page 2).*

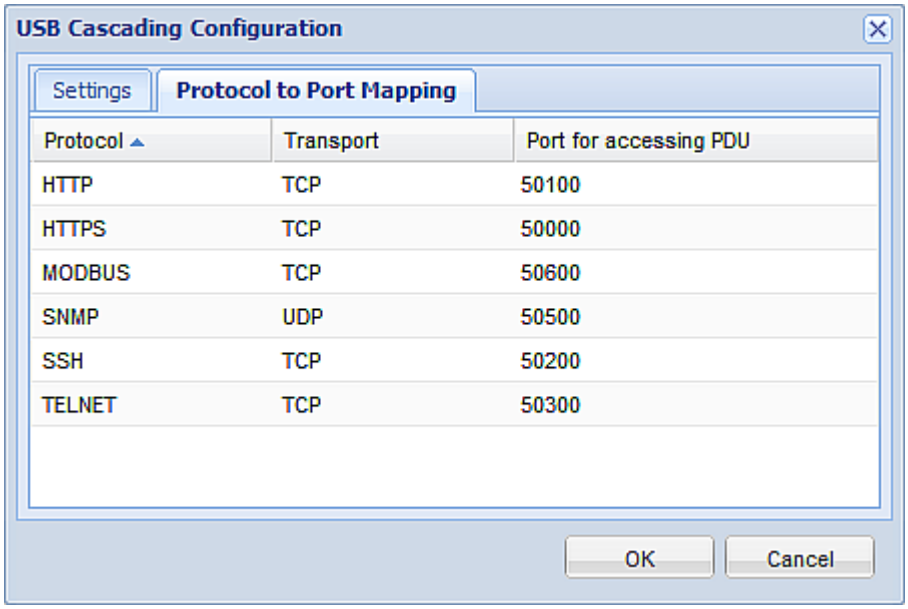
To configure the cascading mode:

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

3. Verify that the "Position in cascaded chain" field shows 0 (Master), indicating that this PX is the master device.
4. Select the preferred cascading mode in the "Cascading mode" field.
   - Bridging: Each device in the USB-cascading configuration is accessed with a different IP address. This is the default.
   - Port Forwarding: Each device in the USB-cascading configuration is accessed with the same IP address but with a different port number assigned. For details the port numbers, see ***Port Number Syntax*** (on page 157).

   Note: If reversing or disconnecting the USB cable from a slave device, causing the slave device to become a master or standalone device, you must plug an Ethernet cable to it to update its USB-cascading status.
5. Click OK.
6. If selecting Port Forwarding, a list of port numbers for diverse networking protocols will be available on the "Protocol to Port Mapping" tab of each cascaded device.

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



For information on accessing each cascaded device in the Port Forwarding mode, see ***Port Forwarding Examples*** (on page 159).

Overview of the Cascading Modes

You must apply a cascading mode to the USB-cascading configuration. See ***Setting the Cascading Mode*** (on page 154).

Overview:

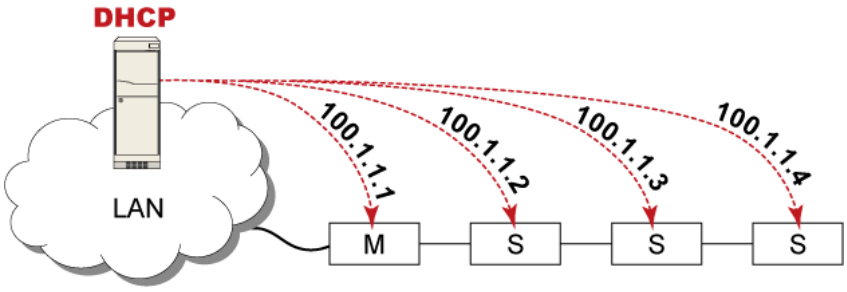
- The Bridging mode supports the wired network only while the Port Forwarding mode supports both wired and wireless networks.
- All cascading modes support both DHCP and static IP addressing.
- In the Bridging mode, each cascaded device has a unique IP address. In the Port Forwarding mode, all cascaded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

Illustration:

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

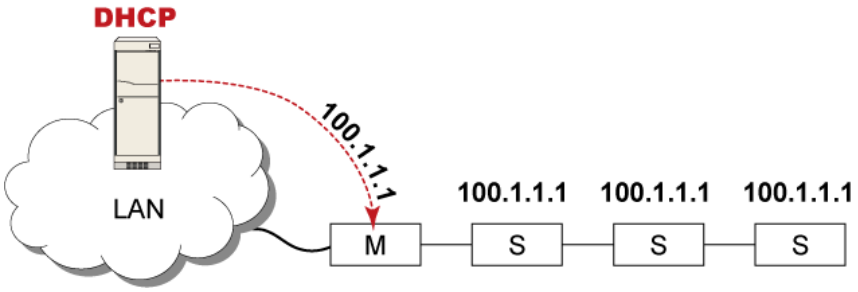
- **"Bridging" mode:**

  As illustrated in the following diagram, the DHCP server communicates with every cascaded device respectively and assigns four different IP addresses accordingly. Each device has one IP address. The way to remotely access each cascaded device is completely the same as accessing a standalone device in the network.



- **"Port Forwarding" mode:**

  The DHCP server communicates with the master device only and assigns one IP address. All slave devices use the same IP address as the master device. You must specify a 5XXXX port number (where X is a number) when remotely accessing any slave device through the network. See ***Port Number Syntax*** (on page 157).



Port Number Syntax

In the Port Forwarding mode, all devices in the USB-cascading configuration share the same IP address. To access any cascaded device, you must assign an appropriate port number to it.

- Master device: The port number is either *5NNXX* or the standard TCP/UDP port.
- Slave device: The port number is *5NNXX*.

5NNXX port number syntax:

- NN is a two-digit number representing the network protocol as shown below:

Protocols	NN
HTTPS	00
HTTP	01
SSH	02
TELNET	03
SNMP	05
MODBUS	06

- XX is a two-digit number representing the device position as shown below:

Position	XX
Master device	00
Slave 1	01

Position	XX
Slave 2	02
Slave 3	03
Slave 4	04
Slave 5	05
Slave 6	06
Slave 7	07

For example, to access the Slave 4 device via Modbus/TCP, the port number is 50604. See ***Port Forwarding Examples*** (on page 159) for further illustrations.

Tip: The full list of each cascaded device's port numbers can be retrieved from the web interface. See **Setting the Cascading Mode** *(on page 154).*

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 PX does NOT allow you to modify the standard TCP/UDP port configuration, including HTTP, HTTPS, SSH, Telnet, SNMP and Modbus/TCP.

Port Forwarding Examples

To access a cascaded device in the Port Forwarding mode, assign a port number to the IP address.

- Master device: Assign proper 5NNXX port numbers or standard TCP/UDP ports. See ***Port Number Syntax*** (on page 157) for details.
- Slave device: Assign proper 5NNXX port numbers.

Assumption: *The Port Forwarding mode is applied to a USB-cascading configuration comprising three Raritan products. The IP address is 192.168.84.77.*

Master device:

Position code for the master device is 00 so each port number is 5NN00 as shown below.

Protocols	Port numbers
HTTPS	50000
HTTP	50100
SSH	50200
TELNET	50300
SNMP	50500
MODBUS	50600

Examples using "5NN00" ports:

- To access the master device via HTTPS, the IP address is:
  https://192.168.84.77:50000/
- To access the master device via HTTP, the IP address is:
  http://192.168.84.77:50100/
- To access the master device via SSH, the command is:
  ssh -p 50200 192.168.84.77

Examples using standard TCP/UDP ports:

- To access the master device via HTTPS, the IP address is:
  https://192.168.84.77:443/
- To access the master device via HTTP, the IP address is:
  http://192.168.84.77:80/
- To access the master device via SSH, the command is:
  ssh -p 22 192.168.84.77

Slave 1 device:

Position code for Slave 1 is 01 so each port number is 5NN01 as shown below.

Protocols	Port numbers
HTTPS	50001
HTTP	50101
SSH	50201
TELNET	50301
SNMP	50501
MODBUS	50601

Examples:

- To access Slave 1 via HTTPS, the IP address is:
  https://192.168.84.77:50001/
- To access Slave 1 via HTTP, the IP address is:
  http://192.168.84.77:50101/
- To access Slave 1 via SSH, the command is:
  ssh -p 50201 192.168.84.77

Slave 2 device:

Position code for Slave 2 is 02 so each port number is 5NN02 as shown below.

Protocols	Port numbers
HTTPS	50002
HTTP	50102
SSH	50202
TELNET	50302
SNMP	50502
MODBUS	50602

Examples:

- To access Slave 2 via HTTPS, the IP address is:
  https://192.168.84.77:50002/
- To access Slave 2 via HTTP, the IP address is:
  http://192.168.84.77:50102/

- To access Slave 2 via SSH, the command is:

  ssh -p 50202 192.168.84.77

Setting Data Logging

The PX 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 PX 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 PX device's SNMP agent must be enabled for this feature to work. See **Enabling SNMP** *(on page 348). In addition, using an NTP time server ensures accurately time-stamped measurements.*

Enabling Data Logging

By default, data logging is enabled. You must have "Administrator" or "Change Pdu, Inlet, Outlet & Overcurrent Protector Configuration" permissions to change the setting.

To configure the data logging feature:

1. Choose Device Settings > Data Logging. The Data Logging Options dialog appears.
2. To enable the data logging feature, select the "enable" checkbox in the Enable Data Logging field.
3. Type a number in the Measurements Per Log Entry field. Valid range is from 1 to 600. The default is 60.
4. Verify that all sensor logging is enabled. If not, click Enable All to have all sensors selected.
5. Click OK.

Important: Although it is possible to selectively enable/disable logging for individual sensors on the PX in Step 4, it is NOT recommended.

Configuring SMTP Settings

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

If any email messages fail to be sent successfully, the failure event and reason are available in the event log. See ***Viewing the Local Event Log*** (on page 288).

Note: See **Event Rules and Actions** *(on page 236) for information on creating event rules to send email notifications.*

To set SMTP server settings:

1. Choose Device Settings > SMTP Server. The SMTP Server Settings dialog appears.
2. Type the name or IP address of the mail server in the Server Name field.
3. Type the port number for the SMTP server in the Port field. The default is 25.
4. Type an email address for the sender in the Sender Email Address field.
5. Type the number of email retries in the "Number of Sending Retries" field. The default is 2 retries.
6. Type the time interval between email retries in the "Time Interval Between Sending Retries (in minutes)" field. The time is measured in minutes. The default is 2 minutes.
7. If your SMTP server requires password authentication, do this:
   a. Select the Server Requires Authentication checkbox.
   b. Type a user name in the User Name field.
   c. Type a password in the Password field.
8. If your SMTP server supports the Transport Layer Security (TLS), select the "Enable SMTP over TLS (StartTLS)" checkbox. Then do the following:
   a. Click Browse to select the TLS CA certificate file. Then you may:
      - Click Show to view the installed certificate's contents.
      - Click Remove to delete the installed certificate if it is inappropriate.
   b. Select or deselect the "Allow expired and not yet valid certificates" checkbox.

- To always send the email messages even though the installed certificate chain contains a certificate that is outdated or not valid yet, select this checkbox.
- To prevent the email messages from being sent when any certificate in the installed certificate chain is outdated or not valid yet, deselect this checkbox.

9. Now that you have set the SMTP settings, you can test it to ensure it works properly. Do the following:
   a. Type the recipient's email address in the Recipient Email Addresses field. Use a comma to separate multiple email addresses.
   b. Click Send Test Email.
   c. Check if the recipient(s) receives the email successfully.
10. Click OK.

Configuring Data Push Settings

If any Raritan asset sensors have been connected to PX, you can push the asset sensor data to a remote server for data synchronization. The data will be sent in JSON format using HTTP POST requests. You need to set up the destination and authentication for data push on the PX.

For instructions on connecting asset sensors, see ***Connecting Asset Management Sensors*** (on page 54).

After configuring the destination and authentication settings, do either or both of the following:

- To perform the data push after the occurrence of a certain event, create the data push action and assign it to an event rule. See ***Push Out Sensor Readings*** (on page 243).
- To push the data at a regular interval, schedule the data push action. See ***Scheduling an Action*** (on page 262).

To configure data push settings:

1. Choose Device Settings > Data Push. The Data Push dialog appears.
2. Click New. The Add New Destination dialog appears.
3. In the URL field, determine the following information.
   - Click the arrow to select http or https.
   - Type the URL or host name in the accompanying text box.
4. If the destination server requires authentication, select the "Use authentication" checkbox, and provide the authentication information:
   - In the "User name" field, type the login name.
   - In the Password field, type the login password.

5. In the "Entry type" field, determine the data that will be transmitted.
   - Asset management information: Transmit the information of the specified asset sensor(s), including the general status of the specified sensor(s) and a list of asset tags on blade extension strips if any.
   - Asset management log: Transmit the log of all asset sensors, which is generated when there are changes made to asset tags and asset sensors, including asset tag connection or disconnection events.
6. If "Asset management information" is selected in the above step, specify the asset sensor(s) whose log to send. The PX has only one FEATURE port so only one asset sensor is available.
   - To specify the asset sensor, select it in the Available list box and click (Add) or (Add All).
   - To remove the asset sensor, select it in the Selected list box and click (Remove) or (Remove All).
7. Click OK.

Specifying the Device Altitude

You must specify the PX device's altitude above sea level if a Raritan's DPX differential air pressure sensor is attached. This is because the device's altitude is associated with the altitude correction factor. See ***Altitude Correction Factors*** (on page 677).

The default altitude measurement unit is meter. You can have the measurement unit vary between meter and foot according to user credentials. See ***Setting Default Measurement Units*** (on page 150).

To specify the altitude of the PX device:

1. Click the PDU folder.

   Note: The folder is named "my PX" by default. The name can be customized. See **Naming the PDU** *(on page 130).*

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

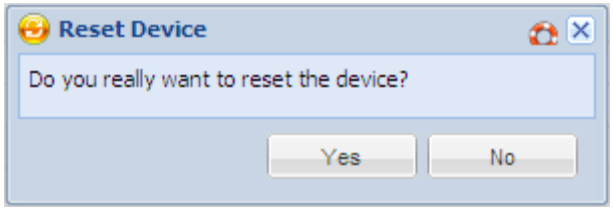
Rebooting the PX Device

You can remotely reboot the PX device via the web interface.

Resetting the PX does not interrupt the operation of connected servers because there is no loss of power to outlets. Outlets that have been powered on prior to the reset remain powered on and outlets that have been powered off remain powered off during and after the reset.

To reboot the device:

1. Choose Maintenance > Unit Reset. The Reset Device dialog appears.



2. Click Yes to reset the PX.
3. A message appears with a countdown timer showing the remaining time of the operation. It takes about one minute to complete.
4. When the reset is complete, the Login page opens. Now you can log back in to the PX device.

Note: If you are not redirected to the Login page after the reset is complete, click the underlined text "this link" in the message.

Resetting All Active Energy Readings

An active energy reading is a value of total accumulated energy, which is never reset, even if the power fails or the PX is reset. 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.

To reset all active energy readings of the PX:

1. Click the PDU folder in the PX Explorer pane to open the PDU page.

   Note: The folder is named "my PX" by default. The name can be customized. See **Naming the PDU** *(on page 130).*

2. Click Reset All Active Energy Counters in the Settings section.
3. Click Yes on the confirmation message. Now all 'Active Energy' readings on the PX are reset to 0 (zero) Wh.

Tip: You can also reset the active energy readings of an individual inlet. See **Resetting Inlet Active Energy Readings** *(on page 227). To reset the active energy readings of specific outlets only, see* **Resetting Outlet Active Energy Readings** *(on page 223).*

Monitoring Total Active Energy or Power

This section applies only to multi-inlet models, including PX in-line monitors.

A PX device with multiple inlets has two additional sensors for reporting power-related readings at the PDU level: total active energy and total active power.

For a regular PX model with multiple inlets:

- Total active energy = sum of all inlets' active energy values
- Total active power = sum of all inlets' active power values

For an in-line monitor with multiple inlets/outlets:

- Total active energy = sum of all outlets' active energy values
- Total active power = sum of all outlets' active power values

Tip: You can reset the active energy sensor(s) as needed. See **Resetting All Active Energy Readings** *(on page 165).*

To view the total active energy and/or power of a multi-inlet PX:

1. Click the PDU folder.

   Note: The folder is named "my PX" by default. The name can be customized. See **Naming the PDU** *(on page 130).*

2. Locate the Power section in the right pane. Both values and states of Active Power and Active Energy are displayed.

Checking the Internal Beeper State

The internal beeper can alert you if any overcurrent protector, including fuses and circuit breakers, has tripped or blown on the PX. See ***Beeper*** (on page 104).

If intended, you can set an event rule to turn on the internal beeper when a specific event occurs. See ***Event Rules and Actions*** (on page 236).

You can remotely check this beeper's state.

To check the internal beeper's state:

1. Click the PDU folder.

   Note: The folder is named "my PX" by default. The name can be customized. See **Naming the PDU** *(on page 130).*

2. Locate the "Internal Beeper" section in the right pane. Either of the following states is displayed.
   - Off: The beeper is turned off.
   - Active: The beeper is turned on. A field titled "Activation reason" appears below the beeper state, indicating why the beeper sounds an alarm.

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

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

Tip: To check the internal beeper state via CLI, see **PDU Configuration** *(on page 368).*

Setting the EnergyWise Configuration

If a Cisco® EnergyWise energy management architecture is implemented in your place, you can enable the Cisco EnergyWise endpoint implemented on the PX device so that this device becomes part of the Cisco EnergyWise domain.

The Cisco EnergyWise feature implemented on the PX is disabled by default.

To set the Cisco EnergyWise configuration:

1. Choose Device Settings > EnergyWise. The EnergyWise Configuration dialog appears.
2. In the Enable EnergyWise field, select the "enable" checkbox to enable the Cisco EnergyWise feature.

3. In the "Domain name" field, type the name of a Cisco EnergyWise domain where the PX belongs. The domain name comprises up to 127 printable ASCII characters.
   - Spaces and asterisks are NOT acceptable.
4. In the "Domain password" field, type the authentication password (secret) for entering the Cisco EnergyWise domain. The password comprises up to 127 printable ASCII characters.
   - Spaces and asterisks are NOT acceptable.
5. In the Port field, type a User Datagram Protocol (UDP) port number for communications in the Cisco EnergyWise domain. The port ranges from 1 to 65535. Default is 43440.
6. In the "Polling interval" field, type a polling interval to determine how often the PX is queried in the Cisco EnergyWise domain. The polling interval ranges from 30 to 600 seconds. Default is 180 seconds.
7. Click OK.

For PX3-3000, PX3-4000, and PX3-5000 series, the parent/child relationship is formed after the Cisco EnergyWise feature is enabled.

- The PDU becomes a parent domain member.
- All outlets become children of the PDU.

User Management

The PX is shipped with one built-in user profile: **admin**, which is used for initial login and configuration. This profile has full permissions, and should be reserved for the system administrator. It cannot be deleted and its permissions are not user-configurable except for the SNMP v3 permission.

All users must have a user profile, which specifies a login name and password, and contains additional (optional) information about the user. Every user profile must have at least a role to determine the user's permissions. See ***Setting Up Roles*** (on page 174).

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

Creating a User Profile

To create a user profile:

1. Choose User Management > Users. The Manage Users dialog appears.
2. Click New. The Create New User dialog appears.

3. Type the information about the user in the corresponding fields. Note that User Name, Password and Confirm Password fields are required.

Field	Type this...
User Name	The name the user enters to log in to the PX. ▪ 4 to 32 characters ▪ Case sensitive ▪ Spaces are NOT permitted.
Full Name	The user's first and last names.
Password, Confirm Password	▪ 4 to 64 characters ▪ Case sensitive ▪ Spaces are permitted.
Telephone Number	The user's telephone number
eMail Address	The user's email address ▪ Up to 64 characters ▪ Case sensitive

4. Select the Enabled checkbox. Enabled users can log in to the PX device.
5. Select the "Force password change on next login" checkbox if you prefer a password change by the user when the user logs in for the first time after this checkbox is enabled.

Note: Users with both the Change Local User Management and Change Security Settings permissions can choose to ignore the password change request. See **Login** *(on page 108).*

6. Click the SNMPv3 tab to set the SNMPv3 access permission. The permission is disabled by default.
   a. To permit the SNMPv3 access by this user, select the "Enable SNMPv3 access" checkbox. Otherwise, leave the checkbox disabled.

Note: The SNMPv3 protocol must be enabled for SNMPv3 access. See **Configuring SNMP Settings** *(on page 142).*

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

Field	Description
Security Level	Click the drop-down arrow to select a preferred security level from the list:

Field	Description
	▪ NoAuthNoPriv: No authentication and no privacy. ▪ AuthNoPriv: Authentication and no privacy. ▪ AuthPriv: Authentication and privacy. This is the default.
Use Password as Authentication Pass Phrase	*This checkbox is configurable only if AuthNoPriv or AuthPriv is selected.* When the checkbox is selected, the authentication pass phrase is identical to the user's password. To specify a different authentication pass phrase, disable the checkbox.
Authentication Pass Phrase	Type the authentication pass phrase in this field if the "Use Password as Authentication Pass Phrase" checkbox is disabled. The pass phrase must consist of 8 to 32 ASCII printable characters.
Confirm Authentication Pass Phrase	Re-type the same authentication pass phrase for confirmation.
Use Authentication Pass Phrase as Privacy Pass Phrase	*This checkbox is configurable only if AuthPriv is selected.* When the checkbox is selected, the privacy pass phrase is identical to the authentication pass phrase. To specify a different privacy pass phrase, disable the checkbox.
Privacy Pass Phrase	Type the privacy pass phrase in this field if the "Use Authentication Pass Phrase as Privacy Pass Phrase" checkbox is disabled. The pass phrase must consist of 8 to 32 ASCII printable characters.
Confirm Privacy Pass Phrase	Re-type the same privacy pass phrase for confirmation.
Authentication Protocol	Click the drop-down arrow and select the desired authentication protocol from the list. Two protocols are available: ▪ MD5 ▪ SHA-1 (default)

Field	Description
Privacy Protocol	Click the drop-down arrow and select the desired privacy protocol from the list. Two protocols are available: ▪ DES (default) ▪ AES-128

7. Click the SSH tab to enter the public key if the public key authentication for the SSH service is enabled. See ***Changing SSH Settings*** (on page 143).
   a. Open the SSH public key with a text editor.
   b. Copy and paste all contents in the text editor into the Public Key field on the SSH tab.
8. Click the Roles tab to determine the permissions of the user.
9. Select one or multiple roles by selecting corresponding checkboxes.
   - The Admin role provides full permissions.
   - The Operator role provides limited permissions for frequently-used functions. See ***Setting Up Roles*** (on page 174) for the scope of permissions. This role is selected by default.
   - If no roles meet your needs, you can:
     - *Modify the permissions of an existing role:* To modify the permissions of any role, double-click the role or highlight it and then click Edit Role. See ***Modifying a Role*** (on page 175).
     - *Create a new role by clicking the Manage Roles button:* See ***Creating a Role*** (on page 174).

   Note: With multiple roles selected, a user has the union of all roles' permissions.
10. To change any measurement units displayed in the web interface and command line interface for this new user, click the Preferences tab, and do any of the following:
    - In the Temperature Unit field, select °C (Celsius) or °F (Fahrenheit) as the measurement unit for temperatures.
    - In the Length Unit field, select "Meter" or "Feet" as the measurement unit for length or height.
    - In the Pressure Unit field, select "Pascal" or "psi" as the measurement unit for pressure.

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

Note: The measurement unit change only applies to the web interface and command line interface. Users can change the measurement units at any time by setting up their own user preferences. See **Setting Up Your Preferred Measurement Units** *(on page 173).*

Modifying a User Profile

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

To modify a user profile:

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

   To change the password, type a new password in the Password and Confirm Password fields. If the password field is left blank, the password is not changed.
5. To change the SNMPv3 access permissions, click the SNMPv3 tab and make necessary changes. For details, see Step 6 of ***Creating a User Profile*** (on page 168).
6. To change the permissions, click the Roles tab and do one of these:
   - Select or deselect any role's checkbox.
   - To modify the permissions of any role, double-click the role or highlight it and then click Edit Role. See ***Modifying a Role*** (on page 175).
7. To change the measurement unit for temperature, length or pressure, click the Preferences tab, and select a different option from the drop-down list.

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

Deleting a User Profile

Delete outdated or redundant user profiles when necessary.

To delete user profiles:

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

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

Setting Up Your Preferred Measurement Units

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

Tip: Preferences can also be changed by administrators for specific users from the Preferences tab of the Manage Users dialog. See **Creating a User Profile** *(on page 168).*

Note: The measurement unit change only applies to the web interface and command line interface. Setting your preferences does not change the default measurement units, which apply to all users before any individual user or the administrator sets preferred measurement units on a per-user basis. See **Setting Default Measurement Units** *(on page 150) for information on changing default measurement units.*

To change the measurement units applied to your PX user interfaces:

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

Setting Up Roles

A role defines the operations and functions a user is permitted to perform or access. Every user must be assigned at least a role.

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

- The Admin role provides full permissions. You can neither modify nor delete this role.
- The Operator role provides limited permissions for frequently-used functions. You can modify or delete this role. By default, the Operator role contains these permissions:

  - Acknowledge Alarms
  - View Event Settings
  - View Local Event Log
  - Change Pdu, Inlet, Outlet & Overcurrent Protector Configuration
  - Change Own Password
  - Switch Outlet (all outlets)

  Note: PX3-3000 and PX3-4000 series are NOT outlet-switching capable so the "Switch Outlet" permission is not available.

  The Operator role is assigned to a newly created user profile by default. See ***Creating a User Profile*** (on page 168).

Creating a Role

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

To create a role:

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

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

2. Click New. The Create New Role dialog appears.
3. Type the role's name in the Role Name field.
4. Type a description for the role in the Description field.
5. Click the Privileges tab to assign one or multiple permissions.
   a. Click Add. The "Add Privileges to new Role" dialog appears.
   b. Select the permission you want from the Privileges list.

c. If the permission you selected contains any argument setting, the Arguments list is shown to the right, such as the Switch Actuator permission. Then select one or multiple arguments.

   For example, if the Switch Outlet permission is selected, the Arguments list shows all outlets for you to determine which outlets this role can control. Select the desired outlets' checkboxes or select the checkbox labeled "all" if you want to select all outlets.

d. Click Add to add the selected permission (and arguments if any).

e. Repeat Steps *a* to *d* until you add all necessary permissions.

6. Click OK.

Now you can assign the new role to any users. See ***Creating a User Profile*** (on page 168) or ***Modifying a User Profile*** (on page 172).

Modifying a Role

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

To modify a role:

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

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

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

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

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

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

6. To delete any permissions, do this:

   a. Select the permission you want to remove by clicking it. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.

   b. Click Delete.

7. To add any permissions, do this:

   a. Click Add. The "Add Privileges to Role XXX" dialog appears, where XXX is the role name.

b. Select the permission you want from the Privileges list.

c. If the permission you selected contains any argument setting, the Arguments list is shown to the right, such as the Switch Actuator permission. Then select one or multiple arguments.

For example, if the Switch Outlet permission is selected, the Arguments list shows all outlets for you to determine which outlets this role can control. Select the desired outlets' checkboxes or select the checkbox labeled "all" if you want to select all outlets.

d. Click Add to add the selected permission (and arguments if any).

e. Repeat Steps *a* to *d* until you add all necessary permissions.

8. To change a specific permission's arguments, do this:

a. Select the permission by clicking it.

b. Click Edit. The "Edit arguments of privilege XXX" dialog appears, where XXX is the privilege name.

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

c. Select the argument you want. You can make multiple selections.

d. Click OK.

9. Click OK.

Deleting a Role

You can delete any role other than the Admin role.

To delete a role:

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

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

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

Access Security Control

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

Tip: You can also create and install the certificate or set up external authentication servers to control any access. See **Setting Up a TLS Certificate** *(on page 192) and* **Setting Up External Authentication** *(on page 198).*

Forcing HTTPS Encryption

You can force all accesses to the PX via HTTP to be redirected to HTTPS. See ***Changing HTTP(S) Settings*** (on page 140).

Configuring the Firewall

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

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

By default the firewall is disabled.

To configure the firewall:

1. Enable the firewall. See ***Enabling the Firewall*** (on page 177).
2. Set the default policy. See ***Changing the Default Policy*** (on page 178).
3. Create firewall rules specifying which addresses to accept and which ones to discard. See ***Creating Firewall Rules*** (on page 179).

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

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

Enabling the Firewall

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

To enable the PX firewall:

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

2. To enable the IPv4 firewall, click the IPv4 tab, and select the Enable IPv4 Access Control checkbox.
3. To enable the IPv6 firewall, click the IPv6 tab, and select the Enable IPv6 Access Control checkbox.
4. Click OK.

Changing the Default Policy

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

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

Default policies for inbound and outbound traffic can be different.

To change the default policy for inbound traffic:

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

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

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

To change the default policy for outbound traffic:

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

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

Creating Firewall Rules

Firewall rules determine whether to accept or discard traffic to/from the PX, based on the IP address of the host sending or receiving the traffic. When creating firewall rules, keep these principles in mind:

- **Rule order is important.**

  When traffic reaches or is sent from the PX device, the rules are executed in numerical order. Only the first rule that matches the IP address determines whether the traffic is accepted or discarded. Any subsequent rules matching the IP address are ignored by the PX.

- **Subnet mask is required.**

  When typing the IP address, you must specify BOTH the address and a subnet mask. For example, to specify a single address in a Class C network, use this format:

  x.x.x.x/24

  where */24* = a subnet mask of 255.255.255.0.

  To specify an entire subnet or range of addresses, change the subnet mask accordingly.

Note: Valid IPv4 addresses range from 0.0.0.0 through 255.255.255.255. Make sure the IPv4 addresses entered are within the scope.

To create firewall rules:

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

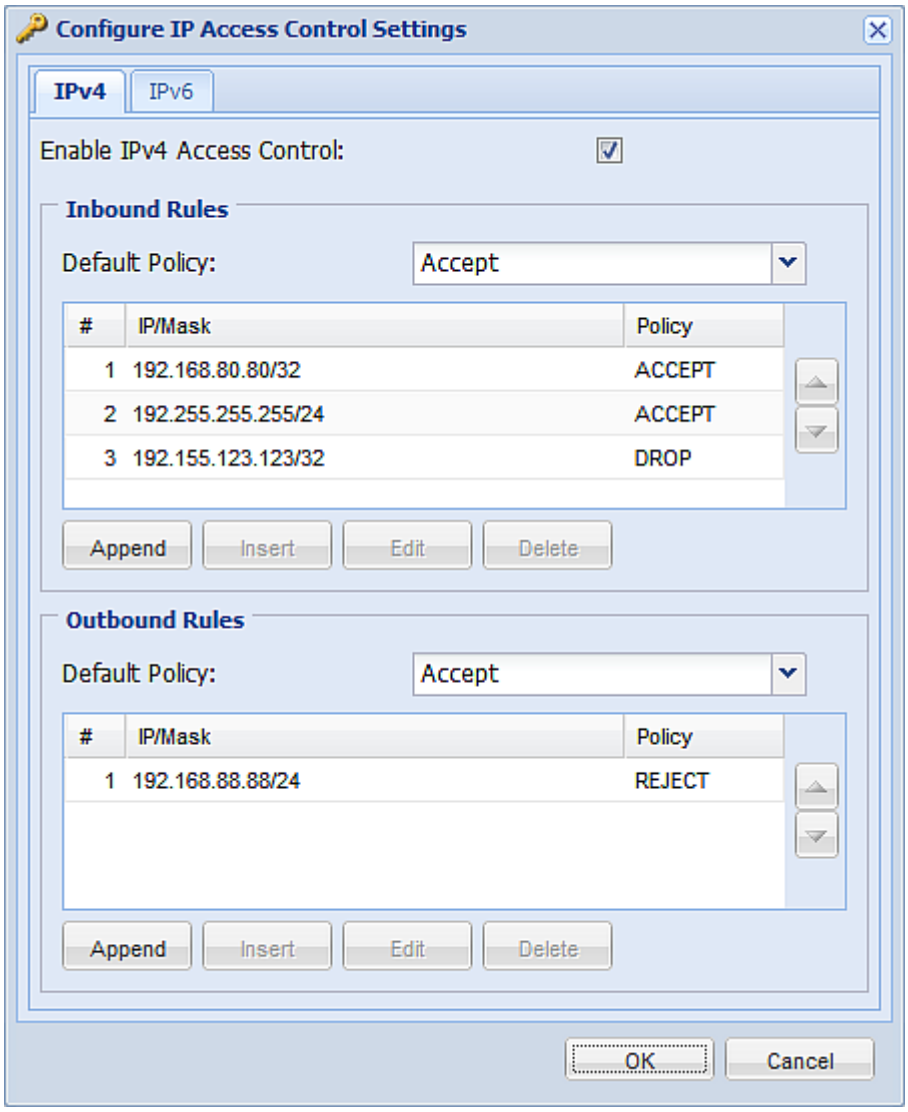
Action	Procedure

Add a rule to the end of the rules list	▪ Click Append. The "Append new Rule" dialog appears.
	▪ Type an IP address and subnet mask in the IP/Mask field.
	▪ Select Accept, Drop or Reject from the drop-down list in the Policy field.
	  ▪ Accept: Accepts traffic from/to the specified IP address(es).
	  ▪ Drop: Discards traffic from/to the specified IP address(es), without sending any failure notification to the source or destination host.
	  ▪ Reject: Discards traffic from/to the specified IP address(es), and an ICMP message is sent to the source or destination host for failure notification.
	▪ Click OK.
	The system automatically numbers the rule.

Action	Procedure

Insert a rule between two existing rules	▪ Select the rule above which you want to insert a new rule. For example, to insert a rule between rules #3 and #4, select #4.
	▪ Click Insert. The "Insert new Rule" dialog appears.
	▪ Type an IP address and subnet mask in the IP/Mask field.
	▪ Select Accept, Drop or Reject from the drop-down list in the Policy field.
	  ▪ Accept: Accepts traffic from/to the specified IP address(es).
	  ▪ Drop: Discards traffic from/to the specified IP address(es), without sending any failure notification to the source or destination host.
	  ▪ Reject: Discards traffic from/to the specified IP address(es), and an ICMP message is sent to the source or destination host for failure notification.
	▪ Click OK.
	The system inserts the rule and automatically renumbers the following rules.

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



7. Click OK. The rules are applied.

Editing Firewall Rules

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

▶ To modify a firewall rule:

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

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

Sorting Firewall Rules

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

To sort the firewall rules:

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

Deleting Firewall Rules

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

To delete a firewall rule:

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

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

Setting Up User Login Controls

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

Enabling User Blocking

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

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

Note: If any user blocking event occurs, you can unblock that user manually by using the "unblock" CLI command via a local connection. See **Unblocking a User** *(on page 520).*

To enable user blocking:

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

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

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

6. Click OK.

Enabling Login Limitations

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

To enable login limitations:

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

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

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

Enabling Strong Passwords

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

To force users to create strong passwords:

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

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

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

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

Enabling Password Aging

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

To force users to change passwords regularly:

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

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

4. Click OK.

Enabling and Editing the Security Banner

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

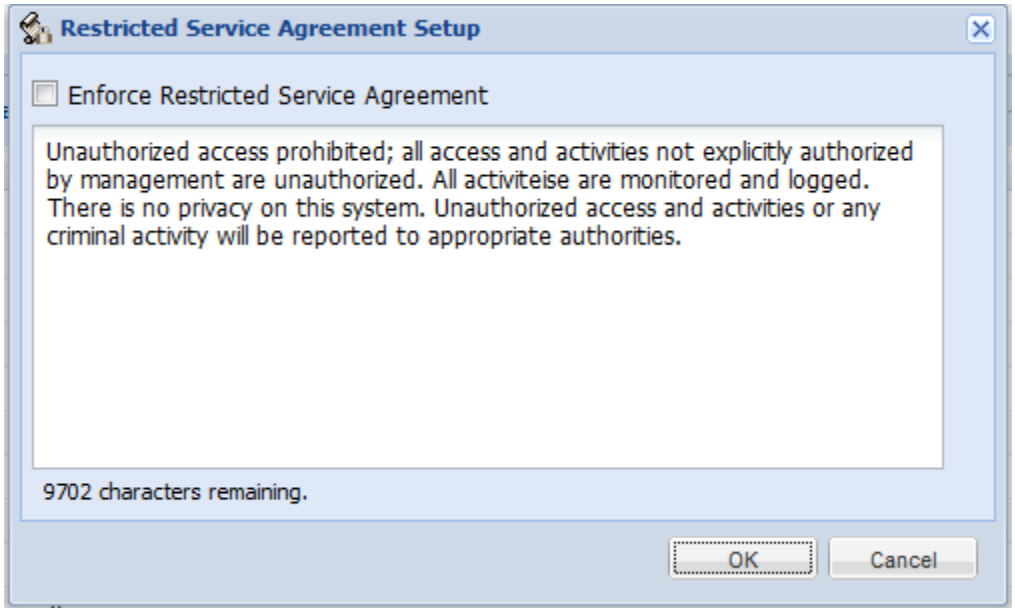
A default agreement is provided. You can edit or replace the default text as needed by typing directly in the security dialog or pasting text into it.

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

If a user declines the agreement, they cannot log in. An event notifying you if a user has accepted or declined the agreement can be created. See ***Default Log Messages*** (on page 267)

To enable the service agreement:

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



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

- In the web interface, select the checkbox labeled "I understand and accept the Restricted Service Agreement."

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

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

Setting Up Role-Based Access Control Rules

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

To set up role-based access control rules:

1. Enable the feature. See ***Enabling the Feature*** (on page 188).
2. Set the default policy. See ***Changing the Default Policy*** (on page 189).
3. Create rules specifying which addresses to accept and which ones to discard when the addresses are associated with a specific role. See ***Creating Role-Based Access Control Rules*** (on page 189).

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

Enabling the Feature

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

To enable role-based access control rules:

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

Changing the Default Policy

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

To change the default policy:

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

Creating Role-Based Access Control Rules

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

To create role-based access control rules:

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

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

Action	Do this...

Add a rule to the end of the rules list	▪ Click Append. The "Append new Rule" dialog appears.
	▪ Type a starting IP address in the Starting IP Address field.
	▪ Type an ending IP address in the Ending IP Address field.
	▪ Select a role from the drop-down list in the Role field. This rule applies to members of this role only.
	▪ Select Allow or Deny from the drop-down list in the Policy field.
	  ▪ Allow: Accepts traffic from the specified IP address range when the user is a member of the specified role
	  ▪ Deny: Drops traffic from the specified IP address range when the user is a member of the specified role
	▪ Click OK.
	The system automatically numbers the rule.

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

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

5. Click OK.

Editing Role-Based Access Control Rules

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

To modify a role-based access control rule:

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

Sorting Role-Based Access Control Rules

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

To sort role-based access control rules:

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

6. Click OK.

Deleting Role-Based Access Control Rules

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

To delete a role-based access control rule:

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

Setting Up a TLS Certificate

Important: Raritan disables SSL 3.0 and uses TLS for releases 3.0.4, 3.0.20 and later releases due to published security vulnerabilities in SSL 3.0. Make sure your network infrastructure, such as LDAP and mail services, uses TLS rather than SSL 3.0.

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

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

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

Note 2: See **Forcing HTTPS Encryption** *(on page 177) for instructions on forcing users to employ TLS when connecting to the PX.*

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

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

Certificate Signing Request

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

Creating a Certificate Signing Request

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

To create a CSR:

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

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

Field	Type this information
Common Name	The fully qualified domain name (FQDN) of your PX device.
Email Address	An email address where you or another administrative user can be reached.

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

- In the Key Creation Parameters section:

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

4. Click Create New SSL Key to create both the CSR and private key. This may take several minutes to complete.
5. To download the newly-created CSR to your computer, click Download Certificate Signing Request.
   a. You are prompted to open or save the file. Click Save to save it onto your computer.
   b. After the file is stored on your computer, submit it to a CA to obtain the digital certificate.
   c. If intended, click Delete Certificate Signing Request to remove the CSR file permanently from the PX device.
6. To store the newly-created private key on your computer, click Download Key. You are prompted to open or save the file. Click Save to save it onto your computer.
7. Click Close to quit the dialog.

Installing a CA-Signed Certificate

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

To install the certificate:

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

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

5. Click Close to quit the dialog.

Creating a Self-Signed Certificate

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

To create and install a self-signed certificate:

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

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

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

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

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

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

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

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

Installing Existing Key and Certificate Files

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

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

To install existing key and certificate files:

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

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

7. Click Close to quit the dialog.

Downloading Key and Certificate Files

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

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

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

Setting Up External Authentication

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

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

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

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

If both local and external authentication is needed, create user profiles on the PX in addition to providing the external AA server's data.

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

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

Important: Raritan disables SSL 3.0 and uses TLS for releases 3.0.4, 3.0.20 and later releases due to published security vulnerabilities in SSL 3.0. Make sure your network infrastructure, such as LDAP and mail services, uses TLS rather than SSL 3.0.

Gathering the External Authentication Information

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

Gathering the LDAP Information

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

To configure LDAP authentication, you need to check:

- The IP address or hostname of the LDAP server
- Whether the Secure LDAP protocol (LDAP over TLS) is being used
  - If Secure LDAP is in use, consult your LDAP administrator for the CA certificate file.
- The network port used by the LDAP server
- The type of the LDAP server, usually one of the following options:
  - *OpenLDAP*
    - If using an OpenLDAP server, consult the LDAP administrator for the Bind Distinguished Name (DN) and password.
  - *Microsoft Active Directory® (AD)*
    - If using a Microsoft Active Directory server, consult your AD administrator for the name of the Active Directory Domain.
- Bind Distinguished Name (DN) and password (if anonymous bind is NOT used)
- The Base DN of the server (used for searching for users)
- The login name attribute (or AuthorizationString)
- The user entry object class
- The user search subfilter (or BaseSearch)

Gathering the RADIUS Information

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

Below is the RADIUS information to gather:

- The IP address or host name of the RADIUS server
- Authentication protocol used by the RADIUS server
- Shared secret for a secure communication
- UDP authentication port used by the RADIUS server
- UDP accounting port used by the RADIUS server

Adding Authentication Servers

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

Adding LDAP Server Settings

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

If the external LDAP/LDAPS server authentication fails, an "Authentication failed" message is displayed. Details regarding the authentication failure are available in the event log. See ***Viewing the Local Event Log*** (on page 288).

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

To add new LDAP/LDAPS server settings:

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

   Important: Without the TLS encryption enabled, you can type either the domain name or IP address in this field, but you must type the fully qualified domain name if the TLS encryption is enabled.

5. Type of LDAP Server - Choose one of the following options:
   - OpenLDAP
   - Microsoft Active Directory. Active Directory is an implementation of LDAP/LDAPS directory services by Microsoft for use in Windows environments.
6. Security - Determine whether you would like to use Transport Layer Security (TLS) encryption, which is a cryptographic protocol that allows the PX to communicate securely with the LDAPS server.

   Three security options are available:
   - StartTLS
   - TLS

- None

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

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

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

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

To duplicate LDAP/LDAPS server settings:

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

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

Note: If the PX 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 PX and the LDAP server to use the same NTP server(s).

Adding RADIUS Server Settings

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

To set up RADIUS authentication:

1. Choose Device Settings > Security > Authentication. The Authentication Settings dialog appears.
2. Select the Radius radio button to enable the RADIUS authentication.
3. Click New to add a RADIUS AA server. The "Create new RADIUS Server Configuration" dialog appears.
4. Type the IP address or host name of the RADIUS server in the IP Address / Hostname field.
5. Select an authentication protocol in the "Type of RADIUS Authentication" field. Your choices include:
   - PAP (Password Authentication Protocol)
   - CHAP (Challenge Handshake Authentication Protocol)

   CHAP is generally considered more secure because the user name and password are encrypted, while in PAP they are transmitted in the clear.
6. By default, the PX uses the standard RADIUS port 1812 (authentication) and 1813 (accounting). If you prefer to use non-standard ports, change the ports.
7. Type the timeout period in seconds in the Timeout field. This sets the maximum amount of time to establish contact with the RADIUS server before timing out. Default is 1 second.
8. Type the number of retries permitted in the Retries field. Default is 3.
9. Type the shared secret in the Shared Secret and Confirm Shared Secret fields. The shared secret is necessary to protect communication with the RADIUS server.
10. To verify if the authentication configuration is set correctly, you may click Test Connection to check whether the PX can connect to the remote authentication server successfully.

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

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

More Information about AD or RADIUS Configuration

For more information about the LDAP configuration using Microsoft Active Directory, see ***LDAP Configuration Illustration*** (on page 620).

For more information on RADIUS configuration, see ***RADIUS Configuration Illustration*** (on page 635).

Sorting the Access Order

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

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

To re-sort the authentication server access list:

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

Testing the Server Connection

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

To test the connection to an authentication server:

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

Editing Authentication Server Settings

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

To modify the external authentication configuration:

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

Deleting Authentication Server Settings

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

To remove one or multiple authentication servers:

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

Disabling External Authentication

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

To disable the external authentication service:

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

Enabling External and Local Authentication Services

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

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

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

To enable both authentication services:

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

Outlet Management

PX allows you to remotely monitor and control outlets and manage outlet settings through the web interface.

Note: To configure power thresholds, see **Setting Power Thresholds** *(on page 229).*

PX3 Latching Relay Behavior

PX3 incorporates latching relays in models with outlet switching. Unlike non-latching relays, latching relays do NOT require power to keep their contacts closed.

PX3 outlet switching can be configured to operate as a true latching relay or to simulate a non-latching relay. The operating mode determines the latching relay behavior when PDU power is lost. Regardless of which mode is selected, power is not required to keep relay contacts closed.

Outlet Relay Behavior in Latching and Non-Latching Mode

Non-Latching Mode:

- Relay always opens when power is lost. This insures all relays are open when power is applied to the PDU.
- Always select this mode if the combined in-rush current of the devices connected to the PDU trip circuit breakers when power is applied to the PDU.
- This is the factory default operating mode.

Latching Mode:

- Relay does not open when power is lost.
- This is the preferred operating mode ONLY if you are sure in-rush current does not trip circuit breakers when power is applied to the PDU.
- Power to the outlet is not disrupted if a PDU internal failure occurs.
- In Latching mode, the following features are disabled.
  - PDU-level outlet state on startup: See ***Setting the PDU-Defined Default State*** (on page 214).
  - Outlet-level outlet state on startup: See ***Setting the Outlet-Specific Default State*** (on page 214).
  - PDU-level outlet initialization delay on startup: See ***Setting the Initialization Delay*** (on page 217).

Setting the Outlet Relay Behavior

1. Click the PDU folder.

   Note: The folder is named "my PX" by default. The name can be customized. See **Naming the PDU** *(on page 130).*

2. Click Setup in the Settings section. The Pdu Setup dialog appears.
3. In the "Relay behavior on power loss" field, select Latching or Non-latching.

Note: To change the outlet relay behavior using the CLI command, see **Setting the Outlet Relay Behavior** *(on page 399).*

Naming Outlets

You can give each outlet a unique name up to 32 characters long to identify the equipment connected to it. The customized name is followed by the label in parentheses.

Note: In this context, a label is an outlet number, such as 1, 2, 3 and so on.

To name an outlet:

1. Expand the Outlets folder in the PX Explorer pane to show all outlets. See ***Expanding the Tree*** (on page 114).
2. In the PX Explorer pane, click the outlet you want. The page specific to that outlet opens in the right pane.
3. Click Setup in the right pane. The setup dialog for the selected outlet appears.

   Tip: Another way to trigger the same dialog is to use the Outlets page. Select the Outlets folder, highlight the outlet on the Outlets page and then click Setup at the bottom of the page.
4. Type a name in the Outlet Name field.
5. Click OK.

Outlet Monitoring

The PX Explorer pane provides quick access to the outlet information. The outlet information, such as RMS current, active power, power factor, and so on, is displayed immediately after an outlet icon in the tree is selected.

Note: RMS refers to Root Mean Square, a statistical method for measuring certain types of variables. In this context, it gives the value of current that is equivalent to a DC value.

Monitoring All Outlets

You can view the current status of all outlets at a time.

To monitor all outlets:

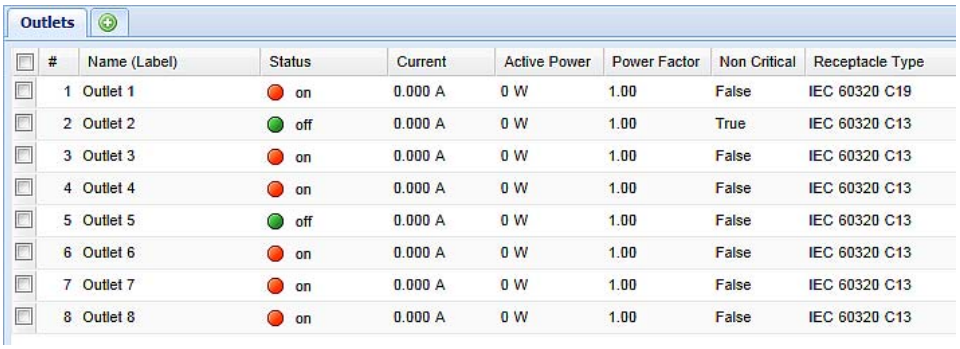
1. Expand the PDU folder in the PX Explorer pane if necessary. See ***Expanding the Tree*** (on page 114).
2. Click the Outlets folder, and the Outlets page opens in the right pane, showing all outlets with the following information:
   - Outlet number (#)

- Outlet name
- Outlet status (on/off)
- Outlet sensor readings:

  - RMS current (A)

  - Active power (W)

  - Power factor
- Non-critical outlet settings (True/False) if the PDU is outlet-switching capable
- Outlet receptacle type



#	Name (Label)	Status	Current	Active Power	Power Factor	Non Critical	Receptacle Type
1	Outlet 1	on	0.000 A	0 W	1.00	False	IEC 60320 C19
2	Outlet 2	off	0.000 A	0 W	1.00	True	IEC 60320 C13
3	Outlet 3	on	0.000 A	0 W	1.00	False	IEC 60320 C13
4	Outlet 4	on	0.000 A	0 W	1.00	False	IEC 60320 C13
5	Outlet 5	off	0.000 A	0 W	1.00	False	IEC 60320 C13
6	Outlet 6	on	0.000 A	0 W	1.00	False	IEC 60320 C13
7	Outlet 7	on	0.000 A	0 W	1.00	False	IEC 60320 C13
8	Outlet 8	on	0.000 A	0 W	1.00	False	IEC 60320 C13

Note: If a sensor row is colored, it means the sensor reading already crosses one of the thresholds, the sensor enters an alarmed state, or the overcurrent protector has tripped or blown. See **The Yellow- or Red-Highlighted Sensors** *(on page 119).*

Monitoring an Outlet

To view a particular outlet's detailed information, follow this procedure.

To monitor an outlet:

1. Expand the Outlets folder in the PX Explorer pane to show all outlets. See ***Expanding the Tree*** (on page 114).
2. Click the outlet you want in the PX Explorer pane, and the outlet's details are shown in the right pane, including:

   - Outlet label (number)
   - Outlet name
   - Outlet status (on/off)

   Note: The outlet status is only available on an outlet-switching capable PX device.

   - Outlet receptacle type

- Line pair associated with this outlet
- Overcurrent protector like a circuit breaker that protects this outlet, if available on your model
- Outlet state on device startup
- Power off period during power cycle
- Non-critical outlet settings (False/True)

Note: The above three pieces of information are only available on an outlet-switching capable PX device.

- Outlet sensor readings:
  - RMS current (A)
  - RMS voltage (V)
  - Active power (W)
  - Apparent power (VA)
  - Power factor
  - Active energy (Wh)
  - Line frequency (Hz), if available on your model

The outlet readings turn to zero if the associated circuit breaker trips or the fuse blows.

Note: If a sensor row is colored, it means the sensor reading already crosses one of the thresholds, the sensor enters an alarmed state, or the overcurrent protector has tripped or blown. See **The Yellow- or Red-Highlighted Sensors** *(on page 119).*

Outlet Switching

This section applies to outlet-switching capable models only.

You can change the power status of one or multiple outlets with one click in the web interface. To change the power state, you must have the *Switch Outlet* permission.

Tip: To switch an outlet using the front panel display, see **Power Control** *(on page 86) for PX3 phase II models or* **Outlet Switching** *(on page 609) for PX3 phase I models.*

Switching Multiple or All Outlets

This section applies to outlet-switching capable models only.

The power state can be changed regardless of each outlet's current state. That is, you can turn on or off or power cycle the outlets even if they are already in the selected state.

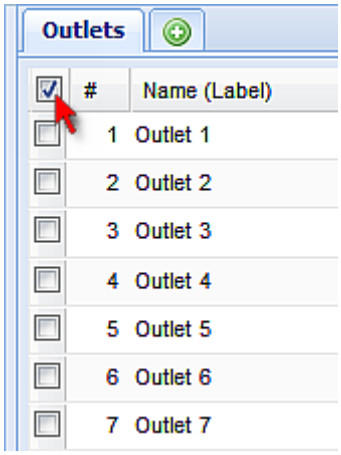
Power cycling the outlet(s) turns the outlet(s) off and then back on.

To turn on or off multiple or all outlets, or cycle their power:

1. Expand the PDU folder in the PX Explorer pane if necessary. See ***Expanding the Tree*** (on page 114).

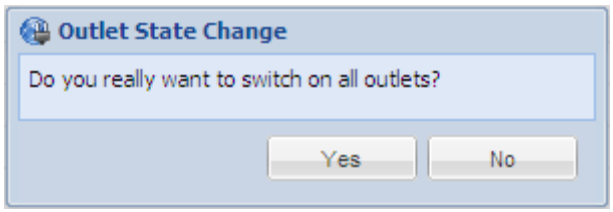
   Note: The folder is named "my PX" by default. The name can be customized. See **Naming the PDU** *(on page 130).*

2. Click the Outlets folder, and the Outlets page opens in the right pane.
3. Select the outlets whose power states you want to change, and ensure their checkboxes are all selected.
   - To select all outlets, select the top checkbox in the header row.



   - To select multiple outlets, click the checkbox of each desired outlet one by one. Or press Shift while clicking on the rows of the first and last outlets to select a range of consecutive outlets.
   - To select a single outlet, select that outlet's checkbox.
4. Click On, Off, or Cycle.

5. A dialog for confirming the operation appears. Click Yes and all outlets switch ON, OFF, or cycle their power.



Switching an Outlet

This section applies to outlet-switching capable models only.

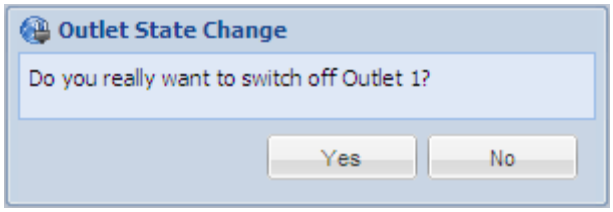
You can turn on or off or power cycle any outlet regardless of the outlet's current state.

Power cycling the outlet(s) turns the outlet(s) off and then back on.

There are different ways to turn an outlet on or off, or cycle its power.

To control an outlet with a particular outlet icon selected:

1. Expand the Outlets folder in the PX Explorer pane to show all outlets. See ***Expanding the Tree*** (on page 114).
2. Click the outlet you want in the PX Explorer pane, and locate the Control section in the right pane.
3. Click On, Off, or Cycle.
4. A dialog for confirming the operation appears. Click Yes and the outlet switches ON, OFF, or cycles its power.



To control an outlet with the Outlets folder icon selected:

- The procedure is similar to the one described in the section titled ***Switching Multiple or All Outlets*** (on page 211).

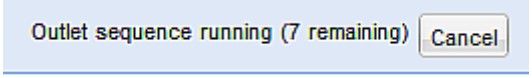
Stopping the Power-On Sequence

This section applies to outlet-switching capable models only.

The PX allows you to stop the outlet power-on sequence while all outlets are being turned on. This function is useful when you have set a certain power-on sequence and certain outlets' power-on delay timing causes it to take a long time to turn on the next outlets, but you do not intend to wait anymore.

To cancel the power-on process:

1. Open the Outlets page to turn on ALL outlets. See ***Switching Multiple or All Outlets*** (on page 211).
2. The Cancel button as shown below appears at the bottom of the Outlets page. The number in parentheses indicates how many outlets are not powered on yet.



3. Click Cancel to immediately stop the power-on process.

Setting the Default Outlet State

This section applies to outlet-switching capable models only.

Default outlet state determines the initial power state of outlets after the PX device powers up. You can set up the default outlet state for all outlets or for a specific outlet. Note that the value set for an individual outlet always overrides the value set for all outlets.

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.

Setting the PDU-Defined Default State

This section applies to outlet-switching capable models only.

This procedure sets the PDU-defined outlet state, which determines the initial power state of all outlets after powering up the PX device.

Tip: To set a different state on a particular outlet, see **Setting the Outlet-Specific Default State** *(on page 214).*

To set the default state for all outlets:

1. Click the PDU folder.

   Note: The folder is named "my PX" by default. The name can be customized. See **Naming the PDU** *(on page 130).*

2. Click Setup in the Settings section. The Pdu Setup dialog appears.
3. In the "Outlet state on device startup" field, click the drop-down arrow and select an option from the list.
   - on: Turns on all outlets when the PX powers up.
   - off: Turns off all outlets when the PX powers up.
   - last known: Restores all outlets to their previous power states before the PX was powered off.
4. Click OK.

Setting the Outlet-Specific Default State

This section applies to outlet-switching capable models only.

By default, the power state of each outlet follows the PDU-defined setting. Setting the default state of a particular outlet to a value other than "PDU defined" overrides the PDU-defined setting on that outlet.

To set the default power state for a specific outlet:

1. Expand the Outlets folder in the PX Explorer pane to show all outlets. See ***Expanding the Tree*** (on page 114).
2. In the PX Explorer pane, click the outlet you want. The page specific to that outlet opens in the right pane.
3. Click Setup in the right pane. The setup dialog for the selected outlet appears.

Tip: Another way to trigger the same dialog is to use the Outlets page. Select the Outlets folder, highlight the outlet on the Outlets page and then click Setup at the bottom of the page.

4. In the "State on device startup" field, click the drop-down arrow and select an option from the list.
   - on: Turns on this outlet when the PX powers up.
   - off: Turns off this outlet when the PX powers up.
   - last known: Restores this outlet to the previous power state before the PX was powered off.
   - PDU defined: The outlet's default power state is determined according to the PDU-defined state. See ***Setting the PDU-Defined Default State*** (on page 214).

Tip: The information in parentheses following the option "PDU defined" indicates the current PDU-defined selection.

5. Click OK.

Changing the Cycling Power-Off Period

This section applies to outlet-switching capable models only.

Power cycling the outlet(s) turns the outlet(s) off and then back on. You can adjust the length of the time it takes for the outlets to turn back on after they are switched OFF.

The power-off period during the power cycle can be set for all outlets or for an individual outlet. Note that the value set for an individual outlet always overrides the value set for all outlets.

Changing the PDU-Defined Cycling Power-Off Period

This section applies to outlet-switching capable models only.

The "PDU-defined" power-off period determines how long it takes for ALL outlets to turn on after they are turned OFF during the power cycle. The default PDU-defined power-off period is 10 seconds (10 s).

Note: To set a different power-off period on a particular outlet, see **Changing the Outlet-Specific Cycling Power-Off Period** *(on page 216).*

To set the power-off period for all outlets:

1. Click the PDU folder.

Note: The folder is named "my PX" by default. The name can be customized. See **Naming the PDU** *(on page 130).*

2. Click Setup in the Settings section. The Pdu Setup dialog appears.
3. In the "Power off period during power cycle" field, click the drop-down arrow and select an option from the list. Valid range is zero second to one hour.

   Time units in the list are explained below:

   - s: second(s)
   - min: minute(s)
   - h: hour(s)

   You can also type a value if the desired time is not listed. For example, type "15 s" for 15 seconds.
4. Click OK.

Tip: When there are a large number of outlets, set the value to a lower number so that you can avoid a long wait before all the outlets are available again.

Changing the Outlet-Specific Cycling Power-Off Period

This section applies to outlet-switching capable models only.

When the power cycling occurs, the default power-off period of each outlet follows the PDU-defined setting. You can adjust the power-off period of a particular outlet so that it is turned back on after a different power-off period.

Setting the power-off period for a particular outlet to a value other than "PDU defined" overrides the PDU-defined setting on that outlet.

To set the power-off period for a specific outlet:

1. Expand the Outlets folder in the PX Explorer pane to show all outlets. See ***Expanding the Tree*** (on page 114).
2. In the PX Explorer pane, click the outlet you want. The page specific to that outlet opens in the right pane.
3. Click Setup in the right pane. The setup dialog for the selected outlet appears.

Tip: Another way to trigger the same dialog is to use the Outlets page. Select the Outlets folder, highlight the outlet on the Outlets page and then click Setup at the bottom of the page.

4. In the "Power off period during power cycle" field, click the drop-down arrow and select an option from the list. Valid range is zero second to one hour.

   Time units in the list are explained below:

   - s: second(s)
   - min: minute(s)
   - h: hour(s)
   - To make the outlet's power-off period identical to the PDU-defined setting, select the "PDU defined" option. See ***Changing the PDU-Defined Cycling Power-Off Period*** (on page 215).

   Tip: The information in parentheses following the option "PDU defined" indicates the current PDU-defined selection.

   You can also type a value if the desired time is not listed. For example, type "15 s" for 15 seconds.

5. Click OK.

Setting the Initialization Delay

This section applies to outlet-switching capable models only.

The outlet initialization delay determines how long the PX device waits before providing power to all outlets during power cycling or after recovering from a temporary power loss. This is useful in cases where power may not initially be stable after being restored, or when UPS batteries may be charging.

To set the initialization delay for all outlets:

1. Click the PDU folder.

   Note: The folder is named "my PX" by default. The name can be customized. See **Naming the PDU** *(on page 130).*

2. Click Setup in the Settings section. The Pdu Setup dialog appears.
3. In the "Outlet initialization delay on device startup" field, click the drop-down arrow and select an option from the list. Valid range is 1 second to 1 hour.

   Time units in the list are explained below:

   - s: second(s)
   - min: minute(s)
   - h: hour(s)

You can also type a value if the desired time is not listed. For example, type "15 s" for 15 seconds.

4. Click OK.

Tip: When there are a large number of outlets, set the value to a lower number so that you can avoid a long wait before all the outlets are available again.

Setting the Inrush Guard Delay

This section applies to outlet-switching capable models only.

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. The inrush guard delay feature prevents 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.

To set the inrush guard delay time:

1. Click the PDU folder.

   Note: The folder is named "my PX" by default. The name can be customized. See **Naming the PDU** *(on page 130).*

2. Click Setup in the Settings section. The Pdu Setup dialog appears.
3. In the Inrush Guard Delay field, select a delay from 100 milliseconds to 2 seconds.
   - ms: millisecond(s)
   - s: second(s)

   Type a value if the desired time is not listed. For example, type "600 ms" for 600 milliseconds.
4. Click OK.

Setting the Outlet Power-On Sequence

This section applies to outlet-switching capable models only.

By default, the outlets are sequentially powered on in ascending order from outlet 1 to the highest-numbered outlet when turning ON or power cycling all outlets on the PX device. 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.

To set the outlet power-on sequence:

1. Trigger the Outlet Sequence Setup dialog by doing either of the following:
   - Click the Outlets folder, and the Outlets page opens in the right pane. Click Sequence Setup.
   - Click the PDU folder, and then the Setup button in the Outlet Sequence section.

   Note: The folder is named "my PX" by default. The name can be customized. See **Naming the PDU** *(on page 130).*

   The Outlet Sequence Setup dialog appears, with the current power-up sequence indicated by the outlet order in the list.
2. To change the priority of an outlet, select it from the list and click one of the following buttons.
   - : Moves the outlet to the top of the list, making it the first one to receive power.
   - : Moves the outlet up one position in the list.
   - : Moves the outlet down one position in the list.
   - : Moves the outlet to the bottom of the list, making it the final one to receive power.
   - : Restores the list to the default power-up sequence, that is, the ascending order starting at outlet 1.
3. Click OK.

Next time when power cycling the PX, it will turn on all outlets based on the new order of the list.

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

Setting the Outlet-Specific Power-On Delay

This section applies to outlet-switching capable models only.

You can make a power-on delay occur between two outlets that are turned on consecutively when the PX turns on all outlets.

For example, if the power-up sequence is Outlet 1 through Outlet 12, and you want the PX to wait for 5 seconds after turning on Outlet 3 before turning on Outlet 4, assign a delay of 5 seconds on Outlet 3.

To set the outlet-specific power-on delay:

1. Trigger the Outlet Sequence Setup dialog by doing either of the following:
   - Click the Outlets folder, and the Outlets page opens in the right pane. Click Sequence Setup.
   - Click the PDU folder, and then the Setup button in the Outlet Sequence section.

   Note: The folder is named "my PX" by default. The name can be customized. See **Naming the PDU** *(on page 130).*
2. Click the Delay column of the outlet where a delay is intended after this outlet is turned on, delete the existing value and type a new number in seconds. The number can be a decimal number.
   - To disable the delay, simply type the number 0 (zero).
3. Repeat the above step to change the delay settings of additional outlets.
4. Click OK.

Setting Non-Critical Outlets and Load Shedding Mode

This section applies to outlet-switching capable models only.

When a UPS supplying power to the PX 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.

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

Outlets that are turned off when load shedding is activated are called non-critical. Outlets that are not affected by load shedding are called critical outlets. When load shedding is deactivated, the PX will turn back on all non-critical outlets. By default, all outlets are configured as critical until you configure them otherwise.

Marking All Outlets

This section applies to outlet-switching capable models only.

You can configure all critical and non-critical outlets at a time.

To mark all outlets at a time:

1. Click the PDU folder.

   Note: The folder is named "my PX" by default. The name can be customized. See **Naming the PDU** *(on page 130).*

2. Click Setup in the Load Shedding section. The Load Shedding Setup dialog appears.

   Tip: Another way to trigger the same dialog is to use the Outlets page. Select the Outlets folder, and then click the Setup button near the Load Shedding section at the lower left corner of the page.

3. To mark an outlet as "non-critical," select it from the "Critical outlets" list box, and click to move it to the "Non-critical outlets" list box. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.

   To move all outlets in the "Critical outlets" list box to the "Non-critical outlets" list box, click .

4. To mark an outlet as "critical," select it from the "Non-critical outlets" list box, and click to move it to the "Critical outlets" list box. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.

   To move all outlets in the "Non-critical outlets" list box to the "Critical outlets" list box, click .

5. Click OK.

Marking an Outlet

This section applies to outlet-switching capable models only.

You can also choose to mark a specific outlet as a critical or non-critical outlet in its setup dialog.

To mark an outlet:

1. Expand the Outlets folder in the PX Explorer pane to show all outlets. See ***Expanding the Tree*** (on page 114).
2. In the PX Explorer pane, click the outlet you want. The page specific to that outlet opens in the right pane.

3. Click Setup in the right pane. The setup dialog for the selected outlet appears.

   Tip: Another way to trigger the same dialog is to use the Outlets page. Select the Outlets folder, highlight the outlet on the Outlets page and then click Setup at the bottom of the page.

4. In the Non Critical field, select an option from the drop-down list.
   - True: This option marks the outlet as a non-critical outlet.
   - False: This option marks the outlet as a critical outlet.
5. Click OK.

Activating or Deactivating the Load Shedding Mode

This section applies to outlet-switching capable models only.

When entering the load shedding mode, PX turns OFF all non-critical outlets.

When exiting from the load shedding mode, PX turns ON all non-critical outlets that were ON before entering the load shedding mode.

You can activate or deactivate this mode from the PDU or Outlets page.

To enter or exit from the load shedding mode from the PDU page:

1. Click the PDU folder.

   Note: The folder is named "my PX" by default. The name can be customized. See **Naming the PDU** *(on page 130).*

2. In the Load Shedding section, click Start to enter the load shedding mode or Stop to deactivate the mode.
3. You are then prompted to confirm this operation.

   If you chose to activate the mode in the previous step, click Yes to turn off all non-critical outlets. If you chose to deactivate the mode, click Yes to turn on all non-critical outlets that were previously ON prior to the load shedding mode.

To enter or exit from the load shedding mode from the Outlets page:

1. Expand the PDU folder in the PX Explorer pane if necessary. See ***Expanding the Tree*** (on page 114).
2. Click the Outlets folder, and the Outlets page opens in the right pane.

3. To enter the load shedding mode, click Start near the Load Shedding section at the lower left corner of the page. To exit from the load shedding mode, click Stop.
4. You are then prompted to confirm this operation.

   If you chose to activate the mode in the previous step, click Yes to turn off all non-critical outlets. If you chose to deactivate the mode, click Yes to turn on all non-critical outlets that were previously ON prior to the load shedding mode.

Note: During the load shedding mode, this icon *appears on all non-critical outlets on the Outlets page, and you CANNOT turn on any of them.*

Resetting Outlet Active Energy Readings

You can reset the active energy readings of either one outlet or multiple outlets at a time.

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

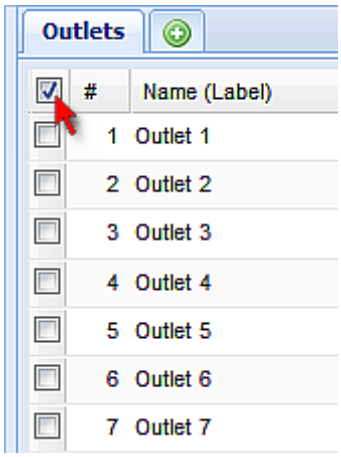
To reset active energy readings of one outlet:

1. Expand the Outlets folder in the PX Explorer pane to show all outlets. See ***Expanding the Tree*** (on page 114).
2. In the PX Explorer pane, select the outlet whose active energy you want to reset.
3. Click Reset Active Energy in the Sensors section.
4. Click Yes on the confirmation message. The "Active Energy" reading of the selected outlet now shows 0 (zero) Wh.

To reset active energy readings of multiple or all outlets:

1. Click the Outlets folder to open the Outlets page.
2. On the Outlets page, select the checkboxes of the outlets whose active energy you wan to reset.
   - To select multiple outlets, click the checkbox of each desired outlet one by one. Or press Shift while clicking on the rows of the first and last outlets to select a range of consecutive outlets.

- To select all outlets, select the top checkbox in the header row.



3. Click Reset Active Energy at the bottom of the page.
4. Click Yes on the confirmation message. The "Active Energy" readings of all selected outlets are now reset to 0 (zero) Wh.

Enabling Front Panel Outlet Switching

This section applies to outlet-switching capable models only.

You can operate the front panel buttons to switch on or off an outlet. By default, this function is disabled.

To enable the front panel outlet switching function:

1. Choose Device Settings > Security > Front Panel Permissions. The Front Panel Permissions dialog appears.
2. Select the "Outlet switching" checkbox.
3. Click OK.

Inlet and Overcurrent Protector Management

You can name each inlet and overcurrent protector or monitor the inlet status. Or you can reset the inlet's active energy reading.

Note: To configure power thresholds, see **Setting Power Thresholds** *(on page 229).*

Naming the Inlet

You can customize the inlet's name for your own purpose. For example, you can name an inlet to identify its power source. The customized name is followed by the label in parentheses.

Note: In this context, the label refers to the inlet number, such as I1.

This function is especially useful if there are multiple inlets on your PX device.

To name the inlet:

1. Click Inlet I1 in the PX Explorer pane, and the Inlet I1 page opens in the right pane.
2. Click Setup. The Inlet I1 Setup dialog appears.
3. Type a new name in the Name field.
4. Click OK.

Naming Overcurrent Protectors

You can name each overcurrent protector for easily identifying them. The customized name is followed by the label in parentheses.

Note: In this context, a label is an overcurrent protector number, such as C1 for a circuit breaker or F1 for a fuse.

To name an overcurrent protector:

1. Expand the Overcurrent Protectors folder in the PX Explorer pane if needed. See ***Expanding the Tree*** (on page 114).
2. In the PX Explorer pane, click the desired overcurrent protector. The page specific to that overcurrent protector opens in the right pane.
3. Click Setup. The Overcurrent Protector Setup dialog appears.

   Tip: You can also trigger the same dialog by selecting the Overcurrent Protectors folder, then selecting an overcurrent protector and clicking Setup on the Overcurrent Protectors page.
4. Type a new name in the Name field.
5. Click OK.

Monitoring the Inlet

You can view the inlet's details, including its:

- Label (number)
- Customized name

- Inlet sensor readings:
  - RMS current per line (A)
  - RMS voltage per line pair (V)
  - Active power (W)
  - Apparent power (VA)
  - Power factor
  - Active energy (Wh)
  - Unbalanced load percentage (for 3-phase models)
  - Line frequency (Hz), if available on your PDU

Note: If a sensor row is colored, it means the sensor reading already crosses one of the thresholds or the sensor enters the alarmed state. *See* **The Yellow- or Red-Highlighted Sensors** *(on page 119).*

There are two ways to access the inlet information.

To get the overview of the inlet status:

1. Click the Dashboard icon in the PX Explorer pane, and the Dashboard page opens in the right pane.
2. Locate the Inlet section on the Dashboard page.

To view the inlet's details:

Click Inlet I1 in the PX Explorer pane, and the Inlet I1 page opens in the right pane.

Monitoring Overcurrent Protectors

Each overcurrent protector on the PX device delivers power to a bank of outlets, and draws power from one or two lines.

You can view the overcurrent protector's details, including its:

- Label (number)
- Name
- Status (closed/open)
- Type
- Lines associated with this overcurrent protector
- Outlets protected by this overcurrent protector
- Sensor readings:
  - Current drawn (A)
  - Current remaining (A)

Note: If a sensor row is colored, it means the sensor reading already crosses one of the thresholds, the sensor enters an alarmed state, or the overcurrent protector has tripped or blown. See **The Yellow- or Red-Highlighted Sensors** *(on page 119).*

You can view the summary of all overcurrent protectors at a time or the status of individual overcurrent protectors.

To view all overcurrent protectors' status:

You can check the status of all overcurrent protector at a time via either the Dashboard or Overcurrent Protectors page.

- **Using the Dashboard page:**

a. Click the Dashboard icon in the PX Explorer pane, and the Dashboard page opens in the right pane.

b. Locate the Overcurrent Protectors section on the Dashboard page.

- **Using the Overcurrent Protectors page:**

a. Expand the PDU folder in the PX Explorer pane if necessary. See ***Expanding the Tree*** (on page 114).

b. Click Overcurrent Protectors in the PX Explorer pane to open the Overcurrent Protectors page.

To view an overcurrent protector's details:

1. Expand the Overcurrent Protectors folder in the PX Explorer pane if needed. See ***Expanding the Tree*** (on page 114).
2. In the PX Explorer pane, click the desired overcurrent protector. The page specific to that overcurrent protector opens in the right pane.

Resetting Inlet Active Energy Readings

You can manually reset the active energy readings of an individual inlet instead of resetting all active energy readings of the PDU. This is especially useful when your PX has more than one inlet.

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

To reset active energy readings of one inlet:

1. If your PX has multiple inlets, expand the Inlet folder in the PX Explorer pane to show all inlets. See ***Expanding the Tree*** (on page 114). If your PX has only one inlet, skip this step.
2. Select the inlet whose active energy you want to reset.
3. Click Reset Active Energy in the Power section.

4. Click Yes on the confirmation message. The 'Active Energy' reading of the selected inlet now shows 0 (zero) Wh.

Tip: You can reset all active energy readings at a time. See **Resetting All Active Energy Readings** *(on page 165).*

Disabling an Inlet (for Multi-Inlet PDUs)

The PX, if it has more than one inlet, enables all inlets by default so that the PX detects and displays all sensors' readings and states, and reports or shows warnings, events or alarm notifications associated with all inlets, outlets and overcurrent protectors (if available).

After disabling an inlet, the following information or feature is no longer available:

- All of the sensor readings, states, warnings, event or alarm notifications associated with the disabled inlet
- All of the sensor readings, states, warnings, event or alarm notifications for the outlets and overcurrent protectors associated with the disabled inlet
- The outlet-switching functionality, if available, for those outlets associated with the disabled inlet

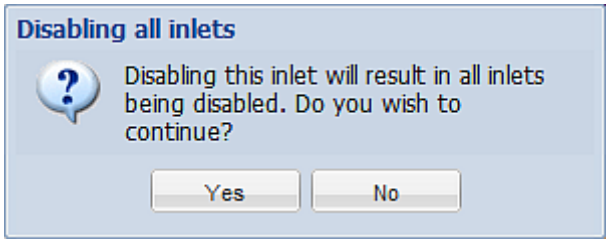
Exception: All active energy sensors continue to accumulate data regardless of whether any inlet has been disabled.

Warning: A disabled inlet, if remaining connected to a power source, continues to receive power from the connected power source and supplies power continuously to the associated outlets and overcurrent protectors.

To disable an inlet:

1. Click the Inlets folder in the PX Explorer pane, and the Inlets page opens in the right pane.
2. Select the inlet that you want to disable.
3. Click Setup.
4. Select the "Disable this inlet" checkbox.
5. To disable additional inlets, repeat the above steps.

6. If disabling an inlet will result in all inlets being disabled, a confirmation dialog appears, indicating that all inlets will be disabled. Then click Yes to confirm this operation or No to abort it.



Setting Power Thresholds

Setting and enabling the thresholds causes the PX to generate alert notifications when it detects that any component's power state crosses the thresholds. See ***The Yellow- or Red-Highlighted Sensors*** (on page 119).

There are four thresholds for each sensor: Lower Critical, Lower Warning, Upper Warning and Upper Critical.

- Upper and Lower Warning thresholds indicate the sensor reading enters the warning level.
- Upper and Lower Critical thresholds indicate the sensor reading enters the critical level.

To avoid generating a large amount of alert events, you can set the assertion timeout and deassertion hysteresis.

For detailed information, see ***Sensor Threshold Settings*** (on page 667).

Note: After setting the thresholds, remember to configure event rules. See **Event Rules and Actions** *(on page 236).*

Setting an Outlet's Thresholds

You can set up the thresholds, deassertion hysteresis and assertion timeout for a particular outlet.

The threshold values set for an individual outlet will override the bulk threshold values stored on that outlet. See ***Bulk Configuration for Outlet Thresholds*** (on page 230).

To set the thresholds for an outlet:

1. Expand the Outlets folder in the PX Explorer pane to show all outlets. See ***Expanding the Tree*** (on page 114).
2. In the PX Explorer pane, click the outlet you want. The page specific to that outlet opens in the right pane.

3. Click Setup in the right pane. The setup dialog for the selected outlet appears.

   Tip: Another way to trigger the same dialog is to use the Outlets page. Select the Outlets folder, highlight the outlet on the Outlets page and then click Setup at the bottom of the page.

4. In the Threshold Configuration table, click the sensor whose thresholds you want to configure.
5. Click Edit or double-click the desired sensor. A threshold setup dialog appears.
6. Configure the Lower Critical, Lower Warning, Upper Warning and Upper Critical thresholds respectively.
   - To enable any threshold, select the corresponding checkbox. To disable a threshold, deselect the checkbox.
   - After any threshold is enabled, type an appropriate numeric value in the accompanying text box.
7. To set the deassertion hysteresis, type a numeric value in the Deassertion Hysteresis field. See ***"To De-assert" and Deassertion Hysteresis*** (on page 672).
8. To set the assertion timeout, type a numeric value in the Assertion Timeout (samples) field. See ***"To Assert" and Assertion Timeout*** (on page 670).
9. Click OK in the threshold setup dialog to retain the changes.
10. To set the thresholds for other sensors, repeat Steps 4 to 9.
11. Click OK.

Important: The final step is required or the threshold changes are not saved.

Bulk Configuration for Outlet Thresholds

The PX allows you to set the power thresholds for multiple outlets at a time so that you can save time when configuring a number of outlet thresholds.

Note: To set the power thresholds for an individual outlet, you can either follow the instructions below or those described in the section **Setting an Outlet's Thresholds** *(on page 229).*

▶ To configure thresholds, deassertion hysteresis and assertion timeout for multiple outlets:

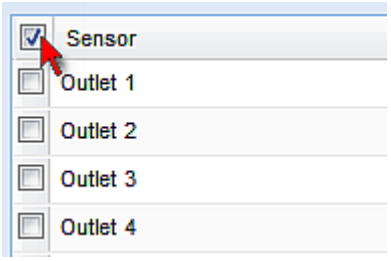
1. Expand the PDU folder in the PX Explorer pane if necessary. See ***Expanding the Tree*** (on page 114).

Note: The folder is named "my PX" by default. The name can be customized. See **Naming the PDU** *(on page 130).*

2. Click the Outlets folder. The Outlets page opens.
3. Click Bulk Setup. The Outlet Threshold Bulk Setup dialog appears, with a list of all outlets.
4. In the "Show Outlet Sensors of Type" field, select the type of power thresholds you want to configure.
5. In the "For Outlets of Receptacle Type" field, select the receptacle type you want to configure.

   All outlets of the selected receptacle type are then listed.

   - To show all outlets on the PX regardless of receptacle types, select Any.
6. Select desired outlets by having their corresponding checkboxes selected.
   - To select all outlets in the list, select the checkbox labeled Sensor in the header row, and all checkboxes are selected.



   - To select partial outlets, select the corresponding checkboxes of those outlets by clicking their checkboxes.
   - To deselect any outlet, just click the checkbox once again.
7. Click Edit Thresholds. The threshold bulk setup dialog appears.
8. Configure the Lower Critical, Lower Warning, Upper Warning and Upper Critical thresholds respectively.
   - To enable any threshold, select the corresponding checkbox. To disable a threshold, deselect the checkbox.
   - After any threshold is enabled, type an appropriate numeric value in the accompanying text box.
9. To set the deassertion hysteresis, type a numeric value in the Deassertion Hysteresis field. See ***"To De-assert" and Deassertion Hysteresis*** (on page 672).
10. To set the assertion timeout, type a numeric value in the Assertion Timeout (samples) field. See ***"To Assert" and Assertion Timeout*** (on page 670).
11. Click OK.

Setting Inlet Thresholds

You can set the inlet thresholds so that the alerts are generated when the inlet current and/or voltage crosses the thresholds.

To set the inlet thresholds:

1. Click Inlet I1 in the PX Explorer pane, and the Inlet I1 page opens in the right pane.
2. Click Setup. The Inlet I1 Setup dialog appears.
3. In the Threshold Configuration table, click the sensor whose thresholds you want to configure.
4. Click Edit or double-click the desired sensor. A threshold setup dialog appears.
5. Configure the Lower Critical, Lower Warning, Upper Warning and Upper Critical thresholds respectively.
   - To enable any threshold, select the corresponding checkbox. To disable a threshold, deselect the checkbox.
   - After any threshold is enabled, type an appropriate numeric value in the accompanying text box.
6. To set the deassertion hysteresis, type a numeric value in the Deassertion Hysteresis field. See ***"To De-assert" and Deassertion Hysteresis*** (on page 672).
7. To set the assertion timeout, type a numeric value in the Assertion Timeout (samples) field. See ***"To Assert" and Assertion Timeout*** (on page 670).
8. Click OK in the threshold setup dialog to retain the changes.
9. To set the thresholds for other sensors, repeat Steps 4 to 8.
10. Click OK.

Important: The final step is required or the threshold changes are not saved.

Setting an Overcurrent Protector's Thresholds

Setting the overcurrent protector thresholds enables the PX to generate alerts when any overcurrent protector crosses the thresholds.

To set thresholds for an overcurrent protector:

1. Expand the Overcurrent Protectors folder in the PX Explorer pane if needed. See ***Expanding the Tree*** (on page 114).
2. In the PX Explorer pane, click the desired overcurrent protector. The page specific to that overcurrent protector opens in the right pane.

3. Click Setup. The Overcurrent Protector Setup dialog appears.
4. In the Threshold Configuration table, click the sensor whose thresholds you want to configure.
5. Click Edit or double-click the desired sensor. A threshold setup dialog appears.
6. Configure the Lower Critical, Lower Warning, Upper Warning and Upper Critical thresholds respectively.
   - To enable any threshold, select the corresponding checkbox. To disable a threshold, deselect the checkbox.
   - After any threshold is enabled, type an appropriate numeric value in the accompanying text box.
7. To set the deassertion hysteresis, type a numeric value in the Deassertion Hysteresis field. See ***"To De-assert" and Deassertion Hysteresis*** (on page 672).
8. To set the assertion timeout, type a numeric value in the Assertion Timeout (samples) field. See ***"To Assert" and Assertion Timeout*** (on page 670).
9. Click OK.

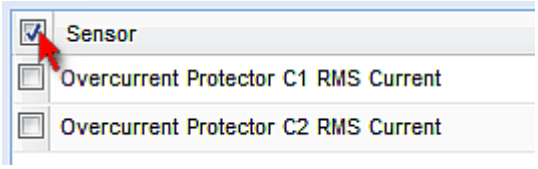
Bulk Configuration for Overcurrent Protector Thresholds

The PX allows you to set power thresholds for multiple overcurrent protectors at a time to save your time.

Note: To set the power thresholds for an individual overcurrent protector, you can either follow the instructions below or those described in the section **Setting an Overcurrent Protector's Thresholds** *(on page 232).*

To configure thresholds, deassertion hysteresis and assertion timeout for multiple overcurrent protectors:

1. Click the Overcurrent Protectors folder in the PX Explorer pane. The Overcurrent Protectors page opens.
2. Click Bulk Setup. The Overcurrent Protector Threshold Bulk Setup dialog appears, with a list of all overcurrent protectors.
3. Select desired overcurrent protectors by having their corresponding checkboxes selected.
   - To select all overcurrent protectors, select the checkbox labeled Sensor in the header row, and all checkboxes are selected.



- To select partial overcurrent protectors, click the corresponding checkboxes of those overcurrent protectors.
- To deselect any overcurrent protectors, just click their checkboxes once again.

4. Click Edit Thresholds. The threshold bulk setup dialog appears.
5. Configure the Lower Critical, Lower Warning, Upper Warning and Upper Critical thresholds respectively.
   - To enable any threshold, select the corresponding checkbox. To disable a threshold, deselect the checkbox.
   - After any threshold is enabled, type an appropriate numeric value in the accompanying text box.
6. To set the deassertion hysteresis, type a numeric value in the Deassertion Hysteresis field. See ***"To De-assert" and Deassertion Hysteresis*** (on page 672).
7. To set the assertion timeout, type a numeric value in the Assertion Timeout (samples) field. See ***"To Assert" and Assertion Timeout*** (on page 670).
8. Click OK.

Setting Thresholds for Total Active Energy or Power

This section applies only to multi-inlet models, including PX in-line monitors.

Thresholds for total active energy and total active power are disabled by default. You can enable and set them so that you are alerted when the total active energy or total active power hits a certain level.

For a regular PX model with multiple inlets:

- Total active energy = sum of all inlets' active energy values
- Total active power = sum of all inlets' active power values

For an in-line monitor with multiple inlets/outlets:

- Total active energy = sum of all outlets' active energy values
- Total active power = sum of all outlets' active power values

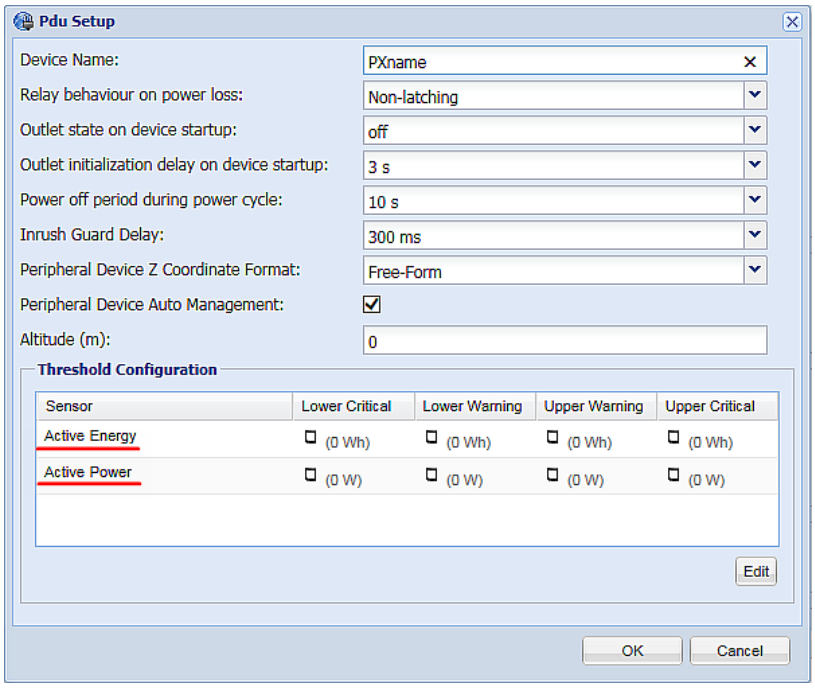
Tip: You can reset the active energy sensor(s) as needed. See **Resetting All Active Energy Readings** *(on page 165).*

To set thresholds for total active energy and/or power on a multi-inlet PX:

1. Click the PDU folder.

Note: The folder is named "my PX" by default. The name can be customized. See **Naming the PDU** *(on page 130).*

2. Click Setup in the Settings section. The Pdu Setup dialog appears.
3. In the Threshold Configuration table, click the sensor whose thresholds you want to configure.
4. Click Edit or double-click the desired sensor. A threshold setup dialog appears.
5. Configure the Lower Critical, Lower Warning, Upper Warning and Upper Critical thresholds respectively.
   - To enable any threshold, select the corresponding checkbox. To disable a threshold, deselect the checkbox.
   - After any threshold is enabled, type an appropriate numeric value in the accompanying text box.
6. To set the deassertion hysteresis, type a numeric value in the Deassertion Hysteresis field. See ***"To De-assert" and Deassertion Hysteresis*** (on page 672).
7. To set the assertion timeout, type a numeric value in the Assertion Timeout (samples) field. See ***"To Assert" and Assertion Timeout*** (on page 670).
8. Click OK.



Event Rules and Actions

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

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

- System Event Log Rule: This causes ANY event occurred to the PX to be recorded in the internal log. It is enabled by default.
- System SNMP Notification Rule: This causes SNMP traps or informs to be sent to specified IP addresses or hosts when ANY event occurs to the PX. It is disabled by default.
- System Tamper Detection Alarmed: This causes the PX to send alarm notifications if a DX tamper sensor has been connected and the PX detects that the tamper sensor enters the alarmed state.
- System Tamper Detection Unavailable: This causes the PX to sends alarm notifications if a DX tamper sensor has been connected and the PX detects that the communication with the connected tamper sensor is lost.

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

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

Components of an Event Rule

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

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

Creating an Event Rule

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

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

Creating Actions

The PX comes with three built-in actions:

- System Event Log Action: This action records the selected event in the internal log when the event occurs.
- System SNMP Notification Action: This action sends SNMP notifications to one or multiple IP addresses after the selected event occurs.
- System Tamper Alarm: This action causes the PX to show the alarm for the DX tamper sensor in the Alarms section of the Dashboard until a person acknowledges it. By default, this action has been assigned to the built-in tamper detection event rules. For information on acknowledging an alarm, see ***Alarms List*** (on page 123).

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

The built-in actions cannot be deleted.

To create new actions:

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

Action	Function
Execute an action group	Creates a group of actions comprising existing actions. See ***Action Group*** (on page 239).
Alarm	Requires the user to acknowledge the alert when it is generated. If needed, you can have the alert notifications regularly generated until a person takes the acknowledgment action. See ***Alarm*** (on page 240).
External beeper	Enables or disables the connected external beeper, or causes it to enter an alarm cycle. See ***External Beeper*** (on page 241).
Log event message	Records the selected events in the internal log. See ***Log an Event Message*** (on page 242).

Action	Function
Push out sensor readings	Sends asset management sensor data to a remote server using HTTP POST requests. See ***Push Out Sensor Readings*** (on page 243).
Request LHX/SHX maximum cooling	Applies the maximum cooling to the LHX/SHX device. See ***Request LHX/SHX Maximum Cooling*** (on page 244). This option is available only when the Schroff LHX/SHX support has been enabled.
Send snapshots via email	Emails the snapshots captured by a connected Logitech® webcam (if available). See ***Send a Snapshot via Email*** (on page 244).
Send email	Emails a textual message. See ***Send EMail*** (on page 245).
Send SNMP notification	Sends SNMP traps or informs to one or multiple SNMP destinations. See ***Send an SNMP Notification*** (on page 246).
Syslog message	Makes the PX automatically forward event messages to the specified syslog server. See ***Syslog Message*** (on page 249).
Send sensor report	Reports the readings or status of the selected sensors, including internal or external sensors. See ***Send Sensor Report*** (on page 250).
Send SMS message	Sends a message to a mobile phone. See ***Send SMS Message*** (on page 253).
Internal beeper	Turns on or off the internal beeper. See ***Internal Beeper*** (on page 254).
Switch LHX/SHX	Switches on or off the LHX/SHX device. See ***Switch LHX/SHX*** (on page 254). This option is available only when the Schroff LHX/SHX support has been enabled.
Record snapshots to webcam storage	Makes a connected webcam start or stop taking snapshots. See ***Record Snapshots to Webcam Storage*** (on page 256).
Change load shedding state	Enters or quits the load shedding mode. See ***Change Load Shedding State*** (on page 252).
Switch outlets	Switches on, off or cycles the power to the specified outlet(s). See ***Switch Outlets*** (on page 255).

Action	Function
Switch peripheral actuator	Switches on or off the mechanism or system connected to the specified actuator. See ***Switch Peripheral Actuator*** (on page 256).

Note: The "Change load shedding state" and "Switch outlets" options are only available for outlet-switching capable models.

6. Click OK to save the new action.

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

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

Action Group

You can create an action group that performs up to 32 actions. After creating such an action group, you can easily assign this set of actions to an event rule rather than selecting all needed actions one by one per rule.

To create an action group:

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

   To move all actions to the Used Actions list box, click . A maximum of 32 actions can be grouped.
7. To remove an action from the action group, select it from the Used Actions list box, and click to move it to the Available Actions list box. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.

To remove all actions, click .

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

Alarm

The Alarm is an action that requires users to acknowledge an alert. This helps ensure that the user is aware of the alert.

If the Alarm action has been included in a specific event rule and no one acknowledges that alert after it occurs, the PX resends or regenerates an alert notification regularly until the alert is acknowledged or it reaches the maximum number of alert notifications.

For information on acknowledging an alarm, see ***Alarms List*** (on page 123).

To create an Alarm action:

1. Click the Actions tab.
2. Click New.
3. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number starting at 1.
4. In the Action field, click the drop-down arrow and select the desired action: Alarm.
5. In the Alarm Notifications list box, specify one or multiple ways to issue the alert notifications.
   a. In the Available Actions field, select the method to send alert notifications. Available methods vary, depending on how many notification-based actions have been created.

      Notification-based action types include:

      - External beeper
      - Syslog message
      - Send email
      - Send SMS message
      - Internal beeper

      If no appropriate actions are available, click Create New Notification Action to immediately create them.

   b. Click to add the selected method to the Alarm Notifications list box.
   c. Repeat the above steps to add more methods if needed.

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

6. In the Notification Options section, configure the notification-resending or -regenerating feature.
   a. To enable the notification-resending feature, select the "Enable re-scheduling of alarm notifications" checkbox. To disable this feature, deselect the checkbox.
   b. In the "Period in Minutes" field, specify the time interval (in minutes) at which the alert notification is resent or regenerated regularly. You can either directly type a numeric value or click the Up/Down arrow keys to adjust the time.
   c. In the "Max. numbers" field, specify the maximum number of times the alert notification is resent. Values range from 1 to infinite.
7. If needed, you can instruct the PX to send the acknowledgment notification after the alarm is acknowledged in the Acknowledgment Notifications list box. **(Optional)**
   a. In the Available Actions field, select the method to send the acknowledge notification. Available methods are identical to those for generating alarm notifications.
   b. Click to add the selected method to the Acknowledgment Notifications list box.
   c. Repeat the above steps to add more methods if needed.
      - To remove any method from the Acknowledgment Notifications list box, select that method and click .
8. Click OK.

External Beeper

If an external beeper is connected to the PX, the PX can change the beeper's behavior or status to respond to a certain event.

To control the connected external beeper:

1. Click the Actions tab.
2. Click New.
3. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number starting at 1.
4. In the Action field, click the drop-down arrow and select the desired action: External beeper.

5. From the Beeper Port drop-down list, select the port where the external beeper is connected. This port is the FEATURE port.
6. From the Beeper Action drop-down list, select an action for the external beeper to carry out.
   - Alarm: Causes the external beeper to sound an alarm cycle every 20 seconds - stays on for 0.7 seconds and then off for 19.3 seconds.
   - On: Turns on the external beeper so that it buzzes continuously.
   - Off: Turns off the external beeper so that it stops buzzing.
7. Click OK.

Note: If you create an event rule for the external beeper but disconnect it when an event causes it to beep, the beeper no longer beeps after it is re-connected even though the event triggering the beeping action remains asserted.

Log an Event Message

This option records the selected events in the internal log.

To create a log event message:

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

Push Out Sensor Readings

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

Before creating this action, make sure that you have properly defined the destination servers and the sensor data type in the Data Push dialog. See ***Configuring Data Push Settings*** (on page 163).

Tip: To send the asset sensor data at a regular interval, schedule this action. See **Scheduling an Action** *(on page 262). Note that the "Asset management log" is generated only when there are changes made to any asset sensors or asset tags, such as connection or disconnection events.*

To push out the sensor data:

1. Choose Device Settings > Event Rules. The Event Rules Settings dialog opens.
2. Click the Actions tab.
3. Click New.
4. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number starting at 1.
5. In the Action field, click the drop-down arrow and select the desired action: Push out sensor readings.
6. Select a server or host which receives the asset sensor data in the Destination field.
   - If the desired destination is not available yet, go to the Data Push dialog to enter it. See ***Configuring Data Push Settings*** (on page 163).
7. Click OK.

Request LHX/SHX Maximum Cooling

If Schroff LHX/SHX Support is enabled, the LHX/SHX-related actions will be available. See ***Enabling and Disabling Schroff LHX/SHX Heat Exchanger Support*** (on page 335).

The "Request LHX/SHX Maximum Cooling" action applies the maximum cooling to the SHX-30 device only. The LHX-20 and LHX-40 devices do not support this feature.

In the maximum cooling mode, an SHX-30 device runs at 100% fan speed and the cold water valve is open 100%.

To request maximum cooling for SHX-30:

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

Send a Snapshot via Email

This option notifies one or multiple persons for the selected events by emailing snapshots or videos captured by a connected Logitech® webcam.

To create a send snapshot via email action:

1. Choose Device Settings > Event Rules. The Event Rules Settings dialog opens.
2. Click the Actions tab.
3. Click New.
4. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number starting at 1.
5. In the Action field, click the drop-down arrow and select the desired action: Send snapshots via email.
6. In the "Recipients email addresses" field, specify the email address(es) of the recipient(s). Use a comma to separate multiple email addresses.

7. To use the SMTP server specified in the SMTP Server Settings dialog, select the Use Default SMTP Server checkbox.

   To use a different SMTP server, select the Use Custom SMTP Settings checkbox.

   If the SMTP server settings are not configured yet, click Configure. See ***Configuring SMTP Settings*** (on page 162) for the information of each field.

8. Select the webcam that is capturing the images you want sent in the email.
9. Use the slide bars to increase or decrease the following:
   - Number of Snapshots - the number of snapshots to be included in the sequence of images that are taken when the event occurs. For example, you can specify 10 images be taken once the event triggers the action.
   - Snapshots/Mail field - the number of snapshots from the sequence to be sent at one time in the email.
   - "Time before first Snapshot (s):" - the amount of time (in seconds) between when the event is triggered and the webcam begins taking snapshots.
   - "Time between Snapshots (s):" - the amount of time between when each snapshot is taken.
10. Click OK.

Send EMail

You can configure emails to be sent when an event occurs and can customize the message.

Messages consist of a combination of free text and PX placeholders. The placeholders represent information is pulled from the PX and inserted into the message.

For example:

```
[USERNAME] logged into the device on [TIMESTAMP]
```

translates to

```
JQPublic logged into the device on 2012-January-30 21:00
```

See ***Email and SMS Message Placeholders*** (on page 277) for a list and definition of available variables.

To configure sending emails:

1. Choose Device Settings > Event Rules. The Event Rules Settings dialog opens.

2. Click the Actions tab.
3. Click New.
4. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number starting at 1.
5. In the Action field, click the drop-down arrow and select the desired action: Send email.
6. In the "Recipients email addresses" field, specify the email address(es) of the recipient(s). Use a comma to separate multiple email addresses.
7. To use the SMTP server specified in the SMTP Server Settings dialog, select the Use Default SMTP Server checkbox.

   To use a different SMTP server, select the Use Custom SMTP Settings checkbox.

   If the SMTP server settings are not configured yet, click Configure. See ***Configuring SMTP Settings*** (on page 162) for the information of each field. Default messages are sent based on the event. See ***Default Log Messages*** (on page 267) for a list of default log messages and events that trigger them.
8. If needed, select the Use Custom Log Message checkbox, and then create a custom message up to 1024 characters in the provided field.
   - To start a new line in the text box, press Enter.
   - Click the Information icon to open the Event Context Information dialog, which contains a list of placeholders and their definitions. See ***Email and SMS Message Placeholders*** (on page 277) for more details.
9. Click OK.

Send an SNMP Notification

This option sends an SNMP notification to one or multiple SNMP destinations.

To configure sending an SNMP notification:

1. Choose Device Settings > Event Rules. The Event Rules Settings dialog opens.
2. Click the Actions tab.
3. Click New.

4. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number starting at 1.
5. In the Action field, click the drop-down arrow and select the desired action: Send SNMP notification.
6. Select the type of SNMP notification. See either procedure below according to your selection.

To send SNMP v2c notifications:

1. From the Notification Type drop-down, select SNMPv2c Trap or SNMPv2c Inform.
2. For SNMP INFORM communications, leave the resend settings at their default or:
   a. In the Timeout (sec) field, enter the interval of time, in seconds, after which a new inform communication is resent if the first is not received. For example, resend a new inform communication once every 3 seconds.
   b. In the Number of Retries field, enter the number of times you want to resend the inform communication if it fails. For example, inform communications are resent up to 5 times when the initial communication fails.
3. In the Host fields, enter the IP address of the device(s) you want to access. This is the address to which notifications are sent by the SNMP system agent.
4. In the Port fields, enter the port number used to access the device(s).
5. In the Community fields, enter the SNMP community string to access the device(s). The community is the group representing the PX and all SNMP management stations.

Tip: An SNMP v2c notification action only permits entering a maximum of three SNMP destinations. To assign more than three SNMP destinations to a specific rule, first create several SNMP v2c notification actions, each of which contains completely different SNMP destinations, and then add all of these SNMP v2c notification actions to the same rule.

To send SNMP v3 notifications:

1. From the Notification Type drop-down, select SNMPv3 Trap or SNMPv3 Inform.
2. For SNMP TRAPs, the engine ID is prepopulated.
3. For SNMP INFORM communications, leave the resend settings at their default or:

a. In the Timeout (sec) field, enter the interval of time, in seconds, after which a new inform communication is resent if the first is not received. For example, resend a new inform communication once every 3 seconds.

b. In the Number of Retries field, enter the number of times you want to resend the inform communication if it fails. For example, inform communications are resent up to 5 times when the initial communication fails.

4. For both SNMP TRAPS and INFORMS, enter the following as needed and then click OK to apply the settings:

   a. Host name

   b. Port number

   c. User ID needed to access the host

   d. Select the host security level

Security level	Description
"noAuthNoPriv"	Select this if no authorization or privacy protocols are needed.
"authNoPriv"	Select this if authorization is required but no privacy protocols are required. • Select the authentication protocol - MD5 or SHA • Enter the authentication passphrase and then confirm the authentication passphrase
"authPriv"	Select this if authentication and privacy protocols are required. • Select the authentication protocol - MD5 or SHA • Enter the authentication passphrase and confirm the authentication passphrase • Select the Privacy Protocol - DES or AES • Enter the privacy passphrase and then confirm the privacy passphrase

Syslog Message

Use this action to automatically forward event messages to the specified syslog server. Determine the syslog transmission mechanism you prefer when setting it up - UDP, TCP or TLS over TCP.

The PX may or may not detect the syslog message transmission failure. If yes, it will log this syslog failure as well as the failure reason in the event log. See ***Viewing the Local Event Log*** (on page 288).

To configure a syslog message action:

1. Choose Device Settings > Event Rules. The Event Rules Settings dialog opens.
2. Click the Actions tab.
3. Click New.
4. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number starting at 1.
5. In the Action field, click the drop-down arrow and select the desired action: Syslog message.
6. In the "Syslog server" field, specify the IP address to which the syslog is forwarded.
7. In the Transport Protocol field, select one of the syslog protocols: TCP or UDP. The default is UDP.

Transport protocol types	Next steps
UDP	▪ In the UDP Port field, specify an appropriate port number. Default is 514. ▪ Select the "Legacy BSD Syslog Protocol (UDP only)" checkbox if applicable.
TCP	If NO TLS certificate is required, type an appropriate port number in the TCP Port field.

Transport protocol types	Next steps
	If a TLS certificate is required, select the "Enable Secure Syslog over TLS" checkbox, and then do the following: a. Specify an appropriate port number in the "TCP Port (TLS)" field. Default is 6514. b. In the CA Certificate field, click Browse to select a TLS certificate. After installing the certificate, you may: ▪ Click Show to view its contents. ▪ Click Remove to delete it if it is inappropriate. c. Determine whether to select the "Allow expired and not yet valid certificates" checkbox. ▪ To always send the event message to the specified syslog server after a TLS certificate has been installed, select this checkbox. ▪ To prevent the event message from being sent to the specified syslog server when any TLS certificate in the selected certificate chain is outdated or not valid yet, deselect this checkbox.

8. Click OK.

Send Sensor Report

You may set the PX so that it automatically reports the latest readings or states of one or multiple sensors by sending a message or email or simply recording the report in a log. These sensors can be either internal or environmental sensors as listed below.

- Inlet sensors, including RMS current, RMS voltage, active power, apparent power, power factor and active energy.
- Outlet sensors, including RMS current, RMS voltage, active power, apparent power, power factor, active energy and outlet state (for outlet-switching capable PDUs only).
- Overcurrent protector sensors, including RMS current and tripping state.
- Peripheral device sensors, which can be any Raritan environmental sensor packages connected to the PX, such as temperature or humidity sensors.

To configure a sensor report action:

1. Choose Device Settings > Event Rules. The Event Rules Settings dialog opens.
2. Click the Actions tab.
3. Click New.

4. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number starting at 1.
5. In the Action field, click the drop-down arrow and select the desired action: Send sensor report.
6. In the Destination Actions field, select the method(s) to report sensor readings or states. The number of available methods varies, depending on how many messaging actions have been created.

   The messaging action types include:

   - Log event message
   - Syslog message
   - Send email
   - Send SMS message

   a. If no messaging actions are available, click Create New Destination Action to immediately create them.

   b. To select any method, select it in the right list box, and click to move it to the left list box. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.

   To select all methods, simply click .

   c. To delete any method, select it in the left list box, and click to move it back to the right list box. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.

   To remove all methods, simply click .
7. In the Available Sensors field, select the desired sensor.

   a. Select the sensor type from the field to the left.

   b. Select the specific sensor from the field to the right.

   c. Click to add the selected sensor to the Report Sensors list box.

   For example, to monitor the current reading of the Inlet 1, select Inlet 1 from the left field, and then select RMS Current from the right field.
8. To report additional sensors simultaneously, repeat the above step to add more sensors.

   - To remove any sensor from the Report Sensors list box, select it and click . To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.
9. To immediately send out the sensor report, click Send Report Now. A message appears, indicating whether the sensor report is sent successfully.
10. To save this action, click OK.

Note: When intending to send a sensor report using custom messages, use the placeholder [SENSORREPORT] to report sensor readings. See **Email and SMS Message Placeholders** *(on page 277).*

Change Load Shedding State

The "Change load shedding state" action is available only when your PX is able to control outlet power. Use this action to activate or deactivate the load shedding mode for responding to a specific event. See ***Setting Non-Critical Outlets and Load Shedding Mode*** (on page 220) for additional information.

To change the load shedding state:

1. Click the Actions tab.
2. Click New.
3. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number starting at 1.
4. In the Action field, click the drop-down arrow and select the desired action: Change load shedding state.
5. From the Operation drop-down, select either of the following:
   - 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.
6. Click OK to save the new action.
7. Click Close to quit the dialog.

Send SMS Message

You can configure emails to be sent when an event occurs and can customize the message.

Messages consist of a combination of free text and PX placeholders. The placeholders represent information which is pulled from the PX and inserted into the message.

A supported modem, such as the Cinterion® GSM MC52i modem, must be plugged in to the PX in order to send SMS messages.

Note: The PX cannot receive SMS messages.

For example:

```
[USERNAME] logged into the device on [TIMESTAMP]
```

translates to

```
JQPublic logged into the device on 2012-January-30 21:00
```

See ***Email and SMS Message Placeholders*** (on page 277) for a list and definition of available variables.

To configure SMS message:

1. Choose Device Settings > Event Rules. The Event Rules Settings dialog opens.
2. Click the Actions tab.
3. Click New.
4. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number starting at 1.
5. In the Action field, click the drop-down arrow and select the desired action: Send SMS message.
6. In the Recipient Phone Number field, specify the phone number of the recipient.
7. Select the Use Custom Log Message checkbox, then create a custom message in the provided field.

   Click the Information icon to open the Event Context Information dialog, which contains a list of placeholders and their definitions. See ***Email and SMS Message Placeholders*** (on page 277) for more details.

   Note: Only the 7-bit ASCII charset is supported for SMS messages.
8. Click OK.

Internal Beeper

You can have the built-in beeper of the PX turned on or off when a certain event occurs.

To switch the internal beeper:

1. Click the Actions tab.
2. Click New.
3. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number starting at 1.
4. In the Action field, click the drop-down arrow and select the desired action: Internal beeper.
5. Select an option from the Operation field.
   - Turn Beeper On: Turns on the internal beeper to make it buzz.
   - Turn Beeper Off: Turns off the internal beeper to make it stop buzzing.
6. Click OK.

Switch LHX/SHX

If Schroff LHX/SHX Support is enabled, the LHX/SHX-related actions will be available. See ***Enabling and Disabling Schroff LHX/SHX Heat Exchanger Support*** (on page 335).

Use this action to switch the LHX/SHX on or off when, for example, temperature thresholds are reached.

To create a switch LHX/SHX action:

1. Choose Device Settings > Event Rules. The Event Rules Settings dialog opens.
2. Click the Actions tab.
3. Click New.
4. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number starting at 1.
5. In the Action field, click the drop-down arrow and select the desired action: Switch LHX/SHX.
6. From the Operation drop-down, select Turn LHX/SHX On or Turn LHX/SHX Off.

7. From the Available LHX/SHXs list box, click on the LHX/SHX to be turned on or off, then click or to add to the Switched LHX/SHXs list box. Use or to remove the LHX/SHX from the Switched LHXs list box, thereby removing the action.
8. Click OK.

Switch Outlets

The "Switch outlets" action is available only when your PX is outlet-switching capable. This action turns on, off or power cycles a specific outlet.

To switch on, off or power cycle any outlet(s):

1. Click the Actions tab.
2. Click New.
3. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number starting at 1.
4. In the Action field, click the drop-down arrow and select the desired action: Switch outlets.
5. From the Operation drop-down list, 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).
6. To select the outlet where this action will be applied, select it from the Available Outlets list box and click to move it to the Switched Outlets list box. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.

   To move all outlets to the Switched Outlets list box, click .
7. To remove any outlet from the Switched Outlets list, select it from the Switched Outlets list box and click to move it to the Available Outlets list box. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.

   To remove all outlets, click .
8. Click OK to save the new action.
9. Click Close to quit the dialog.

Switch Peripheral Actuator

If you have any actuator connected to the PX, you can set up the PX so it automatically turns on or off the system controlled by this actuator when a specific event occurs.

Note: For information on connecting actuators to the PX, see **DX Sensor Packages** *(on page 45).*

To switch on or off the system connected to an actuator:

1. Click the Actions tab.
2. Click New.
3. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number starting at 1.
4. In the Action field, click the drop-down arrow and select the desired action: Switch peripheral actuator.
5. From the Operation drop-down list, select an operation for the selected actuator.
   - Turn On: Turns on the selected actuator.
   - Turn Off: Turns off the selected actuator.
6. To select the actuator where this action will be applied, select it from the Available Actuators list and click to add it to the Switched Actuators list box. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.

   To add all actuators to the Switched Actuators list box, click .
7. To remove any actuator from the Switched Actuators list, select it and click to move it back to the Available Actuators list box. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.

   To remove all actuators, click .
8. Click OK.

Record Snapshots to Webcam Storage

This option allows you to define an action that starts or stops a specific webcam from taking snapshots.

To configure a record snapshot to webcam storage action:

1. Choose Device Settings > Event Rules. The Event Rules Settings dialog opens.

2. Click the Actions tab.
3. Click New.
4. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number starting at 1.
5. In the Action field, click the drop-down arrow and select the desired action: Record snapshots to webcam storage.
6. Select a webcam from the Webcam drop-down.
7. Selecting the action to perform - Start recording or Stop recording. If "Start recording" is selected, do the following:
   a. Use the slide bar to specify the total number of snapshots to be taken when the event occurs. The maximum amount of snapshots that can be stored on the PX is ten (10). If you set it for a number greater than ten and the storage location is on the PX, after the tenth snapshot is taken and stored, the oldest snapshots are overwritten.

   Tip: By default, the storage location is on the PX. You can specify a remote server to store the snapshots. See **Configuring Webcam Storage** *(on page 331).*

   b. In the "Time before first Snapshot (s):" field, use the slide bar to specify the amount of time (in seconds) between when the event is triggered and the webcam begins taking snapshots.
   c. In the "Time between Snapshots (s):" field, use the slide bar to specify the amount of time between each snapshot being taken.
8. Click OK.

Creating Rules

After required actions are available, you can create event rules to determine what actions are taken to respond to specific events.

By default, the PX provides the following built-in event rules:

- System Event Log Rule
- System SNMP Notification Rule
- System Tamper Detection Alarmed
- System Tamper Detection Unavailable

If the built-in rules do not satisfy your needs, create new ones.

To create event rules:

1. Choose Device Settings > Event Rules. The Event Rule Settings dialog appears.

2. On the Rules tab, click New.
3. In the "Rule name" field, type a new name for identifying the rule. The default name is New Rule <number>, where <number> is a sequential number.
4. Select the Enabled checkbox to activate this event rule.
5. Click Event to select an event for which you want to trigger an action. A pull-down menu showing various types of events appears.
   - Select the desired event type from the pull-down menu, and if a submenu appears, continue the navigation until the desired event is selected.

   Note: To select all items or events listed on the same submenu, select the option enclosed in brackets, such as <Any sub-event>, <Any Server> and <Any user>.
6. According to the event you selected in the previous step, the "Trigger condition" field containing three radio buttons may or may not appear.

Event types	Radio buttons
Numeric sensor threshold-crossing events, or the occurrence of the selected event -- true or false	Available radio buttons include "Asserted," "Deasserted" and "Both." ▪ Asserted: The PX takes the action only when the event occurs. This means the status of the described event transits from FALSE to TRUE. ▪ Deasserted: The PX takes the action only when the event condition disappears. This means the status of the described event transits from TRUE to FALSE. ▪ Both: The PX takes the action both when the event occurs (asserts) and when the event condition disappears (deasserts).
Discrete (on/off) sensor state change	Available radio buttons include "Alarmed/Open/On," "No longer alarmed/Closed/Off" and "Both." ▪ Alarmed/Open/On: The PX takes the action only when the chosen sensor enters the alarmed, open or on state. ▪ No longer alarmed/Closed/Off: The PX takes the action only when the chosen sensor returns to the normal, closed or off state. ▪ Both: The PX takes the action whenever the chosen sensor switches its state.

Event types	Radio buttons
Sensor availability	Available radio buttons include "Unavailable," "Available" and "Both." ▪ Unavailable: The PX takes the action only when the chosen sensor is NOT detected and becomes unavailable. ▪ Available: The PX takes the action only when the chosen sensor is detected and becomes available. ▪ Both: The PX takes the action both when the chosen sensor becomes unavailable or available.
Network interface link state	Available radio buttons include "Link state is up," "Link state is down" and "Both." ▪ Link state is up: The PX takes the action only when the network link state changes from down to up. ▪ Link state is down: The PX takes the action only when the network link state changes from up to down. ▪ Both: The PX takes the action whenever the network link state changes.
Function enabled or disabled	Available radio buttons include "Enabled," "Disabled" and "Both." ▪ Enabled: The PX takes the action only when the chosen function is enabled. ▪ Disabled: The PX takes the action only when the chosen function is disabled. ▪ Both: The PX takes the action when the chosen function is either enabled or disabled.
User logon state	Available radio buttons include "Logged in," "Logged out," and "Both." ▪ Logged in: The PX takes the action only when the selected user logs in. ▪ Logged out: The PX takes the action only when the selected user logs out. ▪ Both: The PX takes the action both when the selected user logs in and logs out.

Event types	Radio buttons
Restricted service agreement	Available radio buttons include "Accepted," "Declined," and "Both." ▪ Accepted: The PX takes the action only when the specified user accepts the restricted service agreement. ▪ Declined: The PX takes the action only when the specified user rejects the restricted service agreement. ▪ Both: The PX takes the action both when the specified user accepts or rejects the restricted service agreement
Server monitoring event	Available radio buttons include "Monitoring started," "Monitoring stopped," and "Both." ▪ Monitoring started: The PX takes the action only when the monitoring of any specified server starts. ▪ Monitoring stopped: The PX takes the action only when the monitoring of any specified server stops. ▪ Both: The PX takes the action when the monitoring of any specified server starts or stops.
Server reachability	Available radio buttons include "Unreachable," "Reachable," and "Both." ▪ Unreachable: The PX takes the action only when any specified server becomes inaccessible. ▪ Reachable: The PX takes the action only when any specified server becomes accessible. ▪ Both: The PX takes the action when any specified server becomes either inaccessible or accessible.

Event types	Radio buttons
Device connection or disconnection, such as a USB-cascaded slave device	Available radio buttons include "Connected," "Disconnected" and "Both." ▪ Connected: The PX takes the action only when the selected device is physically connected to it. ▪ Disconnected: The PX takes the action only when the selected device is physically disconnected from it. ▪ Both: The PX takes the action both when the selected device is physically connected to it and when it is disconnected.
Outlet power state change	Available radio buttons include "On," "Off" and "Both." ▪ On: The PX takes the action only when the chosen outlet is turned ON. ▪ Off: The PX takes the action only when the chosen outlet is turned OFF. ▪ Both: The PX takes the action when the chosen outlet is either turned ON or OFF.
PDU load shedding	Available radio buttons include "Started," "Stopped" and "Both." ▪ Started: The PX takes the action only when activating the load shedding mode. ▪ Stopped: The PX takes the action only when deactivating the load shedding mode. ▪ Both: The PX takes the action whenever the load shedding mode is activated or deactivated.

Note: The outlet power state change and PDU load shedding events are available only for outlet-switching capable models.

7. In the Actions field, select the desired action from the "Available actions" list box, and click to move it to the "Selected actions" list box. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.
   - To add all actions, simply click .
   - If the desired action is not available yet, click Create New Action to immediately create it. Upon complete, the newly-created action is moved to the "Selected actions" list box.

8. To remove any action, select it from the "Selected actions" list box, and click to move it back to the "Available actions" list box. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.
   - To remove all actions, click .
9. Click OK to save the new event rule.

   Note: If you do not click OK before quitting the current settings page, a message appears. Then click Yes to save the changes, Discard to abort or Cancel to return to the current settings page.
10. Repeat Steps 2 to 10 to create additional event rules.
11. Click Close to quit the dialog.

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 PX report the reading or state of a specific environmental sensor regularly by scheduling the "Send Sensor Report" action.

When scheduling an action, make sure you have a minimum of 1-minute buffer time between this action's execution time and creation time. Otherwise, the scheduled action will NOT be performed at the specified time if the buffer time is too short. For example, if you want an action to be performed at 11:00 am, you should finish scheduling this action at 10:59 am or earlier.

To schedule any action(s):

1. Choose Device Settings > Event Rules. The Event Rule Settings dialog appears.
2. Click the Scheduled Actions tab.
3. Click New.
4. In the "Timer name" field, type a name for this scheduled action. The default name is New Timer <n>, where <n> is the sequential number starting at 1.
5. Make sure the Enabled checkbox is selected, or the PX will not carry out this scheduled action.
6. Select the desired time frequency from the Execution Time field and then specify the time interval or a specific date and time in the Time field.

Time options	Frequency settings
Minutes	The frequency in minutes ranges from every minute, every 5 minutes, every 10 minutes and so on until every 30 minutes.
Hourly	The hourly option sets the timing to either of the following: ▪ The Minute field is set to 0 (zero). Then the action is performed at 1:00 am, 2:00 am, 3:00 am and so on. ▪ The Minute field is set to a non-zero value. For example, if it is set to 30, then the action is performed at 1:30 am, 2:30 am, 3:30 am and so on.
Daily	You need to specify the time for this daily option. For example, if you specify 13:30 in the Time field, the action is performed at 13:30 pm every day.
Weekly	Both the day and time must be specified for the weekly option. Days range from Sunday to Monday.
Monthly	Both the date and time must be specified for the monthly option. The dates range from 1 to 31, and the time is specified in 24-hour format. Note that NOT every month has the date 31, and February in particular does not have the date 30 and probably even 29. Check the calendar when selecting 29, 30 or 31.
Yearly	This option requires three settings: ▪ Month - January through December. ▪ Date - 1 to 31. ▪ Time - the value is specified in 24-hour format.

7. In the Actions field, select the desired action from the "Available actions" list box, and click to move it to the "Selected actions" list box. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.

   - To add all actions, simply click .
   - If the desired action is not available yet, click Create New Action to immediately create it. Upon complete, the newly-created action is moved to the "Selected actions" list box. See ***Creating Actions*** (on page 237).

     When creating new actions from the Scheduled Actions tab, available actions are less than usual because it is meaningless to schedule certain actions like "Alarm," "Log event message," "Send email," "Syslog message" and the like.

8. To remove any action, select it from the "Selected actions" list box, and click to move it back to the "Available actions" list box. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.

- To remove all actions, click .

9. Click OK.

Send Sensor Report Example

Below is an example of a scheduled action set to send a temperature sensor report via email hourly.

In this example,

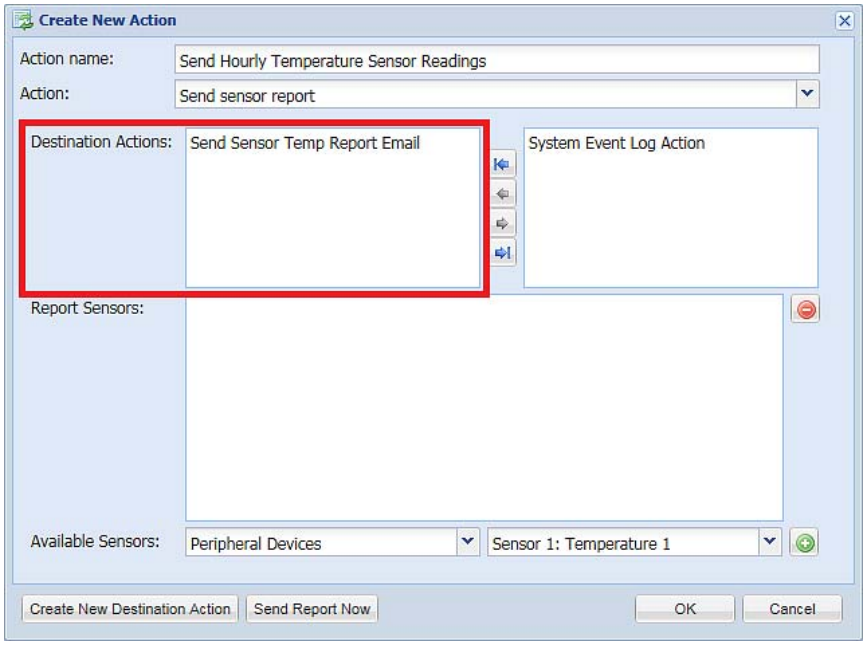
a. Define a 'Send email' destination action that is name *Send Sensor Temp Report Email*.
   - This destination action sends an email to the specified recipient(s).

b. Define a 'Send sensor report' action that is named *Send Hourly Temperature Sensor Readings*.
   - This action reports temperature sensor readings via the selected destination action -- Send Sensor Temp Report Email.

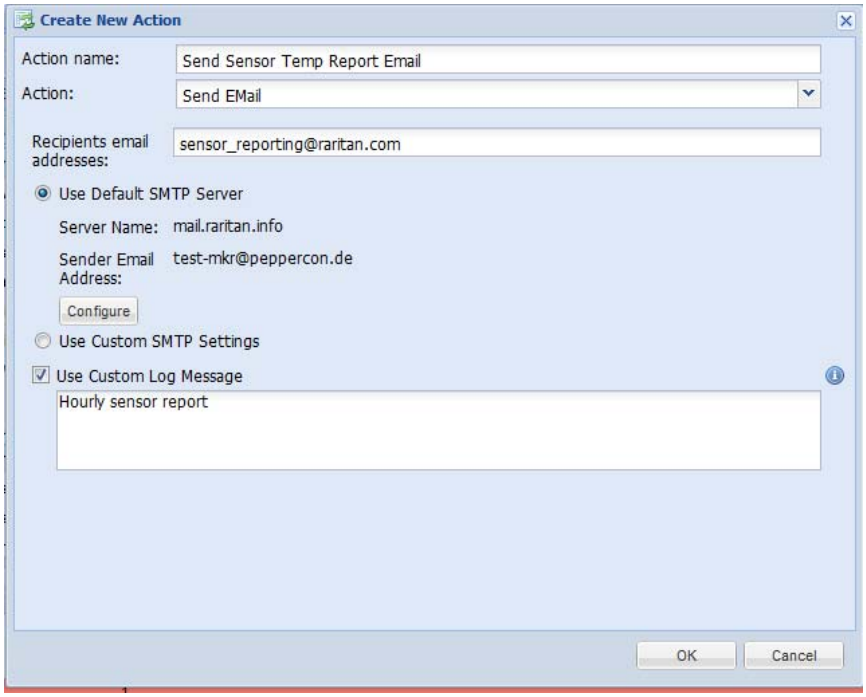
c. Define a timer that is named *Hourly Sensor Temperature Readings*.
   - This timer determines that the 'Send Hourly Temperature Sensor Readings' action shall take place on an hourly basis.

Detailed steps:

1. If you have not already done so, create the destination action 'Send Sensor Temp Report Email', which is performed when the 'Send Hourly Temperature Sensor Readings' action occurs.

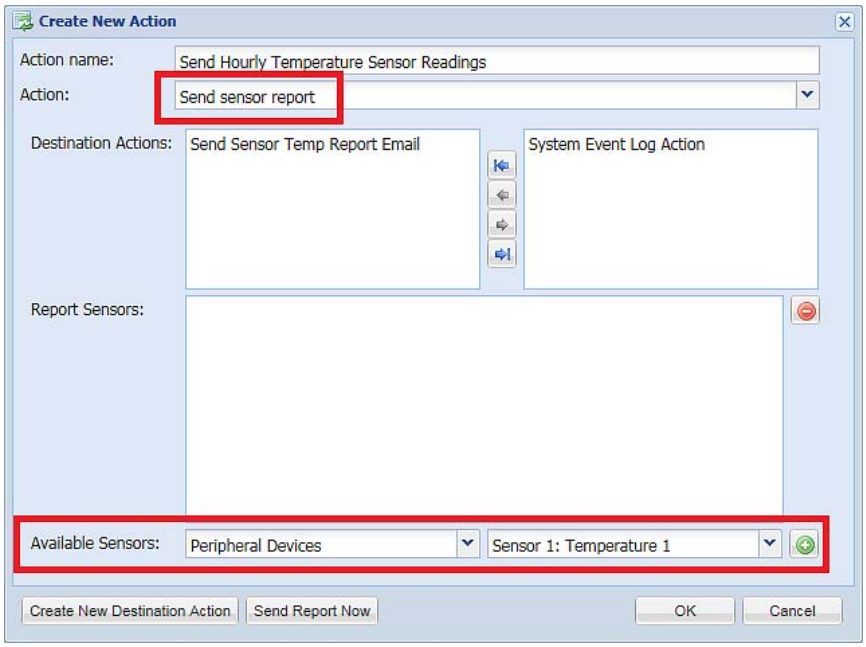


- You must create the destination action as illustrated below prior to creating the 'Send Hourly Temperature Sensor Readings' action. For details, see ***Send EMail*** (on page 245).



2. Create the 'Send sensor report' action -- *Send Hourly Temperature Sensor Readings*.
   a. Choose Device Settings > Event Rules. The Event Rule Settings dialog appears.
   b. Click the Actions tab > New.
   c. Enter the following information.

- Type the action's name -- *Send Hourly Temperature Sensor Readings*.
- Select the 'Send sensor report' action.
- Select the destination action 'Send Sensor Temp Report Email'.
- Add the desired temperature sensor(s) from the Available Sensors list to the Report Sensors box.



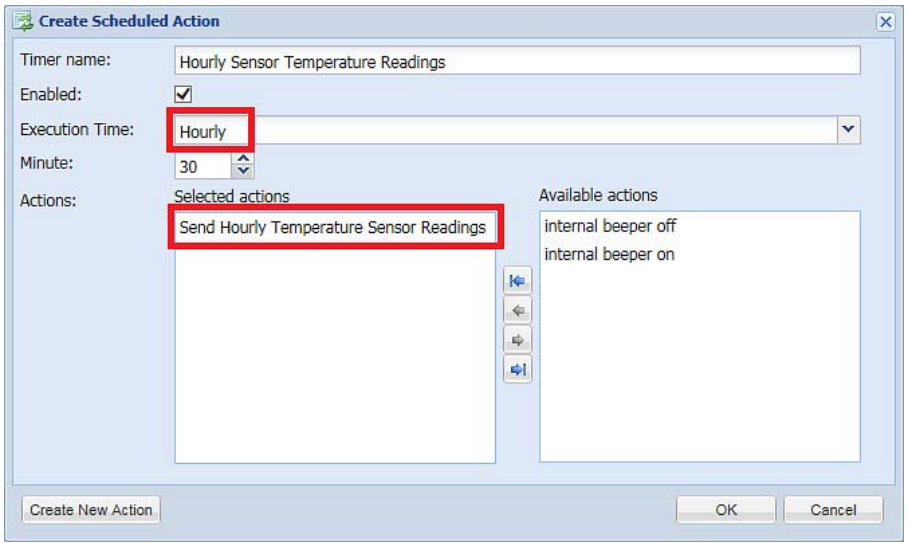
d. Click OK. For details, see ***Send Sensor Report*** (on page 250).

3. Create a timer for this newly-created action in the same Event Rule Settings dialog.

   a. Click the Scheduled Actions tab > New.

   b. Enter the following information.

- Type the timer name -- *Hourly Sensor Temperature Readings.*
- Select the Enabled checkbox.
- Select Hourly, and set the Minute to 30.
- Select the 'Send Hourly Temperature Sensor Readings' action.



c. Click OK. For details, see ***Scheduling an Action*** (on page 262).

Then the PX will regularly send out an email containing the specified temperature sensor readings at 0:30 am, 1:30 am, 2:30 am, 3:30 am, 4:30 am, and so on until 23:30 pm every day.

Default Log Messages

Following are default log messages triggered and emailed to specified recipients when PX events occur (are TRUE) or, in some cases, do not occur (are FALSE). See ***Send EMail*** (on page 245) for information configuring email messages to be sent when specified events occur.

Event/Context	Default Assertion Message when the Event = TRUE	Default Assertion Message when the Event = FALSE*
Asset Management > State	State of asset strip [STRIPID] ('[STRIPNAME]') changed to '[STATE]'.	
Asset Management > Rack Unit > * > Tag Connected	Asset tag with ID '[TAGID]' connected at rack unit [RACKUNIT], slot [RACKSLOT] of asset strip [STRIPID] ('[STRIPNAME]').	Asset tag with ID '[TAGID]' disconnected at rack unit [RACKUNIT], slot [RACKSLOT] of asset strip [STRIPID] ('[STRIPNAME]').

Event/Context	Default Assertion Message when the Event = TRUE	Default Assertion Message when the Event = FALSE*
Asset Management > Rack Unit > * > Blade Extension Connected	Blade extension with ID '[TAGID]' connected at rack unit [RACKUNIT] of asset strip [STRIPID] ('[STRIPNAME]').	Blade extension with ID '[TAGID]' disconnected at rack unit [RACKUNIT] of asset strip [STRIPID] ('[STRIPNAME]').
Asset Management > Firmware Update	Firmware update for asset strip [STRIPID] ('[STRIPNAME]'): status changed to '[STATE]'.	
Asset Management > Device Config Changed	Config parameter '[PARAMETER]' of asset strip [STRIPID] ('[STRIPNAME]') changed to '[VALUE]' by user '[USERNAME]'.	
Asset Management > Rack Unit Config Changed	Config of rack unit [RACKUNIT] of asset strip [STRIPID] ('[STRIPNAME]') changed by user '[USERNAME]' to: LED Operation Mode '[LEDOPMODE]', LED Color '[LEDCOLOR]', LED Mode '[LEDMODE]'	
Asset Management > Blade Extension Overflow	Blade extension overflow occurred on strip [STRIPID] ('[STRIPNAME]').	Blade extension overflow cleared for strip [STRIPID] ('[STRIPNAME]').
Asset Management > Composite Asset Strip Composition Changed	Composition changed on composite asset strip [STRIPID] ('[STRIPNAME]').	
Card Reader Management > Card inserted	Card Reader with id '[CARDREADERID]' connected.	
Card Reader Management > Card Reader attached	Card Reader with id '[CARDREADERID]' disconnected.	
Card Reader Management > Card Reader detached	Card of type '[SMARTCARDTYPE]' with ID '[SMARTCARDID]' inserted.	
Card Reader Management > Card removed	Card of type '[SMARTCARDTYPE]' with ID '[SMARTCARDID]' removed.	
Device > System started	System started.	
Device > System reset	System reset performed by user '[USERNAME]' from host '[USERIP]'.	
Device > Firmware validation failed	Firmware validation failed by user '[USERNAME]' from host '[USERIP]'.	

Event/Context	Default Assertion Message when the Event = TRUE	Default Assertion Message when the Event = FALSE*
Device > Firmware update started	Firmware upgrade started from version '[OLDVERSION]' to version '[VERSION]' by user '[USERNAME]' from host '[USERIP]'.	
Device > Firmware update completed	Firmware upgraded successfully from version '[OLDVERSION]' to version '[VERSION]' by user '[USERNAME]' from host '[USERIP]'.	
Device > Firmware update failed	Firmware upgrade failed from version '[OLDVERSION]' to version '[VERSION]' by user '[USERNAME]' from host '[USERIP]'.	
Device > Device identification changed	Config parameter '[PARAMETER]' changed to '[VALUE]' by user '[USERNAME]' from host '[USERIP]'.	
Device > Device settings saved	Device settings saved from host '[USERIP]'	
Device > Device settings restored	Device settings restored from host '[USERIP]'.	
Device > Data push failed	Data push to URL [DATAPUSH_URL] failed. [ERRORDESC].	
Device > Event log cleared	Event log cleared by user '[USERNAME]' from host '[USERIP]'.	
Device > Bulk configuration saved	Bulk configuration saved from host '[USERIP]'.	
Device > Bulk configuration copied	Bulk configuration copied from host '[USERIP]'.	
Device > Network interface link state is up	The [IFNAME] network interface link is now up.	The [IFNAME] network interface link is now down.
Device > Peripheral Device Firmware Update	Firmware update for peripheral device [EXTSENSORSERIAL] from [OLDVERSION] to [VERSION] [SENSORSTATENAME].	
Device > Sending SMTP message failed	Sending SMTP message to '[RECIPIENTS]' using server '[SERVER]' failed.	
Device > Sending SNMP inform failed or no response	Sending SNMP inform to manager [SNMPMANAGER]:[SNMPMANAGERPORT] failed or no response. [ERRORDESC].	

Event/Context	Default Assertion Message when the Event = TRUE	Default Assertion Message when the Event = FALSE*
Device > Sending Syslog message failed	Sending Syslog message to server [SYSLOGSERVER]:[SYSLOGPORT] ([SYSLOGTRANSPORTPROTO]) failed. [ERRORDESC].	
Device > Sending SMS message failed	Sending SMS message to '[PHONENUMBER]' failed.	
Device > An LDAP error occurred	An LDAP error occurred: [LDAPERRORDESC].	
Device > An Radius error occurred	An Radius error occurred: [RADIUSERRORDESC].	
Device > Unknown peripheral device attached	An unknown peripheral device with rom code '[ROMCODE]' was attached at position '[PERIPHDEVPOSITION]'.	
Device > USB slave connected	USB slave connected.	USB slave disconnected.
Device > WLAN authentication over TLS with incorrect system clock	Established connection to wireless network '[SSID]' via Access Point with BSSID '[BSSID]' using '[AUTHPROTO]' authentication with incorrrect system clock.	
Device > Features > Schroff LHX / SHX Support	Schroff LHX / SHX support enabled.	Schroff LHX / SHX support disabled.
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	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' asserted 'above upper critical' at [READING].	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' deasserted 'above upper critical' at [READING].
Peripheral Device Slot > * > Numeric Sensor > Above upper warning	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' asserted 'above upper warning' at [READING].	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' deasserted 'above upper warning' at [READING].

Event/Context	Default Assertion Message when the Event = TRUE	Default Assertion Message when the Event = FALSE*
Peripheral Device Slot > * > Numeric Sensor > Below lower warning	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' asserted 'below lower warning' at [READING].	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' deasserted 'below lower warning' at [READING].
Peripheral Device Slot > * > Numeric Sensor > Below lower critical	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' asserted 'below lower critical' at [READING].	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' deasserted 'below lower critical' at [READING].
Peripheral Device Slot > * > State Sensor > Unavailable	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' unavailable.	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' available.
Peripheral Device Slot > * > State Sensor > Alarmed / Open / On	Peripheral device '[EXTSENSORNAME]' in slot [EXTSENSORSLOT] is [SENSORSTATENAME].	Peripheral device '[EXTSENSORNAME]' in slot [EXTSENSORSLOT] is [SENSORSTATENAME].
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	Sensor '[INLETSENSOR]' on inlet '[INLET]' asserted 'above upper critical'.	Sensor '[INLETSENSOR]' on inlet '[INLET]' deasserted 'above upper critical'.
Inlet > * > Sensor > * > Above upper warning	Sensor '[INLETSENSOR]' on inlet '[INLET]' asserted 'above upper warning'.	Sensor '[INLETSENSOR]' on inlet '[INLET]' deasserted 'above upper warning'.
Inlet > * > Sensor > * > Below lower warning	Sensor '[INLETSENSOR]' on inlet '[INLET]' asserted 'below lower warning'.	Sensor '[INLETSENSOR]' on inlet '[INLET]' deasserted 'below lower warning'.
Inlet > * > Sensor > * > Below lower critical	Sensor '[INLETSENSOR]' on inlet '[INLET]' asserted 'below lower critical'.	Sensor '[INLETSENSOR]' on inlet '[INLET]' deasserted 'below lower critical'.
Inlet > * > Sensor > * > Reset	Sensor '[INLETSENSOR]' on inlet '[INLET]' has been reset by user '[USERNAME]' from host '[USERIP]'.	
Inlet > * > Pole > * > Sensor > * > Unavailable	Sensor '[POLESENSOR]' on pole '[INLETPOLE]' of inlet '[INLET]' unavailable.	Sensor '[POLESENSOR]' on pole '[INLETPOLE]' of inlet '[INLET]' available.
Inlet > * > Pole > * > Sensor > *	Sensor '[POLESENSOR]' on pole '[INLETPOLE]' of inlet '[INLET]'	Sensor '[POLESENSOR]' on pole '[INLETPOLE]' of inlet '[INLET]'

Event/Context	Default Assertion Message when the Event = TRUE	Default Assertion Message when the Event = FALSE*
> Above upper critical	asserted 'above upper critical'.	deasserted 'above upper critical'.
Inlet > * > Pole > * > Sensor > * > Above upper warning	Sensor '[POLESENSOR]' on pole '[INLETPOLE]' of inlet '[INLET]' asserted 'above upper warning'.	Sensor '[POLESENSOR]' on pole '[INLETPOLE]' of inlet '[INLET]' deasserted 'above upper warning'.
Inlet > * > Pole > * > Sensor > * > Below lower warning	Sensor '[POLESENSOR]' on pole '[INLETPOLE]' of inlet '[INLET]' asserted 'below lower warning'.	Sensor '[POLESENSOR]' on pole '[INLETPOLE]' of inlet '[INLET]' deasserted 'below lower warning'.
Inlet > * > Pole > * > Sensor > * > Below lower critical	Sensor '[POLESENSOR]' on pole '[INLETPOLE]' of inlet '[INLET]' asserted 'below lower critical'.	Sensor '[POLESENSOR]' on pole '[INLETPOLE]' of inlet '[INLET]' deasserted 'below lower critical'.
Modem > Dial-in link established	An incoming call from caller '[CALLERID]' was received.	The incoming call from caller '[CALLERID]' was disconnected: [CALLENDREASON].
Modem > Modem attached	A [MODEMTYPE] modem was attached.	
Modem > Modem detached	A [MODEMTYPE] modem was removed.	
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 > * > Unavailable	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' unavailable.	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' available.
Outlet > * > Sensor > * > Above upper critical	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' asserted 'above upper critical'.	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' deasserted 'above upper critical'.
Outlet > * > Sensor > * > Above upper warning	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' asserted 'above upper warning'.	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' deasserted 'above upper warning'.
Outlet > * > Sensor > * > Below lower warning	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' asserted 'below lower warning'.	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' deasserted 'below lower warning'.
Outlet > * > Sensor > * > Below	Sensor '[OUTLETSENSOR]' on outlet	Sensor '[OUTLETSENSOR]' on

Event/Context	Default Assertion Message when the Event = TRUE	Default Assertion Message when the Event = FALSE*
lower critical	'[OUTLET]' asserted 'below lower critical'.	outlet '[OUTLET]' deasserted 'below lower critical'.
Outlet > * > Sensor > * > Reset	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' has been reset by user '[USERNAME]' from host '[USERIP]'.	
Outlet > * > Sensor > State > On/Off	Outlet '[OUTLET]' state changed to on.	Outlet '[OUTLET]' state changed to off.
Outlet > * > Pole > * > Sensor > Unavailable	Sensor '[POLESENSOR]' on pole '[OUTLETPOLE]' of outlet '[OUTLET]' unavailable.	Sensor '[POLESENSOR]' on pole '[OUTLETPOLE]' of outlet '[OUTLET]' available.
Outlet > * > Pole > * > Sensor > Above upper critical	Sensor '[POLESENSOR]' on pole '[OUTLETPOLE]' of outlet '[OUTLET]' asserted 'above upper critical'.	Sensor '[POLESENSOR]' on pole '[OUTLETPOLE]' of outlet '[OUTLET]' deasserted 'above upper critical'.
Outlet > * > Pole > * > Sensor > Above upper warning	Sensor '[POLESENSOR]' on pole '[OUTLETPOLE]' of outlet '[OUTLET]' asserted 'above upper warning'.	Sensor '[POLESENSOR]' on pole '[OUTLETPOLE]' of outlet '[OUTLET]' deasserted 'above upper warning'.
Outlet > * > Pole > * > Sensor > Below lower warning	Sensor '[POLESENSOR]' on pole '[OUTLETPOLE]' of outlet '[OUTLET]' asserted 'below lower warning'.	Sensor '[POLESENSOR]' on pole '[OUTLETPOLE]' of outlet '[OUTLET]' deasserted 'below lower warning'.
Outlet > * > Pole > * > Sensor > Below lower critical	Sensor '[POLESENSOR]' on pole '[OUTLETPOLE]' of outlet '[OUTLET]' asserted 'below lower critical'.	Sensor '[POLESENSOR]' on pole '[OUTLETPOLE]' of outlet '[OUTLET]' deasserted 'below lower critical'.
Overcurrent Protector > * > Sensor > * > Unavailable	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' unavailable.	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' available.
Overcurrent Protector > * > Sensor > * > Above upper critical	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' asserted 'above upper critical'.	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' deasserted 'above upper critical'.
Overcurrent Protector > * > Sensor > * > Above upper warning	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' asserted 'above upper warning'.	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' deasserted 'above upper warning'.
Overcurrent Protector > * > Sensor > * > Below lower warning	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' asserted 'below lower warning'.	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' deasserted 'below lower warning'.
Overcurrent Protector > * > Sensor > * > Below lower	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' asserted	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]'

critical	'below lower critical'.	deasserted 'below lower critical'.
Overcurrent Protector > * > Sensor > * > Open/Closed	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' is open.	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' is closed.
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 '[SERVER]' is now being monitored.	Server '[SERVER]' is no longer being monitored.
Server Monitoring > * > Unreachable	Server '[SERVER]' is unreachable.	Server '[SERVER]' is reachable.
Server Monitoring > * > Unrecoverable	Connection to server '[MONITOREDHOST]' could not be restored.	
User Activity > * > User logon state	User '[USERNAME]' from host '[USERIP]' logged in.	User '[USERNAME]' from host '[USERIP]' logged out.
User Activity > * > Authentication failure	Authentication failed for user '[USERNAME]' from host '[USERIP]'.	
User Activity > * > User accepted the Restricted Service Agreement	User '[USERNAME]' from host '[USERIP]" accepted the Restricted Service Agreement.	User '[USERNAME]' from host '[USERIP]" declined the Restricted Service Agreement.
User Activity > * > User blocked	User '[USERNAME]' from host '[USERIP]' was blocked.	
User Activity > * > Session timeout	Session of user '[USERNAME]' from host '[USERIP]' timed out.	
User Administration > User added	User '[TARGETUSER]' added by user '[USERNAME]' from host '[USERIP]'.	
User Administration > User modified	User '[TARGETUSER]' modified by user '[USERNAME]' from host '[USERIP]'.	
User Administration > User deleted	User '[TARGETUSER]' deleted by user '[USERNAME]' from host '[USERIP]'.	
User Administration > Password changed	Password of user '[TARGETUSER]' changed by user '[USERNAME]' from host '[USERIP]'.	
User Administration > Password settings changed	Password settings changed by user '[USERNAME]' from host '[USERIP]'.	
User Administration > Role	Role '[TARGETROLE]' added by user	

added	'[USERNAME]' from host '[USERIP]'.	
User Administration > Role modified	Role '[TARGETROLE]' modified by user '[USERNAME]' from host '[USERIP]'.	
User Administration > Role deleted	Role '[TARGETROLE]' deleted by user '[USERNAME]' from host '[USERIP]'.	
Webcam Management > Webcam attached	Webcam '[WEBCAMNAME]' ('[WEBCAMUVCID]') added to port '[WEBCAMUSBPORT]'.	
Webcam Management > Webcam detached	Webcam '[WEBCAMNAME]' ('[WEBCAMUVCID]') removed from port '[WEBCAMUSBPORT]'.	
Webcam Management > Webcam settings changed	Webcam '[WEBCAMNAME]' settings changed by user '[USERNAME]'.	
LHX / SHX > Connected	LHX has been connected to [PORTTYPE] port [PORTID].	LHX has been disconnected from [PORTTYPE] port [PORTID].
LHX / SHX > Operational State	LHX connected to [PORTTYPE] port [PORTID] has been switched on.	LHX connected to [PORTTYPE] port [PORTID] has been switched off.
LHX / SHX > Sensor > Unavailable	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' unavailable.	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' available.
LHX / SHX > Sensor > Above upper critical threshold	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' asserted 'above upper critical'.	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' deasserted 'above upper critical'.
LHX / SHX > Sensor > Above upper warning threshold	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' asserted 'above upper warning'.	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' deasserted 'above upper warning'.
LHX / SHX > Sensor > Below lower warning threshold	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' asserted 'below lower warning'.	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' deasserted 'below lower warning'.
LHX / SHX > Sensor > Below lower critical threshold	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' asserted 'below lower critical'.	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' deasserted 'below lower critical'.
LHX / SHX > Base Electronics Failure	The base electronics on LHX at [PORTTYPE] port '[PORTID]' failed.	
LHX / SHX > Condenser Pump Failure	The condenser pump on LHX at [PORTTYPE] port '[PORTID]' failed.	The condenser pump on LHX at [PORTTYPE] port '[PORTID]' is back to normal.
LHX / SHX > Emergency Cooling	Emergency cooling on LHX at [PORTTYPE] port '[PORTID]' was activated.	Emergency cooling on LHX at [PORTTYPE] port '[PORTID]' was deactivated.

LHX / SHX > Maximum cooling request	Maximum cooling was requested for LHX at [PORTTYPE] port '[PORTID]'.	Maximum cooling is not any more requested for LHX at [PORTTYPE] port '[PORTID]'.
LHX / SHX > Parameter Data Loss	Data loss in parameter memory was detected on LHX at [PORTTYPE] port '[PORTID]'.	
LHX / SHX > ST-Bus Communication Error	An ST-Bus communication error was detected on LHX at [PORTTYPE] port '[PORTID]'.	
LHX / SHX > Collective fault	A collective fault occurred on LHX at [PORTTYPE] port '[PORTID]'.	
LHX / SHX > Door Contact	The door of LHX at [PORTTYPE] port '[PORTID]' was opened.	The door of LHX at [PORTTYPE] port '[PORTID]' was closed.
LHX / SHX > Sensor Failure	A sensor failure (broken or short circuit) occurred on LHX at [PORTTYPE] port '[PORTID]' at sensor '[LHXSENSORID]'.	
LHX / SHX > Fan Failure	A fan motor failure occurred on LHX at [PORTTYPE] port '[PORTID]' at fan '[LHXFANID]'.	
LHX / SHX > Power Supply Failure	A power supply failure occurred on LHX at [PORTTYPE] port '[PORTID]' at power supply '[LHXPOWERSUPPLYID]'.	
LHX / SHX > Threshold Air Inlet	The air inlet temperature threshold on LHX at [PORTTYPE] port '[PORTID]' was crossed.	The air inlet temperature on LHX at [PORTTYPE] port '[PORTID]' is within thresholds.
LHX / SHX > Threshold Air Outlet	The air outlet temperature threshold on LHX at [PORTTYPE] port '[PORTID]' was crossed.	The air outlet temperature on LHX at [PORTTYPE] port '[PORTID]' is within thresholds.
LHX / SHX > Threshold Water Inlet	The water inlet temperature threshold on LHX at [PORTTYPE] port '[PORTID]' was crossed.	The water inlet temperature on LHX at [PORTTYPE] port '[PORTID]' is within thresholds.
LHX / SHX > Threshold Water Outlet	The water outlet temperature threshold on LHX at [PORTTYPE] port '[PORTID]' was crossed.	The water outlet temperature on LHX at [PORTTYPE] port '[PORTID]' is within thresholds.
LHX / SHX > Voltage Low	The supply voltage on LHX at [PORTTYPE] port '[PORTID]' is low.	The supply voltage on LHX at [PORTTYPE] port '[PORTID]' is back to normal.
LHX / SHX > Threshold Humidity	The humidity threshold on LHX at [PORTTYPE] port '[PORTID]' was crossed.	The humidity on LHX at [PORTTYPE] port '[PORTID]' is within thresholds.

LHX / SHX > External Water Cooling Failure	An external water cooling failure occurred on LHX at [PORTTYPE] port '[PORTID]'.	
LHX / SHX > Water Leak	Water leakage was detected on LHX at [PORTTYPE] port '[PORTID]'.	
Power Metering Controller > Power Meter Created	Power meter '[POWERMETER]' was created.	
Power Metering Controller > Power Meter Deleted	Power meter '[POWERMETER]' was deleted."	
Power Metering Controller > Power Meter Modified	Power meter '[POWERMETER]' was modified.	

The asterisk symbol (*) represents anything you select for the 'trigger' events.

Note: The PX does not support 'Power Metering Controller' so you can ignore them.

Email and SMS Message Placeholders

Following are placeholders that can be used in custom event email messages.

Note: Click the Information icon to open the Event Context Information dialog, which contains a list of placeholders and their definitions. Then select the desired placeholder, and either double-click it or click the "Paste into Message" button to insert it into the customized message.

Placeholder	Definition
[ACTIVEINLET]	The label of the newly activated inlet
[AMSBLADESLOTPOSITION]	The (horizontal) slot position, an action applies to
[AMSLEDCOLOR]	The RGB LED color
[AMSLEDMODE]	The LED indication mode
[AMSLEDOPMODE]	The LED operating mode
[AMSNAME]	The name of an asset strip
[AMSNUMBER]	The numeric ID of an asset strip
[AMSRACKUNITPOSITION]	The (vertical) rack unit position, an action applies to
[AMSSTATE]	The human readable state of an asset strip
[AMSTAGID]	The asset tag ID

Placeholder	Definition
[CIRCUITCTRATING]	The circuit CT rating
[CIRCUITCURRENTRATING]	The circuit current rating
[CIRCUITNAME]	The circuit name
[CIRCUITPOLE]	The circuit power line identifier
[CIRCUITSENSOR]	The circuit sensor name
[CIRCUIT]	The circuit identifier
[CONFIGPARAM]	The name of a configuration parameter
[CONFIGVALUE]	The new value of a parameter
[DATETIME]	The human readable timestamp of the event occurrence
[DEVICEIP]	The IP address of the device, the event occurred on
[DEVICENAME]	The name of the device, the event occurred on
[ERRORDESC]	The error message
[EVENTRULENAME]	The name of the matching event rule
[EXTSENSORNAME]	The name of a peripheral device
[EXTSENSORSLOT]	The ID of a peripheral device slot
[EXTSENSOR]	The peripheral device identifier
[IFNAME]	The human readable name of a network interface
[INLETPOLE]	The inlet power line identifier
[INLETSENSOR]	The inlet sensor name
[INLET]	The power inlet label
[ISASSERTED]	Boolean flag whether an event condition was entered (1) or left (0)
[LDAPERRORDESC]	An LDAP error occurred
[LHXFANID]	The ID of a fan connected to an LHX/SHX
[LHXPOWERSUPPLYID]	The ID of an LHX/SHX power supply
[LHXSENSORID]	The ID of an LHX/SHX sensor probe
[MONITOREDHOST]	The name or IP address of a monitored host
[OCPSENSOR]	The overcurrent protector sensor name
[OCP]	The overcurrent protector label
[OLDVERSION]	The firmware version the device is being upgraded from

Placeholder	Definition
[OUTLETPOLE]	The outlet power line identifier
[OUTLETSENSOR]	The outlet sensor name
[OUTLET]	The outlet label
[PDUPOLESENSOR]	The sensor name for a certain power line
[PDUSENSOR]	The PDU sensor name
[PERIPHDEVPOSITION]	The position of an attached peripheral device
[PHONENUMBER]	The phone number an SMS was sent to
[PORTID]	The label of the external port, the event triggering device is connected to
[PORTTYPE]	The type of the external port (for example, 'feature' or 'auxiliary'), the event triggering device is connected to
[POWERMETERPOLE]	The PMC power meter line identifier
[POWERMETERSENSOR]	The PMC power meter sensor name
[POWERMETER]	The PMC power meter ID
[RADIUSERRORDESC]	A Radius error occurred
[ROMCODE]	The rom code of an attached peripheral device
[SENSORREADINGUNIT]	The unit of a sensor reading
[SENSORREADING]	The value of a sensor reading
[SENSORREPORT]	The formatted sensor report contents
[SENSORSTATENAME]	The human readable state of a sensor
[SMTPRECIPIENTS]	The list of recipients, an SMTP message was sent to
[SMTPSERVER]	The name or IP address of an SMTP server
[SYSCONTACT]	SysContact as configured for SNMP
[SYSLOCATION]	SysLocation as configured for SNMP
[SYSNAME]	SysName as configured for SNMP
[TIMEREVENTID]	The id of a timer event
[TIMESTAMP]	The timestamp of the event occurrence
[TRANSFERSWITCHREASON]	The transfer reason
[TRANSFERSWITCHSENSOR]	The transfer switch sensor name
[TRANSFERSWITCH]	The transfer switch label
[UMTARGETROLE]	The name of a user management role, an action was applied on

Placeholder	Definition
[UMTARGETUSER]	The user, an action was triggered for
[USERIP]	The IP address, a user connected from
[USERNAME]	The user who triggered an action
[VERSION]	The firmware version the device is upgrading to

Sample Event Rules

Sample PDU-Level Event Rule

In this example, we want the PX to record the firmware upgrade failure in the internal log when it happens. The sample event rule looks like this:

- Event: Device > Firmware update failed
- Actions: System Event Log Action

To create the above event rule:

1. Select Event > Device to indicate we are specifying an event at the PDU level.
2. Select "Firmware update failed" in the submenu because we want the PX to respond to the event related to firmware upgrade failure.
3. Select System Event Log Action as we intend to record the firmware update failure event in the internal log.

Sample Outlet-Level Event Rule

In this example, we want the PX to send SNMP notifications to the SNMP manager for any sensor change event of outlet 3.

Note: The SNMP notifications may be SNMP v2c or SNMP v3 traps or informs, depending on the settings for the System SNMP Notification Action. See **Configuring SNMP Notifications** *(on page 350).*

To do that we would set up an event rule like this:

- Event: Outlet > Outlet 3 > Sensor > Any sub-event
- Actions: System SNMP Notification Action

To create the above event rule:

1. Select Event > Outlet to indicate we are specifying an event at the outlet level.
2. Select "Outlet 3" from the submenu because that is the outlet in question.

3. Select "Sensor" to refer to sensor events.
4. Select "Any sub-event" because we want to specify all events related to all types of outlet sensors and thresholds, such as current, voltage, upper critical threshold, upper warning threshold, lower critical threshold, lower warning threshold, and so on.
5. Select "System SNMP Notification Action" to send SNMP notifications to respond to the specified event.

   Then the SNMP notifications are sent when:

   - Any numeric sensor's reading moves past any threshold into the warning or critical range.
   - Any sensor reading or state returns to normal.
   - Any sensor becomes unavailable.
   - The active energy sensor is reset.
   - Any discrete sensor changes its state -- either from normal to alarmed or from alarmed to normal.

   For example, when the outlet 3's voltage crosses into the upper warning range, 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 PX to send SNMP notifications to the SNMP manager for any sensor change event of the Inlet I1.

Note: The SNMP notifications may be SNMP v2c or SNMP v3 traps or informs, depending on the settings for the System SNMP Notification Action. See **Configuring SNMP Notifications** *(on page 350).*

The event rule is set like this:

- Event: Inlet > Inlet I1 > Sensor > Any sub-event
- Actions: System SNMP Notification Action

▶ To create the above event rule:

1. Select Event > Inlet to indicate we are specifying an event at the inlet level.
2. Select "Inlet I1" from the submenu because that is the inlet in question.
3. Select "Sensor" to refer to sensor events.
4. Select "Any sub-event" because we want to specify all events related to all types of inlet sensors and thresholds, such as current, voltage, upper critical threshold, upper warning threshold, lower critical threshold, lower warning threshold, and so on.

5. Select "System SNMP Notification Action" to send SNMP notifications to respond to the specified event.

   Then the SNMP notifications are sent when:

   - Any numeric sensor's reading moves past any threshold into 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 enters the upper warning range, the SNMP notifications are sent, and when the voltage drops below the upper warning threshold, returning to the normal state, 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 PX to enable the load shedding function when a contact closure sensor enters the alarmed state. This sample event rule requires creating a new action before creating the rule.

Step 1: create a new action for enabling the load shedding mode

1. Choose Device Settings > Event Rules. The Event Rule Settings dialog appears.
2. Click the Actions tab.
3. Click New Action.
4. In the Action Name field, type a name to identify this action. In this illustration, type Activate Load Shedding.
5. In the Action field, select "Change load shedding state."
6. In the Operation field, select Start Load Shedding.
7. Click Save to save this action.

After the new action for enabling the load shedding mode is created, you can create an event rule that can trigger the load shedding mode when the contact closure sensor enters the alarmed state. This sample event rule looks like this:

- Event: Peripheral Device Slot > Slot 1 > State Sensor > Alarmed/Open/On
- Trigger condition: Alarmed/Open/On
- Actions: Activate Load Shedding

Step 2: create the contact closure triggered load shedding event rule

1. Click the Rules tab.
2. Click New Rule.
3. In the "Rule name" field, type a name to identify this event rule. In this illustration, type Contact Closure Triggered Load Shedding.
4. Select the Enabled checkbox. Otherwise, the new event rule will not be carried out.
5. Select Events > Peripheral Device Slot to indicate we are specifying an event related to the environmental sensor.
6. 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 in the submenu.
7. Select State Sensor because the contact closure sensor is a discrete sensor, which indicates the environmental changes through the status changes.
8. Select "Alarmed/Open/On" in the submenu since we want the action "Activate Loading Shedding" to be taken when the selected contact closure sensor changes its state related to the "alarmed" state.
9. In the "Trigger condition" field, select the Alarmed radio button because we want the PX to respond to the event only when the contact closure sensor enters the Alarm state.

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 PX keeps busy because the action or one of the actions taken for a certain event triggers an identical or similar event which will result in an action triggering one event again.

Example 1

This example illustrates an event rule which continuously causes the PX 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 PX 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 PX to continuously power cycle outlets 1 and 2.

Event selected	Action included
Outlet > Outlet 1 > Sensor > State > On/Off	Cycle Outlet 2 (Switch Outlets --> Cycle Outlet --> Outlet 2)
Outlet > Outlet 2 > Sensor > State > On/Off	Cycle Outlet 1 (Switch Outlets --> Cycle Outlet --> Outlet 1)

Modifying an Event Rule

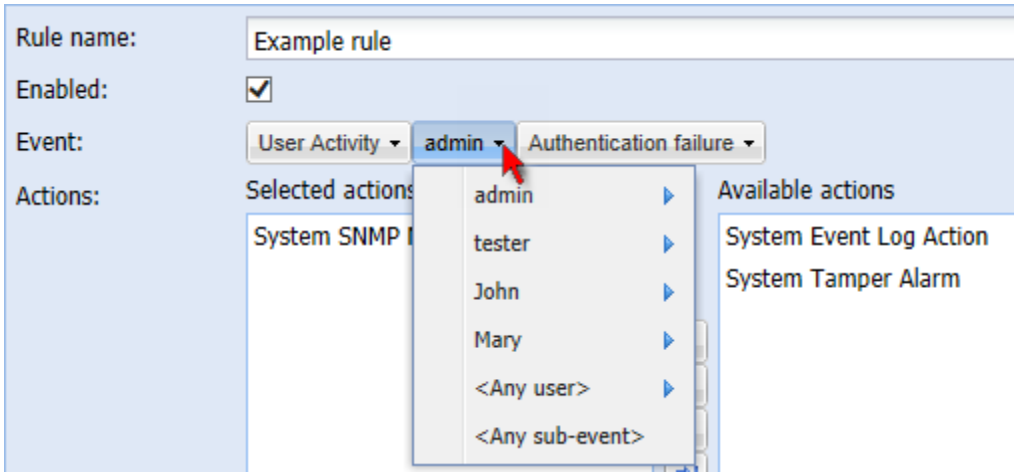
You can change an event rule's event, action, trigger condition and other settings, if any.

Exception: Events and actions selected in the built-in event rules are not changeable, including System Event Log Rule, System SNMP Notification Rule, System Tamper Detection Alarmed, and System Tamper Detection Unavailable.

To modify an event rule:

1. Choose Device Settings > Event Rules. The Event Rule Settings dialog appears.
2. On the Rules tab, select the event rule that you want to modify and click Edit, or simply double-click that rule.
3. To disable the event rule, deselect the Enabled checkbox.
4. To change the event, click the desired tab in the Event field and select a different item from the pull-down menu or submenu.

   For example, in a user activity event rule for the "admin" user, you can click the "admin" tab to display a pull-down submenu showing all user names, and then select a different user name or all users (shown as <*Any user*>).



5. If the "Trigger condition" field is available, you may select a radio button other than the current selection to change the rule triggering condition.
6. To change the action(s), do any of the following in the Actions field:
   - To add any action, select it from the "Available actions" list box, and click . To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.

- To add all actions, click .
- To remove any action, select it from the "Selected actions" list box, and click to move it back to the "Available actions" list box. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.
- To remove all actions, click .
- To create a new action, click Create New Action. The newly created action will be moved to the "Selected actions" list box once it is created. See ***Creating Actions*** (on page 237) for information on creating an action.

7. Click OK to save the changes.

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

8. Click Close to quit the dialog.

Modifying an Action

An existing action can be changed so that all event rules where this action is involved change their behavior accordingly.

Exception: The built-in actions "System Event Log Action" and "System Tamper Alarm" are not user-configurable.

To modify an action:

1. Choose Device Settings > Event Rules. The Event Rule Settings dialog appears.
2. Click the Actions tab.
3. Select the action that you want to modify and click Edit, or simply double-click that action.
4. Make necessary changes to the information shown.
5. Click OK to save the changes.

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

6. Click Close to quit the dialog.

Deleting an Event Rule or Action

If any event rule or action is obsolete, simply remove it.

Note: You cannot delete the built-in event rules and actions.

To delete an event rule or action:

1. Choose Device Settings > Event Rules. The Event Rule Settings dialog appears.
2. To delete an event rule:
   a. Ensure the Rules tab is selected. If not, click the Rules tab.
   b. Select the desired rule from the list. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.
   c. Click Delete.
   d. Click Yes on the confirmation message.
3. To delete an action:
   a. Click the Actions tab.
   b. Select the desired action from the list. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.
   c. Click Delete.
   d. Click Yes on the confirmation message.
4. Click Close to quit the dialog.

A Note about Untriggered Rules

In some cases, a measurement exceeds a threshold causing the PX to generate an alert. The measurement then returns to a value within the threshold, but the PX does not generate an alert message for the Deassertion event. Such scenarios can occur due to the hysteresis tracking the PX uses. See ***"To De-assert" and Deassertion Hysteresis*** (on page 672).

Managing Event Logging

By default, the PX captures certain system events and saves them in a local (internal) event log.

Viewing the Local Event Log

You can view over 2000 historical events that occurred to the PX device in the local event log.

When the log size exceeds 256KB, each new entry overwrites the oldest entry.

To display the local log:

1. Choose Maintenance > View Event Log. The Event Log dialog appears.

   Each event entry in the local log consists of:

   - Date and time of the event
   - Type of the event
   - A description of the event
   - ID number of the event

2. The dialog shows the final page by default. You can:

   - Switch between different pages by doing one of the following:

     - Click or to go to the first or final page.

     - Click or to go to the prior or next page.

     - Type a number in the Page text box and press Enter to go to a specific page.

   - Select a log entry from the list and click Show Details, or simply double-click the log entry to view detailed information.

   Note: Sometimes when the dialog is too narrow, the icon takes the place of the Show Details button. In that case, click and select Show Details to view details.

   - Click to view the latest events.
   - View a specific type of events only by selecting an event type in the Filter Event Class field.

Clearing Event Entries

If it is not necessary to keep existing event history, you can remove all of it from the local log.

To delete all event entries:

1. Choose Maintenance > View Event Log. The Event Log dialog appears.
2. Click Clear Event Log.

3. Click Yes on the confirmation message.

Viewing the Wireless LAN Diagnostic Log

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

To display the wireless LAN diagnostic log:

1. Choose Device Settings > Network. The Network Configuration dialog appears.
2. Click Show WLAN Diagnostic Log. The WLAN Diagnostic Log dialog appears.

   Each entry in the log consists of the event's:

   - ID number
   - Date and time
   - Description

   Note: The Show WLAN Diagnostic Log button is available only when the Network Interface is set to Wireless.

3. The dialog shows the final page by default. You can:
   - Switch between different pages by doing one of the following:

     - Click or to go to the first or final page.

     - Click or to go to the prior or next page.

     - Type a number in the Page text box and press Enter to go to a specific page.
   - Select a log entry from the list and click Show Details, or simply double-click the log entry to view detailed information.

   Note: Sometimes when the dialog is too narrow, the icon takes the place of the Show Details button. In that case, click and select Show Details to view details.

   - Click to view the latest events.

To clear the diagnostic log:

1. Click Clear WLAN Diagnostic Log.
2. Click Yes on the confirmation message.

Viewing Connected Users

You can see which users are connected to the PX device and their status. If you have administrator privileges, you can terminate any user's connection to the PX device.

To view connected users:

1. Choose Maintenance > Connected Users. The Connected Users dialog appears, showing a list of connected users with the following information:

Column	Description
User Name	The login name used by each connected user.
IP Address	The IP address of each user's host. For the login via a local connection (serial RS-232 or USB), <local> is displayed instead of an IP address.
Client Type	The interface through which the user is being connected to the PX. ▪ Web GUI: Refers to the PX web interface. ▪ CLI: Refers to the command line interface (CLI). The information in parentheses following "CLI" indicates how this user is connected to the CLI. - *Serial*: Represents the local connection (serial RS-232 or USB). - *SSH*: Represents the SSH connection. - *Telnet*: Represents the Telnet connection.
Idle Time	The length of time for which a user remains idle. The unit "min" represents minutes.

2. To disconnect any user, click the corresponding Disconnect button.
   a. A dialog appears, prompting you to confirm the operation.
   b. Click Yes to disconnect the user or No to abort the operation. If clicking Yes, the connected user is forced to log out..
3. Click Close to quit the dialog.

Note: All Live Preview sessions sharing the same URL, including one Primary Standalone Live Preview window and two associated remote sessions, are identified as one single "<webcam>" user in the Connected Users dialog. You can disconnect a "<webcam>" user from this dialog to terminate a specific Primary Standalone Live Preview window and all of its remote sessions. See **Sending Snapshots or Videos in an Email or Instant Message** *(on page 327).*

Monitoring Server Accessibility

You can monitor whether specific IT devices are alive by having the PX device continuously ping them. An IT device's successful response to the ping commands indicates that the IT device is still alive and can be remotely accessed.

This function is especially useful when you are not located in an area with Internet connectivity.

Adding IT Devices for Ping Monitoring

PX can monitor the accessibility of any type of IT equipment, such as database servers, remote authentication servers, power distribution units (PDUs), and so on.

PX supports monitoring a maximum of 8 devices.

The default ping settings may not be suitable for monitoring devices that require high connection reliability so it is strongly recommended that you should adjust the ping settings to meet your own needs.

Tip: To make the PX automatically log, send notifications or perform other actions for any server accessibility or inaccessibility events, you can create event rules associated with server monitoring. See **Event Rules and Actions** *(on page 236).*

To add IT equipment for ping monitoring:

1. Choose Device Settings > Server Reachability. The Server Reachability dialog appears.
2. Click New. The Add New Server dialog appears.
3. By default, the "Enable ping monitoring for this server" checkbox is selected. If not, select it to enable this feature.
4. Provide the information required.

Field	Description
IP address/hostname	IP address or host name of the IT equipment which you want to monitor.

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 (in seconds) after successful ping	The wait time before sending the next ping if the previous ping was successfully responded. Valid range is 5 to 600 (seconds).
Wait time (in seconds) after unsuccessful ping	The wait time before sending the next ping if the previous ping was not responded. Valid range is 3 to 600 (seconds).
Number of consecutive unsuccessful pings for failure	The number of consecutive pings without any response before the monitored equipment is declared "Unreachable." Valid range is 1 to 100.
Wait time (in seconds) before resuming pinging after failure	The wait time before the PX 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 PX disables the ping monitoring feature for it and shows "Waiting for reliable connection." Valid range is 0 to 100.

5. Click OK.
6. To add more IT devices, repeat Steps 2 to 5.
7. Click Close to quit the dialog.

In the beginning, the status of the monitored equipment shows "Waiting for reliable connection," which means the requested number of consecutive successful or unsuccessful pings has not reached before the PX can declare that the monitored device is reachable or unreachable.

Example: Ping Monitoring and SNMP Notifications

In this illustration, it is assumed that a significant PDU (IP address: 192.168.84.95) shall be monitored by your PX to make sure that PDU is properly operating all the time, and the PX must send out SNMP notifications (trap or inform) if that PDU is declared unreachable due to power or network failure. The prerequisite for this example is that the power source for your PX is different from the power source for that PDU.

This requires two steps: set up the PDU monitoring and create an event rule.

Step 1: Set up the ping monitoring for the target PDU

1. Choose Device Settings > Server Reachability. The Server Reachability dialog appears.
2. Click New.
3. Type 192.168.84.95 in the "IP address/hostname" field.
4. Ensure the "Enable ping monitoring for this server" checkbox is selected.
5. To make the PX declare the accessibility of the monitored PDU every 15 seconds (3 pings * 5 seconds) when that PDU is accessible, do the following:
   a. In the "Number of successful pings to enable feature" field, type 3.
   b. In the "Wait time (in seconds) after successful ping" field, type 5.
6. To make the PX declare the inaccessibility of the monitored PDU when that PDU becomes inaccessible for around 12 seconds (4 pings * 3 seconds), do the following:
   a. In the "Number of consecutive unsuccessful pings for failure" field, type 4.
   b. In the "Wait time (in seconds) after unsuccessful ping" field, type 3.
7. In the "Wait time (in seconds) before resuming pinging" field, type 60 to make the PX stops pinging the target PDU for 60 seconds (1 minute) after the PDU inaccessibility is declared. After 60 seconds, the PX will re-ping the target PDU.

Step 2: Create an event rule to send SNMP notifications for this PDU

1. Choose Device Settings > Event Rules. The Event Rule Settings dialog appears.
2. Click New.

3. In the "Rule name" field, type "Send SNMP notifications for PDU (192.168.84.95) inaccessibility."
4. Select the Enabled checkbox to enable this new rule.
5. In the Event field, choose Server Monitoring > 192.168.84.95 > Unreachable.
6. In the "Trigger condition" field, select the Unreachable radio button. This makes the PX react only when the target PDU becomes inaccessible.
7. Select the System SNMP Notification Action from the "Available actions" list box, and click to add it to the "Selected actions" list box.

Note: If you have not configured the System SNMP Notification Action to specify the SNMP destination(s), see **Configuring SNMP Notifications** *(on page 350).*

Editing Ping Monitoring Settings

You can edit the ping monitoring settings for any IT device whenever needed.

To modify the ping monitoring settings for an IT device:

1. Choose Device Settings > Server Reachability. The Server Reachability dialog appears.
2. Select the IT device whose settings you want to modify.
3. Click Edit or double-click that IT device. The Edit Server 'XXX' dialog appears, where XXX is the IP address or host name of the IT device.
4. Make changes to the information shown.
5. Click OK.

Deleting Ping Monitoring Settings

When it is not necessary to monitor the accessibility of any IT device, just remove it.

To delete ping monitoring settings for an IT device:

1. Choose Device Settings > Server Reachability. The Server Reachability dialog appears.
2. Select the IT device that you want to remove. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.
3. Click Delete.

4. Click Yes on the confirmation message.
5. Click Close to quit the dialog.

Checking Server Monitoring States

Server monitoring results are available in the Server Reachability dialog after specifying IT devices for the PX device to monitor their network accessibility.

To check the server monitoring states and results:

1. Choose Device Settings > Server Reachability. The Server Reachability dialog appears.
2. The column labeled "Ping Enabled" indicates whether the monitoring for the corresponding IT device is activated or not.
   - : This icon denotes that the monitoring for the corresponding device is enabled.
   - : This icon denotes that the monitoring for the corresponding device is disabled.
3. The column labeled "Status" indicates the accessibility of each monitored equipment.

Status	Description
Reachable	The monitored equipment is accessible.
Unreachable	The monitored equipment is inaccessible.
Waiting for reliable connection	The connection between the PX device and the monitored equipment is not reliably established yet.

4. Click Close to quit the dialog.

Environmental Sensors and Actuators

The PX can monitor the environmental conditions, such as temperature and humidity, where environmental sensors are placed. If an actuator is connected to the PX, you can use it to control a system or mechanism.

To add environmental sensors and actuators:

1. Physically connect environmental sensor packages to the PX device. See ***Connecting Environmental Sensor Packages*** (on page 35).
2. Log in to the PX web interface. The PX should have detected the connected sensors and actuators, and display them in the web interface.
3. Identify each sensor and actuator. See ***Identifying Environmental Sensors and Actuators*** (on page 296).

4. The PX should automatically manage the detected sensors and actuators. Verify whether detected sensors and actuators are managed. If not, have them managed. See ***Managing Environmental Sensors or Actuators*** (on page 300).
5. Configure the sensors and actuators. See ***Configuring Environmental Sensors or Actuators*** (on page 302). The steps include:
   a. Name the sensor or actuator.
   b. If the connected sensor is a Raritan contact closure sensor, specify an appropriate sensor type.
   c. Mark the sensor or actuator's physical location on the rack or in the room.
   d. For a numeric sensor, configure the sensor's threshold, hysteresis and assertion timeout settings.

Note: Numeric sensors show both numeric readings and sensor states to indicate environmental or internal conditions while discrete (on/off) sensors show sensor states only to indicate state changes. Only numeric sensors have threshold settings. As for actuators, they are used to control a device or system so they show state changes only.

Identifying Environmental Sensors and Actuators

Raritan has developed four types of environmental sensor packages - DPX, DPX2, DPX3 and DX series. The ways to identify each type of environmental sensor packages in the web interface are different.

- DPX series: This type of environmental sensor package can be identified through its serial number.
- DPX2, DPX3 and DX series: This type of environmental sensor package can be identified either through its serial number or through its chain position, which consists of the sensor port and its location in the daisy chain.

See ***Matching the Serial Number*** (on page 297) and ***Matching the Position*** (on page 298) in the PX User Guide.

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

Matching the Serial Number

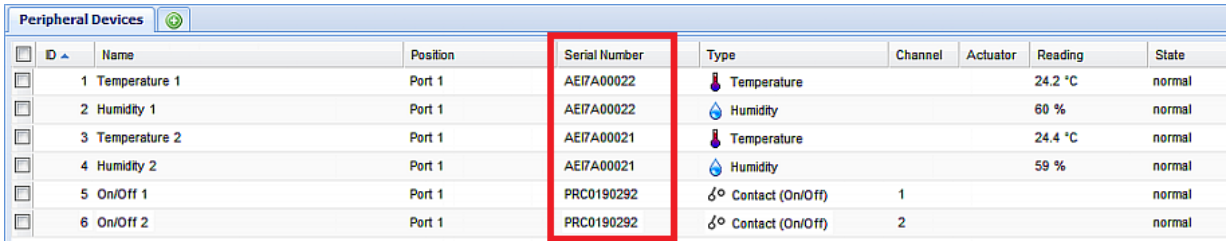
A DPX environmental sensor package includes a serial number tag on the sensor cable.

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

The serial number for each sensor or actuator appears listed in the web interface after each sensor or actuator is detected by the PX.

To identify each detected environmental sensor or actuator via serial numbers:

1. Click Peripheral Devices in the left pane.
2. Match the serial number from the tag to those listed in the sensor table.



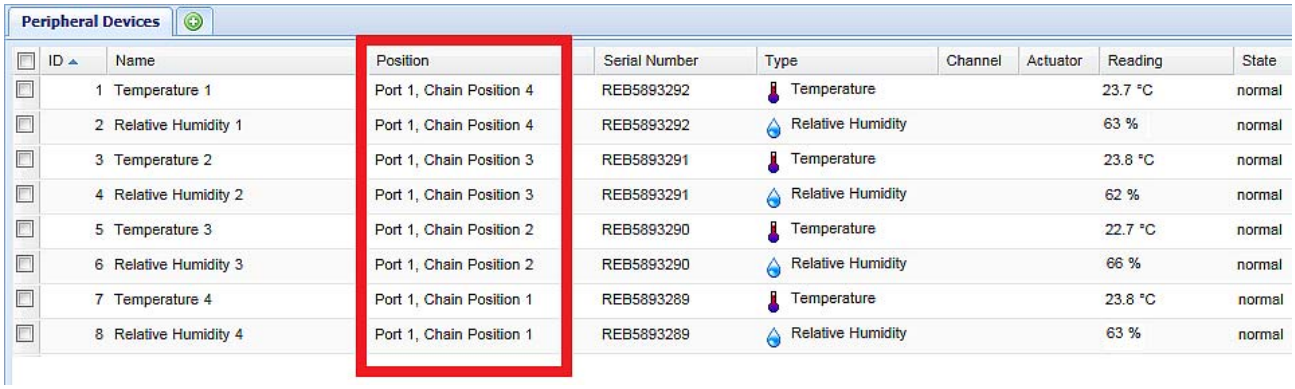
ID	Name	Position	Serial Number	Type	Channel	Actuator	Reading	State
1	Temperature 1	Port 1	AEI7A00022	Temperature			24.2 °C	normal
2	Humidity 1	Port 1	AEI7A00022	Humidity			60 %	normal
3	Temperature 2	Port 1	AEI7A00021	Temperature			24.4 °C	normal
4	Humidity 2	Port 1	AEI7A00021	Humidity			59 %	normal
5	On/Off 1	Port 1	PRC0190292	Contact (On/Off)	1			normal
6	On/Off 2	Port 1	PRC0190292	Contact (On/Off)	2			normal

Matching the Position

DPX2, DPX3 and DX sensor packages can be daisy chained. The PX can indicate each sensor or actuator's position by showing the sensor port where the environmental sensor package is connected as well as its sequence in a sensor daisy chain.

To identify an environmental sensor or actuator through its position:

1. Click Peripheral Devices in the left pane.
2. Locate the Position column, which shows one, two or four pieces of position information.
   - The sensor port number, such as Port 1, Port 2, Port 3 and so on.
   - The sensor or actuator's location in the sensor chain, such as Chain Position 1, Chain Position 2, and so on.

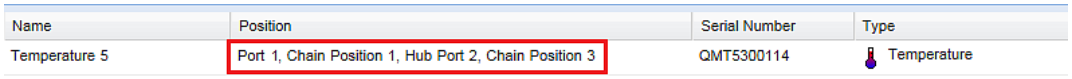


Peripheral Devices

ID	Name	Position	Serial Number	Type	Channel	Actuator	Reading	State
1	Temperature 1	Port 1, Chain Position 4	REB5893292	Temperature			23.7 °C	normal
2	Relative Humidity 1	Port 1, Chain Position 4	REB5893292	Relative Humidity			63 %	normal
3	Temperature 2	Port 1, Chain Position 3	REB5893291	Temperature			23.8 °C	normal
4	Relative Humidity 2	Port 1, Chain Position 3	REB5893291	Relative Humidity			62 %	normal
5	Temperature 3	Port 1, Chain Position 2	REB5893290	Temperature			22.7 °C	normal
6	Relative Humidity 3	Port 1, Chain Position 2	REB5893290	Relative Humidity			66 %	normal
7	Temperature 4	Port 1, Chain Position 1	REB5893289	Temperature			23.8 °C	normal
8	Relative Humidity 4	Port 1, Chain Position 1	REB5893289	Relative Humidity			63 %	normal

   - If a DPX3-ENVHUB4 sensor hub is used, the port number on the hub is also indicated, such as Hub Port 1, Hub Port 2, and so on.

     In addition, two pieces of chain position information are displayed -- the first one indicates the sensor hub's chain position, which is always *Chain Position 1*, and the second one indicates the sensor's or actuator's chain position.



Name	Position	Serial Number	Type
Temperature 5	Port 1, Chain Position 1, Hub Port 2, Chain Position 3	QMT5300114	Temperature

DPX sensor position information:

The PX only displays the sensor port where the DPX sensor package is physically connected. No chain position information is displayed.

For example, if a DPX sensor package is connected to the SENSOR port numbered 1, its Position column only shows "Port 1" no matter a DPX3-ENVHUB4 sensor hub is used or not.

Note: For the PX devices with only one SENSOR port, it always shows "Port 1."

DPX2, DPX3 and DX sensor position information:

The PX displays the sensor package's position in the chain in addition to the sensor port number for DPX2, DPX3 and DX sensor packages.

For example:

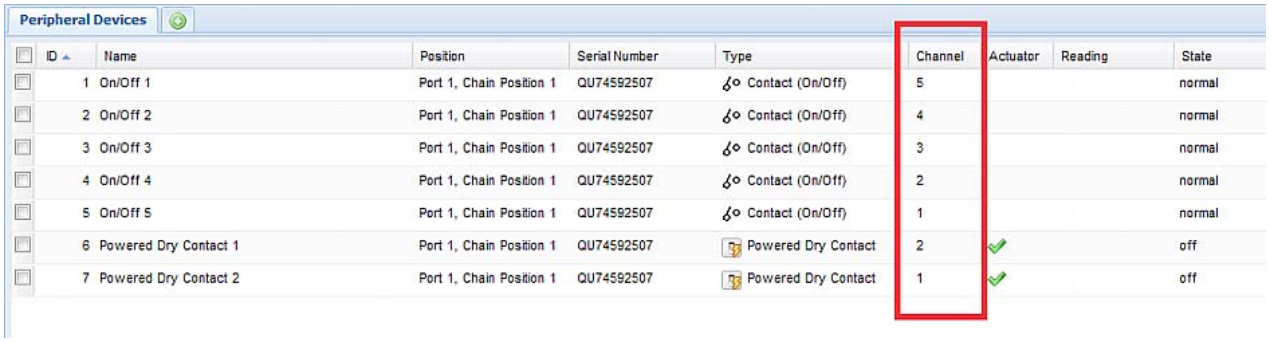
- If a DPX2, DPX3 or DX sensor or actuator is located on the second sensor package in the sensor chain directly connected to the SENSOR port 1, its Position column shows "Port 1, Chain Position 2."
- If this sensor chain is connected to the SENSOR port 1 via the DPX3-ENVHUB4 sensor hub, this sensor's or actuator's Position column becomes "Port 1, Chain Position 1, Hub Port x, Chain Position 2," where x is the hub's port to which this sensor or actuator is physically connected.

Identifying Sensor or Actuator Channels

A sensor package may have multiple contact closure (CC) or dry contact (DC) channels, such as DX-D2C6 or DX-PD2C5.

When the PX initially detects and automatically manages a sensor package with multiple channels, all channels are assigned with ID numbers in sequence.

If you manually manage these channels by selecting "Automatically assign a sensor number," the PX assigns ID numbers randomly because this option assumes that users do not care about the sequence. In this case, see the Channel column to identify each channel correctly. For example, CC1 or DC1 is Channel 1, CC2 or DC2 is Channel 2, and so on.



ID	Name	Position	Serial Number	Type	Channel	Actuator	Reading	State
1	On/Off 1	Port 1, Chain Position 1	QU74592507	Contact (On/Off)	5			normal
2	On/Off 2	Port 1, Chain Position 1	QU74592507	Contact (On/Off)	4			normal
3	On/Off 3	Port 1, Chain Position 1	QU74592507	Contact (On/Off)	3			normal
4	On/Off 4	Port 1, Chain Position 1	QU74592507	Contact (On/Off)	2			normal
5	On/Off 5	Port 1, Chain Position 1	QU74592507	Contact (On/Off)	1			normal
6	Powered Dry Contact 1	Port 1, Chain Position 1	QU74592507	Powered Dry Contact	2	✓		off
7	Powered Dry Contact 2	Port 1, Chain Position 1	QU74592507	Powered Dry Contact	1	✓		off

Managing Environmental Sensors or Actuators

The PX starts to retrieve an environmental sensor's reading and/or state and records the state transitions after the environmental sensor is managed. To control an actuator, you also need to have it managed.

The PX device can manage a maximum of 32 environmental sensors or actuators.

When there are less than 32 managed sensors or actuators, the PX automatically brings detected environmental sensors or actuators under management by default. You have to manually manage a sensor or actuator only when it is not under management.

Tip: You can disable the automatic management feature so that newly connected environmental sensors or actuators are NOT brought under management automatically. See **Disabling the Automatic Management Function** *(on page 312).*

To manually manage an environmental sensor or actuator:

1. Click Peripheral Devices in the left pane.
2. Select the checkbox of the desired sensor or actuator on the Peripheral Devices page. To manage multiple ones, select multiple checkboxes.

   Note: To identify all detected sensors or actuators, see **Identifying Environmental Sensors and Actuators** *(on page 296).*

3. Click Manage. If you selected only one sensor or actuator, the "Manage peripheral device <serial number> (<sensor type>)" dialog appears, where <serial number> is the sensor or actuator's serial number and <sensor type> is its type.

   Note: For a sensor package with contact closure (CC) or dry contact (DC) channels, a channel number is added to the end of the <sensor type>.

4. There are two ways to manage a sensor or actuator:
   - To manage it by letting the PX assign a number to it, select "Automatically assign a sensor number." This method does not release any managed sensors or actuators.
   - To manage it by assigning the number you want to it, select "Manually select a sensor number." Then click the drop-down arrow to select a number.

     If the number you selected was already assigned to a sensor or actuator, that sensor or actuator becomes released after losing this ID number.

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

The manual assignment method is unavailable if you selected multiple sensors or actuators in Step 2.

5. Click OK. The PX starts to display the managed sensor or actuator's reading and state.
6. To manage additional ones, repeat Steps 2 to 5.

Note: When the total number of managed sensors and actuators reaches the maximum, you CANNOT manage additional sensors or actuators unless you remove or replace any managed ones. To remove a sensor or actuator, see **Unmanaging Environmental Sensors or Actuators** *(on page 311).*

Special note for a Raritan humidity sensor:

As of release 3.1.0, a Raritan humidity sensor is able to provide two measurements in the user interface - relative and absolute humidity values.

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

Note: Prior to release 3.1.0, only relative humidity values are available.

Relative humidity sensors can be "automatically" managed but absolute humidity sensors CANNOT. You must "manually" manage absolute humidity sensors if absolute humidity measurements are required.

Relative and absolute humidity values of the same humidity sensor share the same serial number and port position as illustrated below.

However, relative and absolute values of the same humidity sensor DO NOT share the same ID number. The above diagram shows that the two values have different ID numbers -- one is 4 and the other is 5.

Configuring Environmental Sensors or Actuators

You can change the default name to easily identify the managed sensor or actuator, and describe its location with X, Y and Z coordinates.

To configure environmental sensors or actuators:

1. Click Peripheral Devices in the left pane.
2. Select the sensor or actuator that you want to configure.
3. Click Setup in the right pane. The "Setup of peripheral device <serial number> (<sensor type>)" dialog appears, where <serial number> is its serial number and <sensor type> is its type.

   For example, *Setup of peripheral device AEI7A00022 (Temperature)*.
4. Configure available fields properly.

Fields	Description
Name	Assign a name for identification.
Description	Type any descriptive text as needed.
Location (X, Y and Z)	Describe the sensor's or actuator's location by assigning alphanumeric values to the X, Y and Z coordinates. See ***Describing the Sensor's or Actuator's Location*** (on page 304). When the term "Rack Units" appears inside the parentheses in the Z location field, indicating that the Z coordinate format is set to Rack Units, you must type an integer number. See ***Setting the Z Coordinate Format*** (on page 303).
Binary Sensor Subtype	This field is available only when the selected sensor is a contact closure sensor. Select one of the following sensor types: ▪ Contact: The detector/switch is designed to detect the door lock or door open/closed status. ▪ Smoke Detection: The detector/switch is designed to detect the appearance of smoke. ▪ Water Detection: The detector/switch is designed to detect the appearance of water on the floor. ▪ Vibration: The detector/switch is designed to detect the vibration in the floor.
Alarmed to Normal Delay	This field is available only when the selected sensor is the DX-PIR presence detector. It determines the wait time before the PX announces that the presence detector returns to the normal state after it is back to normal. Type both the time and measurement units in this field. For example, type '30 s' for 30 seconds, or '2 min' for 2 minutes.

5. If the selected sensor is a numeric sensor, its threshold settings are displayed in the dialog. See ***Sensor Threshold Settings*** (on page 667) for detailed information.

   There are two types of thresholds: sensor-specific thresholds and default thresholds.

   To use the sensor-specific threshold settings, select the Use Sensor Specific Thresholds radio button.

   - Click Edit or double-click the threshold setting row to open the threshold setup dialog.
   - To enable any threshold, select the corresponding checkbox. To disable a threshold, deselect the checkbox.
   - After any threshold is enabled, type an appropriate numeric value in the accompanying text box.
   - To set the deassertion hysteresis, type a numeric value in the Deassertion Hysteresis field. See ***"To De-assert" and Deassertion Hysteresis*** (on page 672).
   - To set the assertion timeout, type a numeric value in the Assertion Timeout (samples) field. See ***"To Assert" and Assertion Timeout*** (on page 670).

   To use the default threshold settings, select the Use Default Thresholds radio button. To modify the default threshold settings, see ***Changing Default Thresholds*** (on page 305).

   Note: The Upper Critical and Lower Critical values are points at which the PX considers the operating environment critical and outside the range of the acceptable threshold.

6. Click OK.
7. Repeat the same steps to configure additional ones.

Tip: You can configure thresholds of multiple sensors at a time as long as these sensors belong to the same type. See **Setting Thresholds for Multiple Sensors** *(on page 306).*

Setting the Z Coordinate Format

You can use either the number of rack units or a descriptive text to describe the vertical locations (Z coordinates) of environmental sensors and actuators.

To determine the Z coordinate format:

1. Click the PDU folder.

   Note: The folder is named "my PX" by default. The name can be customized. See **Naming the PDU** *(on page 130).*

2. Click Setup in the Settings section. The Pdu Setup dialog appears.
3. In the Peripheral Device Z Coordinate Format field, click the drop-down arrow and select an option from the list.
   - Rack Units: The height of the Z coordinate is measured in standard rack units. When this is selected, you can type a numeric value in the rack unit to describe the Z coordinate of any environmental sensors or actuators.
   - Free-Form: Any alphanumeric string can be used for specifying the Z coordinate.
4. Click OK.

Describing the Sensor's or Actuator's Location

Use the X, Y and Z coordinates to describe each sensor or actuator's physical location. You can use these location values to track records of environmental conditions in fixed locations around your IT equipment. The X, Y and Z values act as additional attributes and are not tied to any specific measurement scheme. If you choose to, you can use non-measurement values. For example:

X = *Brown Cabinet Row*

Y = *Third Rack*

Z = *Top of Cabinet*

Values for the X, Y and Z coordinates may consist of:

- For X and Y: Any combination of alphanumeric characters. The coordinate value can be 0 to 24 characters long.
- For Z when the Z coordinate format is set to *Rack Units*, any numeric value ranging from 0 to 60.
- For Z when the Z coordinate format is set to *Free-Form*, any alphanumeric characters from 0 to 24 characters.

Tip: To configure and retrieve these coordinate values over SNMP, see the PX MIB. To configure and retrieve these values over the CLI, see **Using the Command Line Interface** *(on page 359).*

Changing Default Thresholds

The default thresholds are the initial threshold values that automatically apply to numeric environmental sensors. These values are configured on a sensor type basis, which include:

- Temperature sensors
- Humidity sensors (both relative and absolute humidity)
- Air pressure sensors
- Air flow sensors
- Vibration sensors

Note that changing the default thresholds re-determine the initial thresholds applying to the environmental sensors that are added or detected later on.

In addition, changing the default thresholds also change the thresholds of those environmental sensors where the default thresholds have been selected as their threshold option. See ***Configuring Environmental Sensors or Actuators*** (on page 302).

To change the default threshold settings:

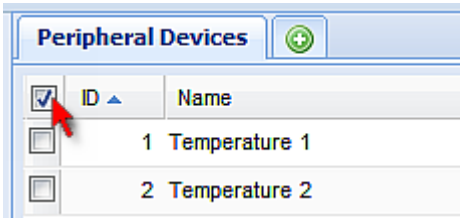
1. Click Peripheral Devices in the left pane.
2. Click Default Thresholds Setup on the Peripheral Devices page. A dialog appears, showing a list of all numeric environmental sensor types.
3. Select the desired sensor type.
4. Click Edit or double-click that sensor type to adjust its threshold settings, deassertion hysteresis or assertion timeout.
   - To enable any threshold, select the corresponding checkbox. To disable a threshold, deselect the checkbox.
   - After any threshold is enabled, type an appropriate numeric value in the accompanying text box.
   - To set the deassertion hysteresis, type a numeric value in the Deassertion Hysteresis field. See ***"To De-assert" and Deassertion Hysteresis*** (on page 672).
   - To set the assertion timeout, type a numeric value in the Assertion Timeout (samples) field. See ***"To Assert" and Assertion Timeout*** (on page 670).
5. Repeat the above step to modify the threshold settings of other numeric sensor types.
6. Click OK.

Setting Thresholds for Multiple Sensors

You can configure thresholds for multiple environmental sensors of *the same type* at a time. For example, if you want all temperature sensors to have identical upper and lower thresholds, follow the procedure below to set up all temperature sensors together.

To configure thresholds of multiple environmental sensors:

1. Click Peripheral Devices in the left pane.
2. Select the checkboxes of those environmental sensors whose threshold settings should be the same. Make sure the selected sensors belong to the same type.
   - To select all of those listed on the Peripheral Devices page, simply select the checkbox in the header row.



3. Click Setup. Note that the Setup button is disabled if any of the selected sensors belongs to a different type.
4. Configure the thresholds as described in ***Configuring Environmental Sensors or Actuators*** (on page 302).
5. Click OK.

Viewing Sensor or Actuator Data

Readings and states of the environmental sensors or actuators will display in the web interface after the sensors and actuators are properly connected and managed.

The Dashboard page shows the information of managed environmental sensors and actuators only, while the Peripheral Devices page shows the information of both managed and unmanaged ones.

Both pages indicate an environmental sensor or actuator's position in either of the following manners:

- **Port <n>**, where <n> is the number of the SENSOR port on the PX where a specific environmental sensor package is connected. DPX sensor packages show this information only.
- **Port <n>, Chain Position <pos_num>**, where <pos_num> is the sensor package's sequential position in a sensor daisy chain. DPX2, DPX3 and DX sensor packages show this information.

If a sensor row is colored, it means the sensor reading already crosses one of the thresholds, the sensor enters an alarmed state, or the overcurrent protector has tripped or blown. See ***The Yellow- or Red-Highlighted Sensors*** (on page 119).

To view managed environmental sensors and actuators only:

1. Click the Dashboard icon in the PX Explorer pane, and the Dashboard page opens in the right pane.
2. Locate the Peripheral Devices section on the Dashboard page. The section shows:
   - Total number of managed sensors and actuators
   - Total number of unmanaged sensors and actuators
   - Information of each managed sensor and actuator, including:
     - Name
     - Position
     - Reading (for numeric sensors)
     - State

To view both managed and unmanaged ones:

Click Peripheral Devices in the left pane.

Detailed information for each connected sensor or actuator is displayed, including:

- ID number
- Name

- Position
- Serial number
- Type
- Channel (for a sensor package with contact closure or dry contact channels)
- Whether the sensor is an 'Actuator' or not (if yes, this icon appears in the Actuator column)
- Reading
- State

States of Managed Sensors

An environmental sensor shows the state after being managed.

Available sensor states vary depending on the sensor type -- numeric or discrete sensors. For example, a contact closure sensor is a discrete (on/off) sensor so it switches between three states only -- unavailable, alarmed and normal.

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

Sensor state	Applicable to
unavailable	All sensors
alarmed	Discrete sensors
normal	All sensors
below lower critical	Numeric sensors
below lower warning	Numeric sensors
above upper warning	Numeric sensors
above upper critical	Numeric sensors

"unavailable" State

The *unavailable* state means the connectivity or communications with the sensor is lost.

The PX pings all managed sensors at regular intervals in seconds. If it does not detect a particular sensor for three consecutive scans, the *unavailable* state is displayed for that sensor.

When the communication with a contact closure sensor's processor is lost, all detectors (that is, all switches) connected to the same sensor package show the "unavailable" state.

Note: When the sensor is deemed unavailable, the existing sensor configuration remains unchanged. For example, the ID number assigned to the sensor remains associated with it.

The PX continues to ping unavailable sensors, and moves out of the *unavailable* state after detecting the sensor for two consecutive scans.

For DPX2, DPX3 or DX sensor packages, all of the connected sensor packages also enter the *unavailable* states if any of them is upgrading its sensor firmware.

"normal" State

This state indicates the sensor is in the normal state.

For a contact closure sensor, usually this state is the normal state you have set.

- If the normal state is set to Normally Closed, the *normal* state means the contact closure switch is closed.
- If the normal state is set to Normally Open, the *normal* state means the contact closure switch is open.

For a Raritan's DPX floor water sensor, the normal state must be set to Normally Open, which means no water is detected.

Note: See the Environmental Sensors Guide or Online Help for information on setting the normal state or dip switch. This guide is available on Raritan's **Support page** *(***http://www.raritan.com/support/***).*

For a numeric sensor, this state means the sensor reading is within the acceptable range as indicated below:

Lower Warning threshold <= Reading < Upper Warning threshold

Note: The symbol <= means smaller than (<) or equal to (=).

"alarmed" State

This state means a discrete (on/off) sensor is in the "abnormal" state.

Usually for a contact closure sensor, the meaning of this state varies based on the sensor's normal state setting.

- If the normal state is set to Normally Closed, the *alarmed* state means the contact closure switch is open.
- If the normal state is set to Normally Open, the *alarmed* state means the contact closure switch is closed.

For Raritan's floor water sensor, the normal state must be set to Normally Closed, which means no water is detected. The *alarmed* state indicates that the presence of water is detected.

Note: See the Environmental Sensors Guide or Online Help for information on setting the normal state or dip switch. This guide is available on Raritan's **Support page** *(***http://www.raritan.com/support/***).*

Tip: A contact closure sensor's LED is lit after entering the alarmed *state. Determine which contact closure switch is in the "abnormal" status according to the corresponding LED.*

"below lower critical" State

This state means a numeric sensor's reading is below the lower critical threshold as indicated below:

Reading < Lower Critical Threshold

"below lower warning" State

This state means a numeric sensor's reading is below the lower warning threshold as indicated below:

Lower Critical Threshold <= Reading < Lower Warning Threshold

---

Note: The symbol <= means smaller than (<) or equal to (=).

"above upper warning" State

This state means a numeric sensor's reading is above the upper warning threshold as indicated below:

Upper Warning Threshold <= Reading < Upper Critical Threshold

---

Note: The symbol <= means smaller than (<) or equal to (=).

"above upper critical" State

This state means a numeric sensor's reading is above the upper critical threshold as indicated below:

Upper Critical Threshold <= Reading

Note: The symbol <= means smaller than (<) or equal to (=).

States of Managed Actuators

DX sensor packages with dry contact channels allow you to connect actuators. An actuator has only three states described below. Note that an actuator is never highlighted in red or yellow regardless of the actuator states.

- unavailable: The communication with the actuator is lost.
- On: The actuator has been turned on.
- Off: The actuator has been turned off.

States of Unmanaged Sensors or Actuators

All sensors or actuators that are physically connected to the PX while NOT under management always show the following state:

- unmanaged

Note: For firmware versions prior to 3.2.1, unmanaged sensors or actuators show the state "unavailable."

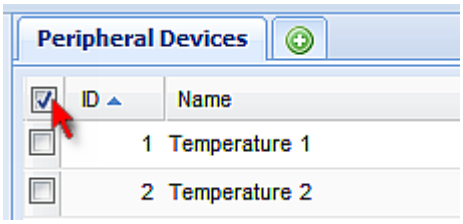
Unmanaging Environmental Sensors or Actuators

When it is unnecessary to monitor a particular environmental factor, you can unmanage or release the corresponding environmental sensor so that the PX device stops retrieving the sensor's reading and/or state. This procedure also applies if you want to unmanage an actuator.

To release a managed sensor or actuator:

1. Click Peripheral Devices in the left pane.
2. Select the checkbox of the desired sensor or actuator on the Peripheral Devices page. To release multiple ones, select multiple checkboxes.
   - To select all of those listed on the Peripheral Devices page, simply select the checkbox in the header row.

Note: If the desired action cannot be performed on any of the selected sensors or actuators, that action becomes unavailable. Deselect the inapplicable ones to perform the action.



3. Click Release.

After a sensor or actuator is removed from management:

- The ID number assigned to it is released, and can be automatically assigned to any newly-detected sensor or actuator if the Auto Management feature has been enabled. See ***Disabling the Automatic Management Function*** (on page 312).
- If it is no longer connected to the PX, it disappears from the sensor list on the Peripheral Devices page.
- If it remains connected, it continues to be listed on the Peripheral Devices page but its state is changed to *unmanaged*. See ***States of Unmanaged Sensors or Actuators*** (on page 311).

Disabling the Automatic Management Function

The factory default is to enable the automatic management feature for environmental sensors and actuators. Therefore, when the total number of managed sensors and actuators has not reached 32 yet, the PX automatically brings newly-connected environmental sensors and actuators under management after detecting them.

When this feature is disabled, the PX no longer automatically manages any newly-detected environmental sensors and actuators, and therefore neither ID numbers are assigned nor sensor readings or states are available for newly-added ones.

To disable the automatic management feature:

1. Click the PDU folder.

Note: The folder is named "my PX" by default. The name can be customized. See **Naming the PDU** *(on page 130).*

2. Click Setup in the Settings section. The Pdu Setup dialog appears.
3. Deselect the Peripheral Device Auto Management checkbox.
4. Click OK.

Controlling Actuators

If you have any DX sensor packages with actuators connected, which can move or control a mechanism or system, you can remotely turn on or off the actuators to control the connected mechanism or system.

To turn on or off an individual actuator:

1. Expand the Peripheral Devices folder in the left pane to show a list of environmental sensors and/or actuators.
2. Click the desired actuator from the navigation tree. That actuator's page opens in the right pane.
3. Click "Switch on" to turn on the actuator, or "Switch off" to turn it off.

To turn on or off multiple actuators:

1. Click Peripheral Devices in the left pane.
2. Select the checkboxes of the desired actuators on the Peripheral Devices page.

   Tip: An actuator is indicated with the icon ✔ *displayed in the 'Actuator' column.*

3. Click "Switch on" or "Switch off" to turn on or off the selected actuators. Confirm you want to switch when prompted.

Enabling the Front Panel Actuator Control

This section applies to PX3 phase II models only. A PX3 phase I model does NOT support this feature.

You can operate the front panel buttons to turn on or off a connected actuator. By default, this function is disabled.

For information on controlling the actuators via the front panel display, see ***Peripherals*** (on page 89).

To enable the front panel actuator control feature:

1. Choose Device Settings > Security > Front Panel Permissions. The Front Panel Permissions dialog appears.
2. Select the "Peripheral actuator control" checkbox.
3. Click OK.

Asset Management

Configure the asset management settings only when an asset sensor is physically connected to the PX device.

Note: To set up an asset management system, see **Connecting Asset Management Sensors** *(on page 54).*

Configuring the Asset Sensor

The PX cannot detect how many rack units (tag ports) a connected asset management sensor supports, so you must provide this information manually.

When you add an asset management sensor, you name it.

To configure an asset sensor (asset strip):

1. Expand the Feature Port folder as needed.
2. Click the asset sensor in the left pane. The asset sensor's page opens in the right pane.

   Note: The asset sensor is named "Asset Strip 1" by default. The name changes after being customized.

   Tip: The same asset sensor's page can be also opened by clicking Feature Port in the left pane, and then double-clicking the asset sensor in the right pane.
3. Click Setup. The setup dialog for the asset sensor appears.

   Tip: You can also trigger the same dialog by clicking Asset Management in the left pane, and then clicking Asset Strip Setup or double-clicking the asset sensor in the right pane.
4. To rename the asset sensor, type a new name in the Name field.
5. In the "Number of Rack Units" field, type the total number of rack units supported by the AMS. Default is 48.
6. Here, rack units are the number of asset management tag ports on the asset management strip. For example, if the AMS has 48 asset management tag ports, it supports up to 48 rack units on a cabinet.
7. Determine how to number all rack units on the asset sensor by selecting an option in the Numbering Mode.
   - Top-Down: The rack units are numbered in the ascending order from the highest to the lowest rack unit.
   - Bottom-Up: The rack units are numbered in the descending order from the highest to the lowest rack unit.

8. In the Numbering Offset field, select the starting number. For example, if you select 3, the first rack unit is numbered 3, the second is numbered 4, the third is numbered 5, and so on until the final number.
9. Indicate how the asset sensor is mounted on the rack in the Orientation field. The rack unit that is most close to the RJ-45 connector of the asset sensor will be marked with the index number 1 in the web interface.

   For the latest version of asset sensors with a built-in tilt sensor, it is NOT necessary to configure the orientation setting manually. The PX device can detect the orientation of the asset sensors and automatically configure it.

   - Top Connector: This option indicates that the asset sensor is mounted with the RJ-45 connector located on the top.
   - Bottom Connector: This option indicates that the asset sensor is mounted with the RJ-45 connector located at the bottom. Click OK.
10. Change the LED color settings as needed. See ***Setting Asset Sensor LED Colors*** (on page 315).
11. Click OK.

Setting Asset Sensor LED Colors

Each LED on the asset sensor indicates the presence and absence of a connected asset tag by changing its color.

By default the LED color of the tag ports with tags connected is green, and the color of the tag ports without tags connected is red. You can change the default LED color settings for all tag ports on an asset sensor assembly.

This feature is accessible only by users with Administrative Privileges.

To configure all LED colors:

1. Expand the Feature Ports folder in the navigation tree.
2. Click the desired asset sensor in the left pane. The page specific to that asset sensor opens in the right pane, showing the asset sensor settings and information of all rack units (tag ports).

   Note: You can also access this dialog by double-clicking the asset sensor shown on the Dashboard page.
3. Click Setup on the asset sensor page. The setup dialog for that asset sensor appears.
4. To change the LED color denoting the presence of a tag, either click a color in the color palette or type the hexadecimal RGB value of the color in the "Color with connected Tag" field.

5. To change the LED color denoting the absence of a tag, either click a color in the color palette or type the hexadecimal RGB value of the color in the "Color without connected Tag" field.
6. Click OK.

Tip: To make a specific LED's color settings different from other LEDs, see **Configuring a Specific Rack Unit** *(on page 316).*

Configuring a Specific Rack Unit

In the PX web interface, a rack unit refers to a tag port on the asset sensor. You can name a specific rack unit, or change its LED color settings so that this LED behaves differently from others on the same asset sensor.

To configure a specific rack unit:

1. Expand the Feature Port folder as needed.
2. Click the asset sensor in the left pane. The asset sensor's page opens in the right pane.

   Note: The asset sensor is named "Asset Strip 1" by default. The name changes after being customized.

   Tip: The same asset sensor's page can be also opened by clicking Feature Port in the left pane, and then double-clicking the asset sensor in the right pane.
3. Select the rack unit whose LED settings you want to change.
4. Click Configure Rack Unit or double-click the selected rack unit. The setup dialog for the selected rack unit appears.
5. In the Name field, type a name for identifying this rack unit.
6. Select either Auto or Manual Override as this rack unit's LED mode.
   - Auto (based on Tag): This is the default setting. With this option selected, the LED follows the global LED color settings.
   - Manual Override: This option differentiates this LED's behavior. After selecting this option, you must select an LED mode and/or an LED color for the selected rack unit.

- LED Mode: Select On to have the LED stay lit, Off to have it stay off, "Slow blinking" to have it blink slowly, or "Fast blinking" to have it blink quickly.
- LED Color: If you select On, "Slow blinking" or "Fast blinking" in the LED Mode field, select an LED color by either clicking a color in the color palette or typing the hexadecimal RGB value of a color in the accompanying text box.

7. Click OK.

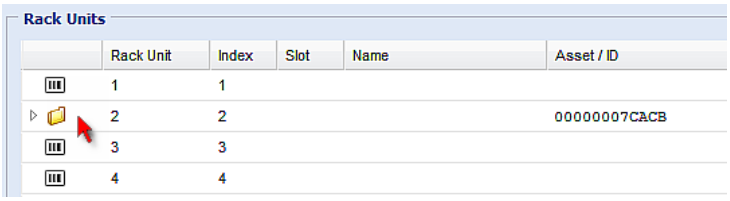
Expanding a Blade Extension Strip

A blade extension strip, like an asset sensor, has multiple tag ports. After connecting it to a specific asset sensor, it is displayed as a folder on that asset sensor's page.

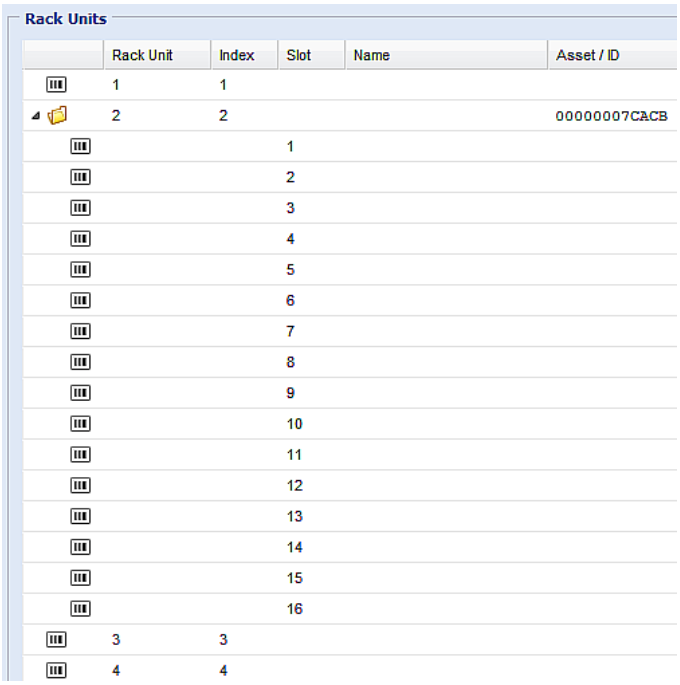
Note: If you need to temporarily disconnect the blade extension strip from the asset sensor, wait at least 1 second before re-connecting it back, or the PX device may not detect it.

To expand a blade extension strip folder:

1. Click the desired asset sensor in the left pane. The selected asset sensor's page opens in the right pane.
2. Locate the rack unit (tag port) where the blade extension strip is connected.



3. Double-click that rack unit or click the white arrow ▷ prior to the folder icon. The arrow then turns into a black, gradient arrow ◢, and all tag ports of the blade extension strip appear below the folder.



To collapse a blade extension strip:

- Double-click the blade extension strip folder, or click the black, gradient arrow ◢ prior to the folder icon. All tag ports under the folder are hidden.

Displaying the Asset Sensor Information

The hardware and software information of the connected asset sensor is available through the web interface.

To display the asset sensor information:

1. Expand the Feature Ports folder in the navigation tree.
2. Click the desired asset sensor in the left pane. The page specific to that asset sensor opens in the right pane, showing the asset sensor settings and information of all rack units (tag ports).

   Note: You can also access this dialog by double-clicking the asset sensor shown on the Dashboard page.

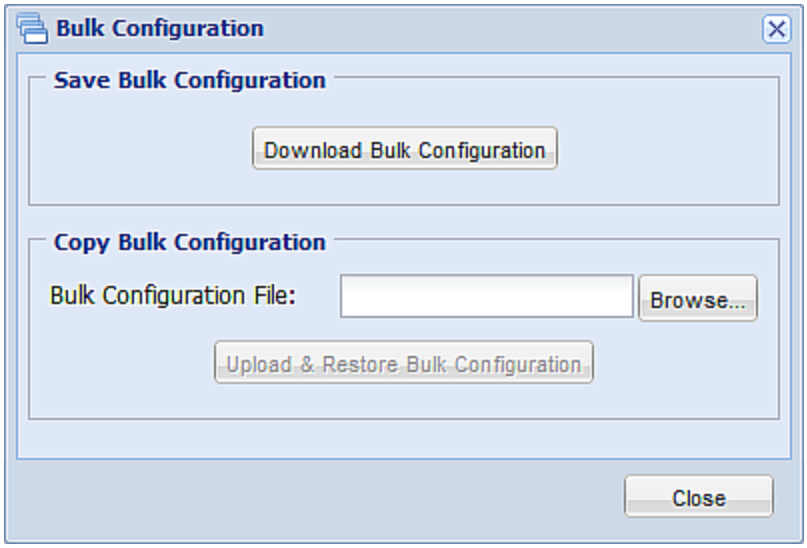
3. Click Extended Device Info, where the asset sensor data is displayed.

4. Click Close to quit the dialog.

Bulk Configuration

The Bulk Configuration feature lets you save the settings of a configured PX device to your PC. You can use this configuration file to copy that configuration to other PX devices of the same model and firmware version.

You must have the Administrator Privileges or "Unrestricted View Privileges" to save and copy the PX configurations.



Note: No device-specific data is saved to the Bulk Configuration file, such as environmental sensor or certain network settings. To back up or restore a specific PX device's all settings, use the Backup/Restore feature instead. See **Backup and Restore of PX Device Settings** *(on page 322).*

Tip: For the alternative to configure multiple PX devices, see **Bulk Configuration or Firmware Upgrade via DHCP/TFTP** *(on page 557). For the other alternative, see* **Configuration or Firmware Upgrade with a USB Drive** *(on page 546).*

Saving the PX Configuration

A source device is an already configured PX device that is used to create a configuration file containing the settings that can be shared between PX devices. These settings include user and role configurations, thresholds, event rules, security settings, and so on.

This file does NOT contain device-specific information, including:

- Device name
- System name, system contact and system location
- Network settings (IP address, gateway, netmask and so on)
- Device logs
- Outlet names
- Outlet status
- Environmental sensor and actuator names
- States and values of environmental sensors and actuators
- TLS certificate

Because the date and time settings are saved in the configuration file, users should exercise caution when distributing the configuration file to the PX devices in a different time zone than the source device.

To save a configuration file:

1. Choose Maintenance > Bulk Configuration. The Bulk Configuration dialog appears.
2. Click Download Bulk Configuration.
3. When the web browser prompts you to open or save the configuration file, click Save. Choose a suitable location and save the configuration file to your PC.

The file is saved in the XML format, and its content is encrypted using the AES-128 encryption algorithm.

Tip: You can also save a configuration file using a Secure Copy (SCP) command. See **Bulk Configuration via SCP** *(on page 584).*

Copying the PX Configuration

A target device is the PX device that loads another PX device's configuration file.

Copying a source PX device's configuration to a target device adjusts the target PX device's settings to match those of the source PX device. In order to successfully copy a source PX device's configuration:

- The user must be the Admin user. Or the Admin role is assigned to the user.
- The target PX device must be running the same firmware version as the source PX device.
- The target PX device must be of the same model type as the source PX device.

  Bulk configuration is permitted if the differences between the target and source device are only mechanical designs which are indicated in a model name's suffix as listed below. In the following list, n represents a number.

  - PDU chassis color, which is indicated as *Kn*, such as K1 and K601

  - Line cord color, which is indicated as *Bn*, such as B2 and B5

  - Line cord length (meters), which is indicated as *An*, such as A0 and A14

  - Line cord length (centimeters), which is indicated as *Ln*

  For example, Raritan's PX2-4724-E2N1K2 and PX2-4724-E2N1K9 share the same specifications, and the only difference is their chassis colors represented by K2 (blue) and K9 (gray).

To copy a PX configuration:

1. Log in to the target device's web interface.
2. If the target device's firmware version does not match that of the source device, update the target's firmware. See ***Firmware Upgrade*** (on page 341).
3. Choose Maintenance > Bulk Configuration. The Bulk Configuration dialog appears.
4. In the Copy Bulk Configuration section, click Browse to select the configuration file stored on your PC.
5. Click Upload & Restore Bulk Configuration to copy the file.

   A message appears, prompting you to confirm the operation and enter the admin password.
6. Enter the admin password, then click Yes to confirm the operation.
7. Wait until the PX device resets and the Login page re-appears, indicating that the configuration copy is complete.

Note: On startup, the PX performs all of its functions, including event rules and logs, based on the new configuration file you have selected instead of the previous configuration prior to the device reset. For example, "Bulk configuration copied" is logged only when the new configuration file contains the "Bulk configuration copied" event rule.

Tip: You can also copy a configuration file using a Secure Copy (SCP) command. See **Bulk Configuration via SCP** *(on page 584).*

Backup and Restore of PX Device Settings

Different from the Bulk Configuration file, the backup file contains device-specific data like network settings. To back up or restore PX device settings, you should perform the Backup/Restore feature.

All PX information is captured in the XML backup file except for the device logs and TLS certificate.

Note: To perform the bulk configuration among multiple PX devices, perform the Bulk Configuration feature instead. See **Bulk Configuration** *(on page 319).*

To download a backup PX XML file:

1. Choose Maintenance > Backup/Restore. The Backup/Restore of Device Settings dialog opens.
2. In the Save Device Settings section, click Download Device Settings. Save the file to your computer.

   The file is saved in the XML format, and its content is encrypted using the AES-128 encryption algorithm.

To restore the PX using a backup XML file:

1. Choose Maintenance > Backup/Restore. The Backup/Restore of Device Settings dialog opens.
2. In the Copy Device Settings section, click Browse to locate the file.
3. Click Upload & Restore Device Settings to upload the file.

   A message appears, prompting you to confirm the operation and enter the admin password.
4. Enter the admin password, then click Yes to confirm the operation.
5. Wait until the PX device resets and the Login page re-appears, indicating that the restore is complete.

Note: On startup, the PX performs all of its functions, including event rules and logs, based on the new configuration file you have selected instead of the previous configuration prior to the device reset. For example, "Bulk configuration copied" is logged only when the new configuration file contains the "Bulk configuration copied" event rule.

Tip: You can also back up and restore a configuration file using a Secure Copy (SCP) command. See **Backup and Restore via SCP** *(on page 585).*

Webcam Management

With a Logitech® webcam connected to the PX device, you can visually monitor the environment around the PX via snapshots or videos captured by the webcam.

- To view snapshots and videos, you need the permission of either "Change Webcam Configuration" or "View Webcam Sanpshots and Configuration."
- To configure webcam settings, you need the "Change Webcam Configuration" permission.

For more information on the Logitech webcam, see the user documentation accompanying it. For information on connecting a webcam to the PX, see ***Connecting a Logitech Webcam*** (on page 63).

You can manually store snapshots taken from the webcam onto the PX or a remote server. See ***Saving Snapshots*** (on page 329) or ***Configuring Webcam Storage*** (on page 331).

Links to snapshots or videos being captured by a webcam can be sent via email or instant message. See ***Sending Snapshots or Videos in an Email or Instant Message*** (on page 327).

Events that trigger emails containing snapshots from a webcam can be created. See ***Creating Actions*** (on page 237).

Configuring Webcams

Before you can configure a webcam, it must be connected to the PX. See ***Connecting a Logitech Webcam*** (on page 63).

To configure a webcam:

1. In the navigation tree, click on the Webcam Management folder. The Webcam Management page opens.
2. Click on the webcam you want to configure and then click Setup at the bottom right of page. The Webcam Setup dialog opens.
3. Enter a name for the webcam. Up to 64 characters are supported.

4. Type the location information in each location field if needed. Up to 63 characters are supported.
5. Select a resolution for the webcam.
   - If you connect two webcams to one USB-A port using a powered USB hub, set the resolution to 352x288 or lower for optimal performance.
6. Select the webcam mode. This can be changed as needed once the webcam is configured.
   a. Video - the webcam is in video mode. Set the Framerate (frames per second) rate.
   b. Snapshot - the webcam displays images from the webcam. Set the "Time between Snapshots" rate as measured in seconds.
7. Click OK. The image or video from the webcam is now available in the PX once you click on the webcam in the navigation tree.

To edit a webcam configuration:

1. In the navigation tree, click on the Webcam Management folder. The Webcam Management page opens.
2. Double-click on the webcam you want to edit. The webcam image or video opens in a new tab.
3. Click Setup .
4. Edit the information as needed. Changes to the resolution do not apply to existing, stored images - it applies only to images and videos taken after the resolution is changed.
5. Click OK.

Adjusting Image Properties

If any snapshot or video properties, such as the brightness, contrast, saturation, and gain settings, do not satisfy your needs, adjust them.

To adjust the image or video properties:

1. Select the webcam shown on the Webcam Management page or in the navigation tree. See ***Configuring Webcams*** (on page 323).
2. Click Setup or .
3. Click the Controls tab.
4. Adjust the desired property by adjusting the corresponding slide bar.

   Or click "Set to webcam defaults" to restore all settings to this webcam's factory defaults.
5. Click OK.

Viewing Webcam Snapshots or Videos

You can switch between snapshots or live videos being captured by a webcam.

The snapshot or video is displayed either in the PX web interface or in a Primary Standalone Live Preview window that you open.

You can open a maximum of five Primary Standalone Live Preview windows.

Note: For remote Live Preview sessions, such as those accessed via a link in an email or instant message, a total of up to three (3) simultaneous Live Preview sessions are supported at a time. One (1) from the originator in the PX interface, and up to two (2) remote sessions. See **Sending Snapshots or Videos in an Email or Instant Message** *(on page 327).*

To switch between snapshot and video modes:

1. Click the desired webcam's icon in the navigation tree.

   Snapshots or videos captured by the webcam are displayed in the right pane of the PX web interface once a webcam is selected in the navigation tree.

   Snapshots and videos can also be displayed in Live Preview mode in the Primary Standalone Live Preview window by clicking on the Live Preview icon .

   Note: All Live Preview sessions sharing the same URL, including one Primary Standalone Live Preview window and two associated remote sessions, are identified as one single "<webcam>" user in the Connected Users dialog. You can disconnect a "<webcam>" user from this dialog to terminate a specific Primary Standalone Live Preview window and all of its remote sessions. See **Viewing Connected Users** *(on page 290).*

2. By default the PX enters the snapshot mode. Wait around one minute for the snapshot to appear.

   In the snapshot mode, three pieces of information are displayed on the top of the image:

   - A snapshot mode icon .
   - The interval time between snapshots (in seconds).
   - A time stamp.

   The webcam's location information, if available, is displayed in the Location pane of the PX web interface.

- To change any image settings, click Setup . See ***Configuring Webcams*** (on page 323) or ***Adjusting Image Properties*** (on page 324).
- To save the snapshot being displayed, click the "Store Snapshot to Webcam Storage" icon . See ***Saving Snapshots*** (on page 329).

3. To switch to the video mode, click Setup and select Video in the Webcam Mode field.

   In the video mode, two pieces of information are displayed on the top of the image:

   - A video mode icon .
   - The number of frames to take per second (fps).

   To change any video settings, click Setup .

4. To return to the snapshot mode, repeat the above step and select Snapshot.

Sending Snapshots or Videos in an Email or Instant Message

Whenever you open a Primary Standalone Live Preview window, a unique URL is generated for this window session, which permits a link to the snapshot or video being captured.

You are able to email or instant message up to two (2) recipients a link to webcams attached to the PX. Users can then click on the links and view snapshots or videos.

A total of three sessions based on the same URL are supported, including a Primary Standalone Live Preview window of the sender and two remote sessions of the recipients.

Note: All Live Preview sessions sharing the same URL, including one Primary Standalone Live Preview window and two associated remote sessions, are identified as one single "<webcam>" user in the Connected Users dialog. You can disconnect a "<webcam>" user from this dialog to terminate a specific Primary Standalone Live Preview window and all of its remote sessions. See **Viewing Connected Users** *(on page 290).*

For explanation of this topic, the message sender is User A and the recipient is User B.

The recipient is able to access the snapshot or video image via the link in any of the following scenarios:

- The snapshot or video remains open in the Primary Standalone Live Preview window in User A's side. If so, even though User A logs out of the PX interface or the login session times out, the link is available.

  Or

- At least a remote session based on the same URL remains open. If so, even though User A has closed the Primary Standalone Live Preview window, the link is available.

  Or

- Neither the Primary Standalone Live Preview window nor any remote session based on the same URL remains open, but the idle timeout period has not expired yet since the last Live Preview window session was closed. For information on idle timeout, see ***Enabling Login Limitations*** (on page 185).

Tip: If the idle timeout has not expired, the <webcam> user for that Live Preview URL remains shown in the Connected Users dialog.

Best Practice

As a best practice, User A should open the snapshot or video using a Primary Standalone Live Preview window and leave that window open at least until User B opens the snapshot or video via the link.

Once User B opens the snapshot or video via the link, User A can close the Primary Standalone Live Preview window.

User B should let User A know that the link has been opened.

To send a snapshot or video link via email or instant message:

1. In the navigation tree, click on the webcam that is capturing the snapshot or video you want to provide a link to other people. The snapshot or video is displayed in Live Preview mode in the right pane.
2. Click on the Live Preview icon located above the snapshot or video. The snapshot or video opens in a standalone Live Preview window.
3. Copy the URL from the Live Preview window, paste it into the email or instant message application. Leave the Live Preview window open at least until the recipient opens the snapshot or video via the link.

Snapshot Storage

Once a snapshot is taken using the Store Snapshot to Webcam Storage feature, it is stored locally on the PX by default. Up to ten (10) images can be stored on the PX at once.

To save more than 10 snapshots, save the images on a Common Internet File System/Samba.

Note: NFS and FTP are not supported for this release and are disabled on the dialog.

Snapshot files are saved as JPG files. The snapshot file is named based on the number of the snapshot starting from 1. So the first snapshot that is taken is named 1.jpg, the second is 2.jpg and so on.

Unless snapshots are deleted manually, the oldest snapshot is automatically deleted from the device when the number of snapshots exceeds ten. Rebooting the PX deletes all webcam snapshots that are saved on the device.

Saving Snapshots

If it is intended to keep the snapshot being displayed on the webcam, you can manually save it onto the PX. A snapshot is saved as a JPEG file and stored on the Snapshots page.

Warning: The snapshots stored on the PX are cleared when rebooting the PX. Check the importance of the snapshots before performing the reset.

To save the snapshot being displayed:

1. In the navigation tree, click on the webcam you want to take a snapshot with. The webcam image is displayed in the right pane.

   The webcam must be in snapshot mode in order to take snapshots. If the webcam is in video mode, click Setup in the right pane above the video image to open the Webcam Setup dialog, then select the Snapshot radio button.

2. Once the snapshot image being taken by the selected webcam is displayed in the right pane, click the Store Snapshot to Webcam Storage icon above the image to take a snapshot. Up to ten (10) snapshots can be stored at once on the device.

3. Click on the Snapshots icon in the navigation tree to verify that those snapshots are successfully saved and listed on the Snapshots page.

Tip: To store snapshots on a remote server rather than the PX, see **Configuring Webcam Storage** *(on page 331).*

Managing the Snapshots Saved to PX

A maximum of 10 saved snapshots can be stored and displayed on the Snapshots page of the PX.

See ***Saving Snapshots*** (on page 329) for instructions on storing snapshots on the PX.

The Snapshots page is categorized into three sections: Storage, Snapshot and Details.

- Storage: shows a list of all saved snapshots.

  On the top of the Storage section, the number following "Used" indicates the total of saved snapshots and the number following "Size" indicates maximum number of snapshots allowed in storage.
- Snapshot: displays the image of the snapshot being selected.
- Details: shows the information which had been entered when the snapshot was saved, including resolution and location settings.

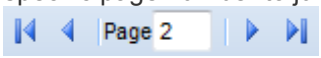
Tip: To save more than 10 snapshots, save snapshots onto a remote server. See **Configuring Webcam Storage** *(on page 331).*

To view the saved snapshots:

1. In the navigation tree, click Snapshots under the Webcam Management folder. The snapshots are displayed in the right pane in the Storage section of the page.
2. View an individual snapshot by clicking on a snapshot file in the Storage section of the page.

   The size of each snapshot file, the date and time each snapshot was taken, and the webcam that took each snapshot, is displayed when viewing snapshots.

   Details, such as the webcam location and/or labels, if any, are displayed in the Details section below the snapshot in the right pane. This information is defined when the webcam is initially configured. See ***Configuring Webcams*** (on page 323).
3. Use the navigation icons to move through each snapshot, or enter a specific page number to jump to that snapshot page.

4. Click the Refresh icon to refresh the page. New snapshots are displayed if they are available.

To delete any snapshot from the storage:

- Delete snapshots by selecting the checkbox next to the snapshot you want to delete, then clicking the Delete icon at the top of the section. To select and delete all snapshots at once, click the checkbox in the checkbox column header, then click the Delete icon.

Configuring Webcam Storage

Once a snapshot is taken using the Store Snapshot to Webcam Storage feature, it is stored locally on the PX by default. Up to ten (10) images can be stored on the PX at once.

To save more than 10 snapshots, save the images on a Common Internet File System/Samba.

Note: NFS and FTP are not supported for this release and are disabled on the dialog.

Snapshot files are saved as JPG files. The snapshot file is named based on the number of the snapshot starting from 1. So the first snapshot that is taken is named 1.jpg, the second is 2.jpg and so on.

Unless snapshots are deleted manually, the oldest snapshot is automatically deleted from the device when the number of snapshots exceeds ten. Rebooting the PX deletes all webcam snapshots that are saved on the device.

To configure another storage location for images:

1. In the navigation tree, click Snapshots under the Webcam Management folder. The Snapshots page opens.
2. Click on the Setup Storage icon . The Storage Setup dialog opens.
3. By default, Local, meaning the PX, is the designated default storage.
4. Select CIFS/Samba as the storage location.
5. Enter the server where to store the images.
6. If needed, enter the share drive/folder to store the images in.
7. Enter the username and password needed to access the server where the images are stored.
8. Enter or use the slide bar to set the number of images that can be saved to the storage location.
9. Click OK.

Network Diagnostics

The PX provides the following tools in the web interface for diagnosing potential networking issues.

- Ping
- Trace Route
- List TCP Connections

Tip: These network diagnostic tools are also available through CLI. See **Network Troubleshooting** *(on page 522).*

Pinging a Host

The Ping tool is useful for checking whether a host is accessible through the network or Internet.

To ping a host:

1. Choose Maintenance > Network Diagnostics > Ping. The Ping Network Host dialog appears.
2. In the Host Name field, type the name or IP address of the host that you want to check.
3. In the Number of Requests field, type a number up to 20 or adjust the value by clicking either arrow. This number determines how many packets are sent for pinging the host.
4. Click Run Ping to start pinging the host. A dialog appears, displaying the Ping results.
5. Click Close to quit the dialog.

Tracing the Network Route

Trace Route lets you find out the route over the network between two hosts or systems.

To trace the route for a host:

1. Choose Maintenance > Network Diagnostics > Trace Route. The "Trace Route to Host" dialog appears.
2. Type the IP address or name of the host whose route you want to check in the Host Name field.
3. In the Timeout (s) field, type a timeout value in seconds to end the trace route operation. Note that if the timeout value is too small, the trace route results may be incomplete.

4. To use the Internet Control Message Protocol (ICMP) packets to perform the trace route command, select the Use ICMP Packets checkbox.
5. Click Run. A dialog appears, displaying the Trace Route results.

Listing TCP Connections

You can use the "List TCP Connections" to display a list of TCP connections.

To list TCP connections:

1. Choose Maintenance > Network Diagnostics > List TCP Connections. The TCP Connections window appears.
2. Click Close to quit the dialog.

Downloading Diagnostic Information

Important: This function is for use by Raritan Field Engineers or when you are directed by Raritan Technical Support.

You can download the diagnostic file from the PX device to a client machine. The file is compressed into a .tgz file and should be sent to Raritan Technical Support for interpretation.

This feature is accessible only by users with Administrative Privileges or "Unrestricted View Privileges."

To retrieve a diagnostic file:

1. Choose Maintenance > Download Diagnostic Information. You are then prompted to save or open the file.
2. Click Save to save the file.
3. E-mail this file as instructed by Raritan Technical Support.

Managing the Schroff LHX/SHX Heat Exchanger

The PX supports monitoring and administering the Schroff® LHX-20, LHX-40 and SHX-30 heat exchanger if this device is connected to the PX.

From the PX, you can do the following remotely:

- Name a connected LHX heat exchanger
- Monitor LHX sensors and operational states
- Configure the air outlet temperature setpoint
- Configure the default fan speed
- Configure sensor thresholds (for alert generation)
- Request maximum cooling using the fan speed and opening the cold water valve
- Acknowledge alerts remotely (for example, return to normal operation after maximum cooling is requested)

The exact information is dependent on your Schroff model. See your Schroff LHX/SHX manual for details on each device's settings and features.

To monitor one LHX/SHX heat exchanger using the PX:

1. Connect an LHX-20, LHX-40 or SHX-30 heat exchanger to the PX if it is not connected yet. See ***Connecting a Schroff LHX/SHX Heat Exchanger*** (on page 65).
2. Enable the support of LHX/SHX heat exchanger on the PX. See ***Enabling and Disabling Schroff LHX/SHX Heat Exchanger Support*** (on page 335).
3. Configure the connected heat exchanger. See ***Configuring the LHX/SHX*** (on page 335).
4. Now you can remotely monitor or control the connected LHX/SHX heat exchanger via the PX.
   - To monitor the heat exchanger, see ***Monitoring the LHX/SHX*** (on page 337).
   - To control the heat exchanger, see ***Turning the LHX/SHX On or Off*** (on page 340).

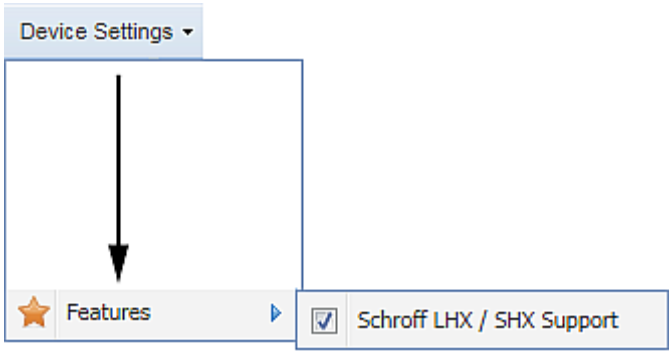
Enabling and Disabling Schroff LHX/SHX Heat Exchanger Support

By default, Schroff LHX/SHX Heat Exchanger support is disabled. As such, support needs to be enabled before the device appears in the navigation tree or on the dashboard.

Additionally, Schroff LHX/SHX Heat Exchanger support must be enabled in order for the LHX-MIB to be accessible through SNMP.

To enable the Schroff LHX/SHX Heat Exchanger:

1. Select Device Settings > Features, and then select the Schroff LHX/SHX Support checkbox.



2. Click Yes to confirm.
3. Reboot the PX.

Configuring the LHX/SHX

After enabling the LHX/SHX support on the PX, the PX should automatically detect the connected LHX/SHX device and display it under the Feature Port folder.

If the LHX/SHX device does not display, this is because the port is not set to Auto mode. Change the mode so that the LHX/SHX device is correctly displayed in the web interface. See ***Configuring the Feature Port*** (on page 151).

After this device is displayed, you can set LHX/SHX temperature or fan speed thresholds for alerts or to customize the name of the LHX/SHX device for easy identification.

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

Setting Up an LHX/SHX

Once a Schroff LHX/SHX heat exchanger is connected, you can set up the device by giving it a name, and configure its setpoint air outlet and default fan speed.

To set up the LHX/SHX:

1. Expand the Feature Port folder as needed.
2. Click the desired LHX/SHX device. Its page opens in the right pane.
3. Click Setup in the Settings section of the page. The Setup dialog opens.
4. Type a name for the heat exchanger in the Name field. The customized LHX/SHX heat exchanger's name is followed by the device type in parentheses.
5. Enter the air outlet's temperature set point in the Setpoint Air Outlet (°C) field.
6. Enter the default fan speed in the Default Fan Speed (%) field.
7. Click OK.

Configuring Temperature and Fan Thresholds

An LHX/SHX heat exchanger is implemented with various sensors for detecting the air temperature, water temperature, and fan speed.

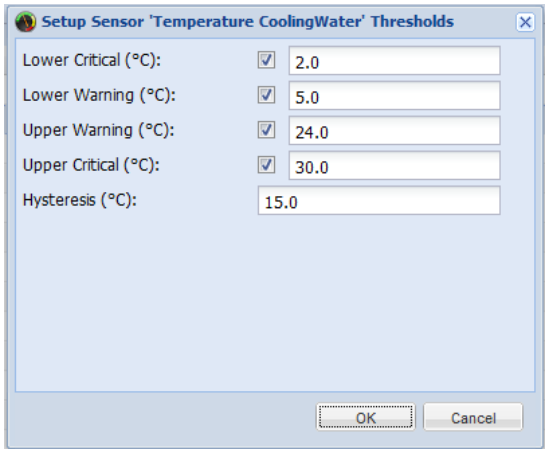
You can set thresholds for these sensors so that the PX alerts you when any sensor readings are getting close to a critical condition.

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

To configure the thresholds for a sensor:

1. Expand the Feature Port folder as needed.
2. Click the desired LHX/SHX device. Its page opens in the right pane.

3. Select the desired sensor in the Sensors table and click Setup Thresholds, or double-click that sensor. The setup dialog for the selected sensor appears.



4. Adjust the threshold and deassertion hysteresis settings. The Upper Critical and Lower Critical values are points at which the PX considers the operating environment critical and outside the range of the acceptable threshold.
   - To enable any threshold, select the corresponding checkbox. To disable a threshold, deselect the checkbox.
   - After any threshold is enabled, type an appropriate numeric value in the accompanying text box.
   - To set the deassertion hysteresis, type a numeric value in the Deassertion Hysteresis field. See ***"To De-assert" and Deassertion Hysteresis*** (on page 672).
   - To set the assertion timeout, type a numeric value in the Assertion Timeout (samples) field. See ***"To Assert" and Assertion Timeout*** (on page 670).
5. Click OK.

Monitoring the LHX/SHX

The PX web interface lets you monitor the status of the connected LHX/SHX heat exchanger as well as the status of LHX/SHX built-in sensors.

Viewing the Summary

Both the Dashboard and Feature Port pages display the summary of the connected LHX/SHX heat exchanger, including the heat exchanger's name and status.

If an LHX/SHX is highlighted in red in the summary, it indicates that there is LHX/SHX sensor failure on that heat exchanger. View the State column to identify failed sensors.

LHX/SHX summary on the Dashboard page:

1. Click the Dashboard icon in the PX Explorer pane, and the Dashboard page opens in the right pane.
2. Locate the LHX/SHX Heat Exchanger section where the LHX/SHX summary is shown.

LHX/SHX summary on the Feature Port page:

- Click the Feature Port folder in the PX Explorer pane.

  The port page opens in the right pane, showing the LHX/SHX summary.

Viewing Details

An LHX/SHX heat exchanger page shows detailed information, including:

- Device information and settings, such as the LHX/SHX device name
- The air outlet temperature
- The default fan speed
- Readings and states of all LHX/SHX built-in sensors
- Alerts and errors, such as failed LHX/SHX sensors or emergency cooling activation
- Accumulative operating hours

If any LHX/SHX sensor enters the critical or warning level, that sensor row is highlighted in red or yellow. See ***The Yellow- or Red-Highlighted Sensors*** (on page 119).

In addition, SHX-30 models indicate the number of power supplies present and if a condenser pump is present, since those options are supported by the SHX-30.

To view details of a specific LHX/SHX heat exchanger:

1. Expand the Feature Port folder as needed.
2. Click the desired LHX/SHX device. Its page opens in the right pane.

Device States and Icon Variations

The PX web interface changes icons to represent different statuses of the connected LHX/SHX heat exchanger.

Icons	Device status
	The heat exchanger is turned ON and operating normally.
	The heat exchanger is turned OFF.
	The heat exchanger is turned ON but enters the critical state because of any LHX/SHX sensor failure.
	At least one of the LHX/SHX sensor readings has entered the warning range.
	NO LHX/SHX device is detected on the specific port.

To identify the cause of a critical state, refer to:

- ***Viewing the Summary*** (on page 338)
- ***Alert States and LHX Event Log*** (on page 339)

Alert States and LHX Event Log

Remote Alert Acknowledgment is supported by the LHX-20 and LHX-40. The SHX-30 does not support Remote Alert Acknowledgment.

When an LHX heat exchanger is physically connected to the PX device, a section labeled Alert States appears on its device page.

The Alert States section contains information identifying the LHX sensors that currently fail.

A button labeled Show Event Log is located in the Alert States section. To view LHX events associated with the PX, click this button.

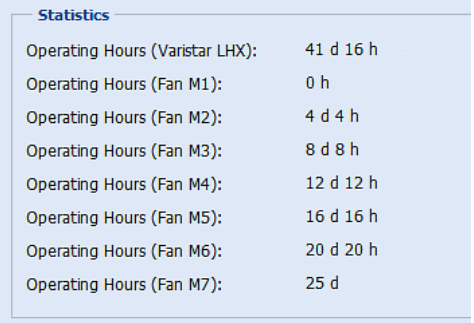
Note: To view the event log for an SHX-30, click Maintenance > View Event Log.

Tip: The Dashboard and Feature Port pages also point out failed sensors. See **Viewing the Summary** *(on page 338).*

Operating Hours

Operating hours are the accumulative time since the LHX/SHX heat exchanger is first connected to the PX device and turned ON.

The PX web interface displays the operating hours both for the heat exchanger and its fans. Operating hour information is located in the Statistics section of each heat exchanger page.



Below are the time units used for operating hours:

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

For example, "3d 5h" means the total operating time is 3 days and 5 hours.

Turning the LHX/SHX On or Off

The PX allows you to remotely turn on or off a connected heat exchanger.

▶ **To control the LHX/SHX heat exchanger:**

1. Expand the Feature Port folder as needed.
2. Click the desired LHX/SHX device. Its page opens in the right pane.

   In the Information section, click either Switch Off or Switch On.
3. If you clicked Switch Off, a dialog appears, prompting you to confirm the operation. Click Yes to turn it off or No to abort the operation.

The heat exchanger's icon changes after being turned on or off. See ***Device States and Icon Variations*** (on page 339).

Requesting Maximum Cooling for an SHX-30

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

When you click Request Maximum Cooling on the PX web interface, the SHX-30 enters into emergency cooling mode and runs at its maximum cooling level of 100% in order to cool the device.

When maximum cooling is requested for an SHX-30, the message "Maximum cooling requested" is displayed in the Alerts section of the page.

For additional information on the SHX-30 maximum cooling feature, see the SHX-30 documentation.

To request maximum cooling for an SHX-30:

1. Expand the Feature Port folder as needed.
2. Click the desired SHX-30 device. Its page opens in the right pane.
3. In the Information section of the page, click Request Maximum Cooling to cool the device. The maximum cooling process begins.
4. Click Cancel Maximum Cooling to stop the process (if needed).

Firmware Upgrade

You may upgrade your PX device to benefit from the latest enhancements, improvements and features.

Firmware files are available on Raritan website's ***Support page*** (***http://www.raritan.com/support/***).

Updating the PX Firmware

When performing the firmware upgrade, the PX keeps each outlet's power status unchanged so no server operation is interrupted. Outlets that have been powered on prior to the firmware upgrade remain powered on and outlets that have been powered off remain powered off during and after the firmware upgrade.

You must be the system administrator or log in to the user profile with the Firmware Update permission to update the PX firmware.

Before starting the upgrade, read the release notes downloaded from the Raritan website's ***Support page*** (***http://www.raritan.com/support/***). If you have any questions or concerns about the upgrade, contact Raritan Technical Support BEFORE upgrading.

On a multi-inlet PDU (any model with X2 or X3 suffixes), all inlets must be connected to the power source for the PDU to successfully upgrade its firmware.

Warning: Do NOT perform the firmware upgrade over a wireless network connection.

Firmware Update via Web Interface

After downloading the latest firmware, log in to the PX web interface to upgrade the firmware.

To update the firmware:

1. Choose Maintenance > Update Firmware. The Update Firmware dialog appears.
2. In the Firmware File field, click Browse to select an appropriate firmware file.
3. Click Upload. A progress bar appears to indicate the upload status.
4. When the upload is complete, version information of both the existing firmware and uploaded firmware is shown, providing you a last chance to terminate the update.
5. To view the certificate of the uploaded firmware, click View Certificate. **Optional.**
6. To proceed with the update, click Update Firmware. The update may take several minutes.

   Warning: Do NOT power off the PX during the update.

   During the firmware update:

- A progress bar appears in the web interface, indicating the update status.
- The front panel display on the PX shows three digits: 'FuP' or 'FUP.'

Exception: A PX3 Phase II model shows the upgrade progress in percent instead of FUP on its LCD display.

- The outlet LEDs flash when the relay boards are being updated.

Exception: If the firmware update does not include the update of the relay board firmware, outlet LEDs do NOT flash.

- No users can successfully log in to the PX.
- The user management operation, if any, is forced to suspend.

7. When the update is complete, a message appears, indicating the update is successful.
8. The PX resets, and the Login page re-appears. You can now log in and resume your operation.

Note 1: The other logged-in users are also logged out when the firmware update is complete.

Note 2: If you are using the PX 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 348) in the User Guide.*

Tip: There are other alternatives to update the firmware. See **Firmware Update via SCP** *(on page 583), and* **Bulk Configuration or Firmware Upgrade via DHCP/TFTP** *(on page 557). Or see* **Firmware Upgrade via USB** *(on page 556).*

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 PX web-interface-based upgrades. Upgrades through other management systems, such as Raritan'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.

Viewing Firmware Update History

The firmware upgrade history, if available, is permanently stored on the PX device.

This history indicates when a firmware upgrade event occurred, the prior and new versions associated with the firmware upgrade event, and the upgrade result.

To view the firmware update history:

1. Choose Maintenance > View Firmware Update History. The Firmware Update History dialog appears, with the following information displayed.
   - Date and time of the firmware upgrade event
   - Previous firmware version
   - Update firmware version
   - Firmware upgrade result
2. You may change the number of displayed columns or re-sort the list for better viewing the data.
3. To view the details of any firmware upgrade event, select it and click Details, or simply double-click the event. The Firmware Update Details dialog appears, showing detailed information of the selected event.
4. Click Close to quit the dialog.

Full Disaster Recovery

If the firmware upgrade fails, causing the PX device to stop working, you can recover it by using a special utility rather than returning the device to Raritan.

Contact Raritan Technical Support for the recovery utility, which works in Windows XP/Vista/7 and Linux. In addition, an appropriate PX firmware file is required in the recovery procedure.

Updating the Asset Sensor Firmware

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

During the firmware upgrade, the following events take place:

- The asset sensor is completely lit up, with the blinking LEDs changing the color from red to green.
- A firmware upgrade process is indicated in the PX web interface.
- An SNMP trap is sent to indicate the firmware upgrade event.

Accessing the Help

The Help menu provides:

- Current firmware and software packages information
- A link to the PX help

Retrieving Software Packages Information

You can check the current firmware version and the information of all open source packages embedded in the PX device through the web interface.

To retrieve the embedded software packages information:

1. Choose Help > About PX iPDU. The About PX iPDU dialog appears, with a list of open source packages displayed.
2. You can click any link in the dialog to access related information or download any software package.

Browsing through the Online Help

The PX Online Help is accessible over the Internet.

To use online help, Active Content must be enabled in your browser. If you are using Internet Explorer 7, you must enable Scriplets. Consult your browser help for information on enabling these features.

To use the PX online help:

1. Choose Help > User Guide. The online help opens in the default web browser.
2. To view the content of any topic, click the topic in the left pane. Then its content is displayed in the right pane.
3. To select a different topic, do any of the following:
   - To view the next topic, click the Next icon in the toolbar.
   - To view the previous topic, click the Previous icon.
   - To view the first topic, click the Home icon.
4. To expand or collapse a topic that contains sub-topics, do the following:
   - To expand any topic, click the white arrow prior to the topic, or double-click that topic. The arrow turns into a black, gradient arrow, and sub-topics appear below the topic.
   - To collapse any expanded topic, click the black, gradient arrow prior to the topic, or double-click the expanded topic. The arrow then turns into a white arrow, and all sub-topics below that topic disappear.
5. To search for specific information, type the key word(s) or string(s) in the Search text box, and press Enter or click the Search icon to start the search.
   - If necessary, select the "Match partial words" checkbox to include information matching part of the words entered in the Search text box.

   The search results are displayed in the left pane.
6. To have the left pane show the list of topics, click the Contents tab at the bottom.
7. To show the Index page, click the Index tab.
8. To email any URL link to the currently selected topic to any person, click the "Email this page" icon in the toolbar.
9. To email your comments or suggestions regarding the online help to Raritan, click the "Send feedback" icon.

10. To print the currently selected topic, click the "Print this page" icon .

Chapter 7 Using SNMP

This SNMP section helps you set up the PX for use with an SNMP manager. The PX can be configured to send traps or informs to an SNMP manager, as well as receive GET and SET commands in order to retrieve status and configure some basic settings.

In This Chapter

Enabling SNMP 348
Configuring Users for Encrypted SNMP v3 349
Configuring SNMP Notifications 350
SNMP Gets and Sets 355

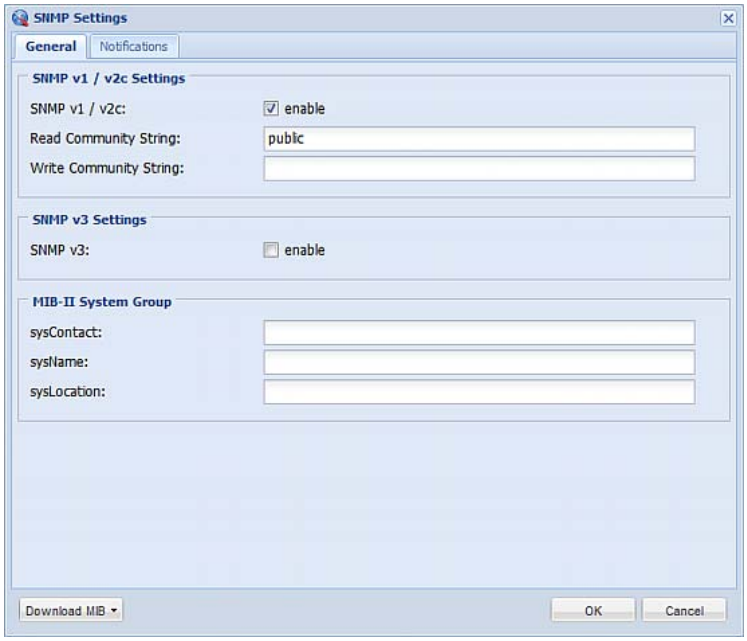
Enabling SNMP

By default, SNMP v1/v2c is enabled on the PX so the PX can communicate with an SNMP manager. If you have disabled the SNMP, it must be enabled to communicate with an SNMP manager.

Note that read-only access is enabled and the community string is public.

To enable SNMP:

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



2. Select the "enable" checkbox in the "SNMP v1 / v2c" field to enable communication with an SNMP manager using SNMP v1 or v2c protocol.
   - Type the SNMP read-only community string in the Read Community String field. Usually the string is "public."
   - Type the read/write community string in the Write Community String field. Usually the string is "private."
3. Select the "enable" checkbox in the "SNMP v3" field to enable communication with an SNMP manager using SNMP v3 protocol.

   Tip: You can permit or disallow a user to access the PX via the SNMP v3 protocol. See **Configuring Users for Encrypted SNMP v3** *(on page 349).*
4. Enter the MIB-II system group information, if applicable:
   a. sysContact - the contact person in charge of the system
   b. sysName - the name assigned to the system
   c. sysLocation - the location of the system
5. Select the MIB to be downloaded. The SNMP MIB for your PX is used by the SNMP manager.

   Important: You must download the SNMP MIB for your PX to use with your SNMP manager. Click Download MIB in this dialog to download the desired MIB file. For details, see **Downloading SNMP MIB** *(on page 356).*
6. Click OK.

Configuring Users for Encrypted SNMP v3

The SNMP v3 protocol allows for encrypted communication. To take advantage of this, users need to have an Authentication Pass Phrase and Privacy Pass Phrase, which act as shared secrets between them and the PX.

To configure users for SNMP v3 encrypted communication:

1. Choose User Management > Users. The Manage Users dialog appears.
2. Select the user by clicking it.
3. Click Edit or double-click the user. The Edit User 'XXX' dialog appears, where XXX is the user name.
4. To change the SNMPv3 access permissions, click the SNMPv3 tab and make necessary changes. For details, see Step 6 of ***Creating a User Profile*** (on page 168).

5. Click OK. The user is now set up for encrypted SNMP v3 communication.

Configuring SNMP Notifications

The PX automatically keeps an internal log of events that occur. See ***Event Rules and Actions*** (on page 236). These events can also be used to send SNMP v2c or v3 notifications to a third-party destination.

The PX provides you with the ability to create SNMPv2c and SNMPv3 TRAP communications, or SNMPv2c and SNMPv3 INFORM communications.

SNMP TRAP communications capture and send information via SNMP, but no confirmation that the communication between the devices has succeeded is provided by the receiving device.

SNMP INFORM communications capture and send information via SNMP, and an acknowledgment that the communication was received by the receiving device is provided. If the inform communication fails, it is resent. You can define the number of times and the intervals to resend the inform communication, or leave the defaults of five resends in three second intervals.

Note: SNMP INFORM communications may take up slightly more network resources than SNMP TRAP communications since there are additional communications between the devices, and due to additional network traffic created should the initial communication fail and another is sent.

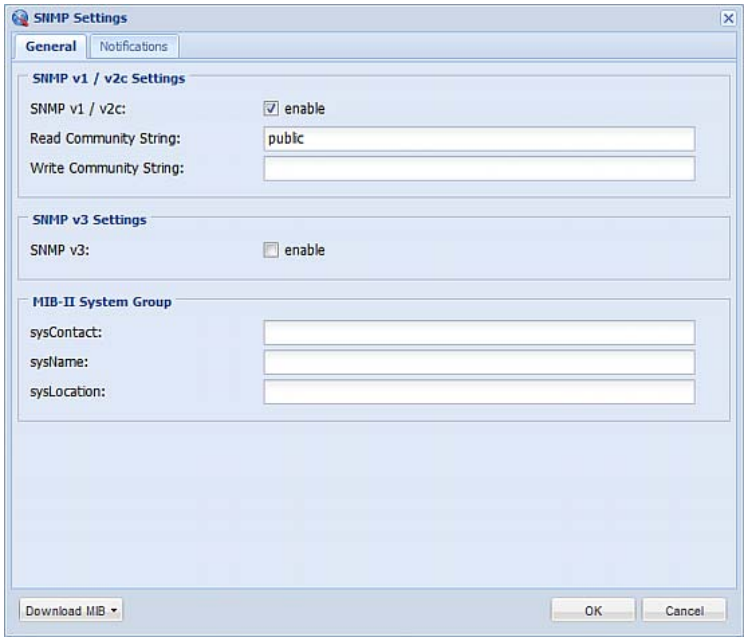
Use SNMP TRAP rules if you do not need confirmation that the communication has succeeded, and if you need to conserve network resources. Use SNMP INFORM communications to ensure more reliable communications, and if network resources can be managed with the potential additional network traffic.

Note: You should update the MIB used by your SNMP manager when updating to a new PX release. This ensures your SNMP manager has the correct MIB for the release you are using. See **Downloading SNMP MIB** *(on page 356).*

SNMPv2c Notifications

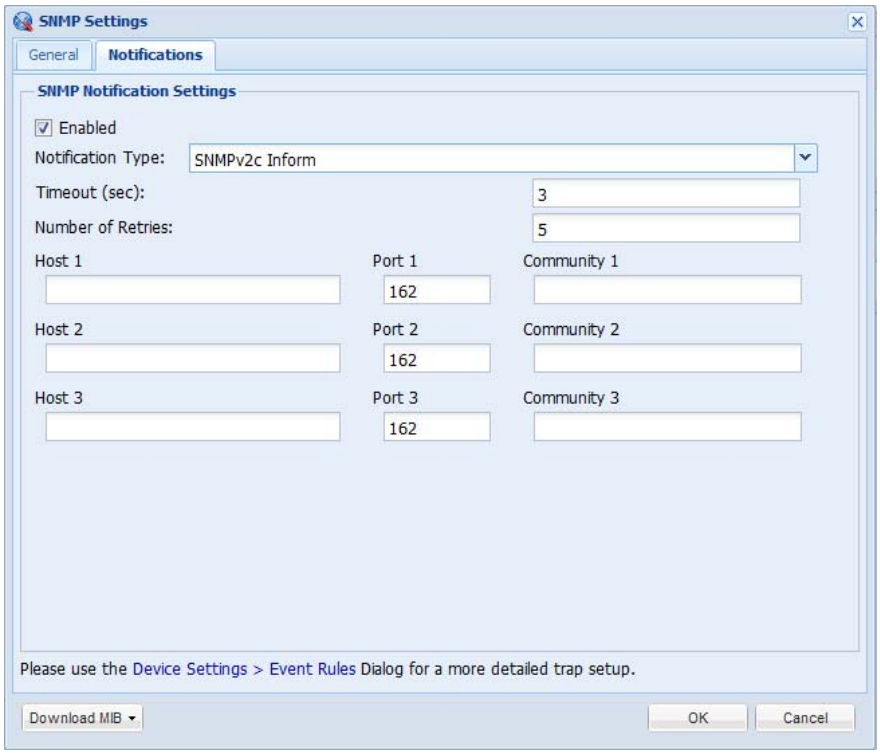
To configure the PX to send SNMP notifications:

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



2. On the Notifications tab, select the Enabled checkbox to enable the SNMP notification feature.

3. From the Notification Type drop-down, select the type of SNMP notification.

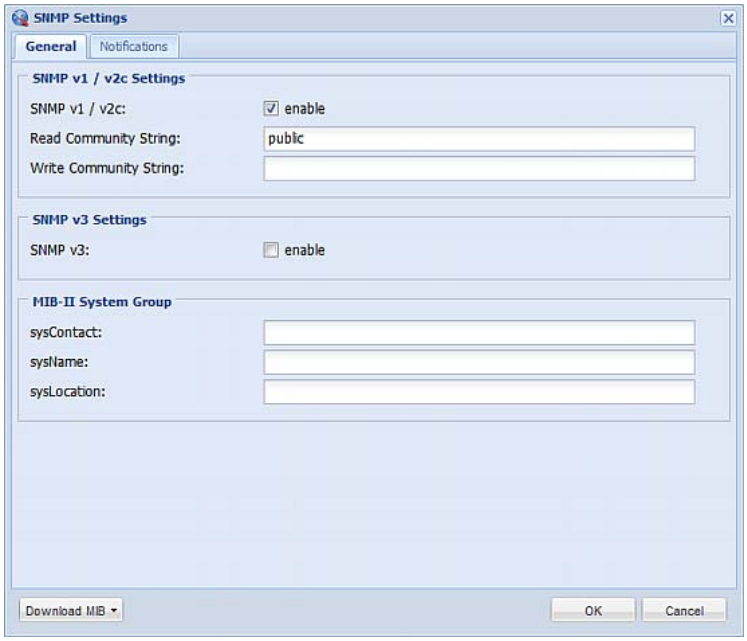


4. For SNMP INFORM communications, leave the resend settings at their default or:
   a. In the Timeout (sec) field, enter the interval of time, in seconds, after which a new inform communication is resent if the first is not received. For example, resend a new inform communication once every 3 seconds.
   b. In the Number of Retries field, enter the number of times you want to resend the inform communication if it fails. For example, inform communications are resent up to 5 times when the initial communication fails.
5. In the Host fields, enter the IP address of the device(s) you want to access. This is the address to which notifications are sent by the SNMP system agent. You can specify up to 3 SNMP destinations.
6. In the Port fields, enter the port number used to access the device(s).
7. In the Community fields, enter the SNMP community string to access the device(s). The community is the group representing the PX and all SNMP management stations.
8. Click OK.

SNMPv3 Notifications

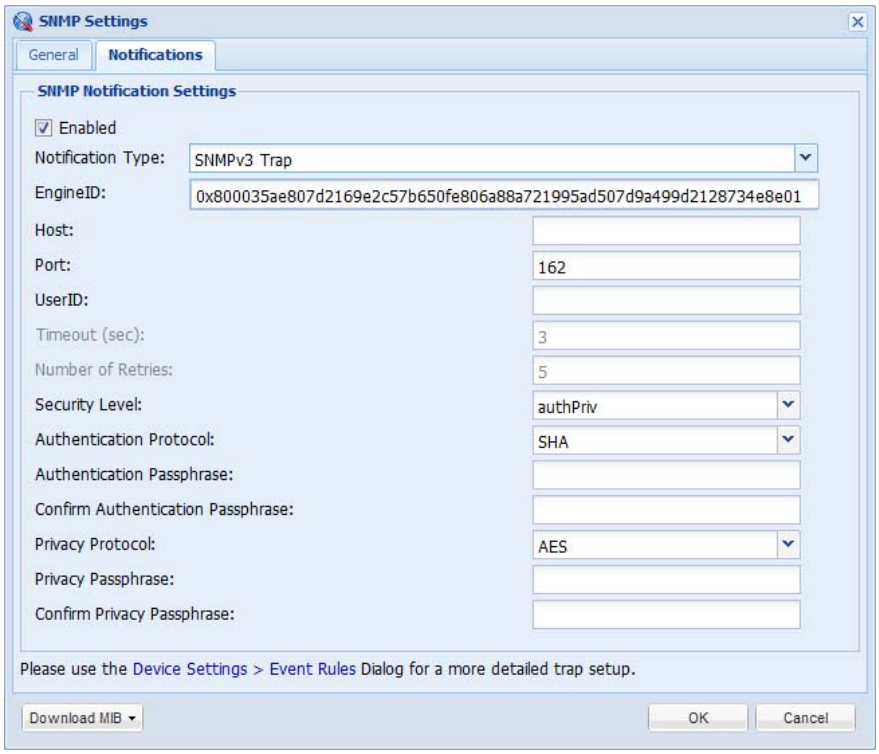
To configure the PX to send SNMPv3 notifications:

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



2. On the Notifications tab, select the Enabled checkbox to enable the SNMP notification feature.

3. From the Notification Type drop-down, select the type of SNMP notification.



4. For SNMP TRAPs, the engine ID is prepopulated.
5. For SNMP INFORM communications, leave the resend settings at their default or:
   a. In the Timeout (sec) field, enter the interval of time, in seconds, after which a new inform communication is resent if the first is not received. For example, resend a new inform communication once every 3 seconds.
   b. In the Number of Retries field, enter the number of times you want to resend the inform communication if it fails. For example, inform communications are resent up to 5 times when the initial communication fails.
6. For both SNMP TRAPS and INFORMS, enter the following as needed and then click OK to apply the settings:
   a. Host name
   b. Port number
   c. User ID needed to access the host
   d. Select the host security level

Security level	Description
"noAuthNoPriv"	Select this if no authorization or privacy protocols are needed.
"authNoPriv"	Select this if authorization is required but no privacy protocols are required. • Select the authentication protocol - MD5 or SHA • Enter the authentication passphrase and then confirm the authentication passphrase
"authPriv"	Select this if authentication and privacy protocols are required. • Select the authentication protocol - MD5 or SHA • Enter the authentication passphrase and confirm the authentication passphrase • Select the Privacy Protocol - DES or AES • Enter the privacy passphrase and then confirm the privacy passphrase

SNMP Gets and Sets

In addition to sending notifications, the PX is able to receive SNMP get and set requests from third-party SNMP managers.

- Get requests are used to retrieve information about the PX, 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 PX device name. When you change the SNMP system name, the device name shown in the web interface is also changed.

  The PX 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 PX MIB.

The PX MIB

The SNMP MIB file is required for using your PX device with an SNMP manager. An SNMP MIB file describes the SNMP functions.

Downloading SNMP MIB

The SNMP MIB file for the PX can be easily downloaded from the web interface. There are two ways to download the SNMP MIB file.

File download via the SNMP Settings dialog:

1. Choose Device Settings > Network Services > SNMP. The SNMP Settings dialog appears.
2. Click Download MIB. A submenu of MIB files appears.
3. Select the desired MIB file to download.
   - PDU2-MIB: The SNMP MIB file for PX power management.
   - ASSETMANAGEMENT-MIB: The SNMP MIB file for asset management.
   - LHX-MIB: The SNMP MIB file for managing the LHX/SHX heat exchanger(s).
4. Click Save to save the file onto your computer.

File download via the Device Information dialog:

1. Choose Maintenance > Device Information.
2. Click the download link in the PDU2-MIB, ASSETMANAGEMENT-MIB or LHX MIB field to download the desired SNMP MIB file.

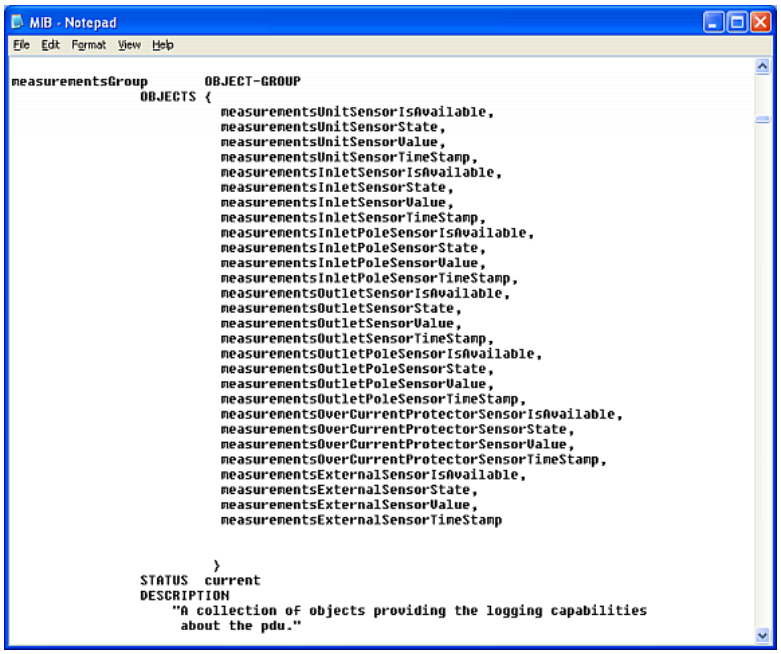
   The "USB Console INF file" link lets you download the USB-to-serial driver that may be required only when the PX is connected to a computer via a USB cable. See ***Installing the USB-to-Serial Driver (Optional)*** (on page 20) for details.
3. Click Save to save the file onto your computer.

Note: If the LHX/SHX support has been enabled, LHX-MIB is available for download in either dialog.

Layout

Opening the MIB reveals the custom objects that describe the PX 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 PX as a whole. One object listed under this group, measurementsUnitSensorValue, is described later in the MIB as "The sensor value". pduRatedCurrent, part of the configGroup group, describes the PDU current rating.

SNMP Sets and Thresholds

Some objects can be configured from the SNMP manager using SNMP set commands. Objects that can be configured have a MAX-ACCESS level of "read-write" in the MIB.

These objects include threshold objects, which causes the PX to generate a warning and send an SNMP notification when certain parameters are exceeded. See ***Setting Power Thresholds*** (on page 229) 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:

- Enable or disable synchronizing the PDU's date and time with NTP servers (synchronizeWithNTPServer OID 1.3.6.1.4.1.13742.4.1.1.48)
- Enable or disable the use of DHCP-assigned NTP servers if synchronization with NTP servers is enabled (useDHCPProvidedNTPServer OID 1.3.6.1.4.1.13742.4.1.1.49)
- Manually assign the primary NTP server if the use of DHCP-assigned NTP servers is disabled (primaryNTPServerAddressType OID 1.3.6.1.4.1.13742.4.1.1.50 and primaryNTPServerAddress OID 1.3.6.1.4.1.13742.4.1.1.51)
- Manually assign the secondary NTP server (optional) (secondaryNTPServerAddressType OID 1.3.6.1.4.1.13742.4.1.1.52 and secondaryNTPServerAddress OID 1.3.6.1.4.1.13742.4.1.1.53)

Tip: To specify the time zone, use the CLI or web interface instead. For the CLI, see **Setting the Time Zone** *(on page 432). For the web interface, see* **Setting the Date and Time** *(on page 146).*

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"
```

Retrieving Energy Usage

You can discover how much energy an IT device consumes by retrieving the Active Energy for the outlet this IT device is plugged into. The Active Energy values are included in the outletSensorMeasurementsTable, along with other outlet sensor readings.

A Note about Enabling Thresholds

When enabling previously disabled thresholds via SNMP, make sure you set a correct value for all thresholds that are supposed to be enabled prior to actually enabling them. Otherwise, you may get an error message.

Chapter 8 Using the Command Line Interface

This section explains how to use the command line interface (CLI) to administer a PX device.

In This Chapter

About the Interface 359
Logging in to CLI 360
Help Command 364
Querying Available Parameters for a Command 365
Showing Information 365
Clearing Information 396
Configuring the PX Device and Network 397
Load Shedding Configuration Commands 513
Power Control Operations 515
Actuator Control Operations 518
Unblocking a User 520
Resetting the PX 520
Network Troubleshooting 522
Retrieving Previous Commands 525
Automatically Completing a Command 525
Logging out of CLI 526

About the Interface

The PX 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 PX device
- Display the PX and network information, such as the device name, firmware version, IP address, and so on
- Configure the PX and network settings
- Troubleshoot network problems

You can access the interface over a local connection using a terminal emulation program such as HyperTerminal, or via a Telnet or SSH client such as PuTTY.

Note: Telnet access is disabled by default because it communicates openly and is thus insecure. To enable Telnet, see **Modifying Network Service Settings** *(on page 140).*

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 PX via a local connection.
2. Launch HyperTerminal on your computer and open a console window. When the window first opens, it is blank.

   Make sure the COM port settings use this configuration:

   - Bits per second = 115200 (115.2Kbps)
   - Data bits = 8
   - Stop bits = 1
   - Parity = None
   - Flow control = None

   Tip: For a USB connection, you can determine the COM port by choosing Control Panel > System > Hardware > Device Manager, and locating the "Dominion PX2 Serial Console" under the Ports group.

3. In the communications program, press Enter to send a carriage return to the PX. The Username prompt appears.

   ```
   Username: _
   ```

4. Type a name and press Enter. The name is case sensitive. Then you are prompted to enter a password.

```
Username: admin
Password: _
```

5. Type a password and press Enter. The password is case sensitive.

   After properly entering the password, the # or > system prompt appears. See ***Different CLI Modes and Prompts*** (on page 363) in the User Guide for more information.

   Tip: The "Last Login" information, including the date and time, is also displayed if the same user profile was used to log in to this product's web interface or CLI.

6. You are now logged in to the command line interface and can begin administering the PX.

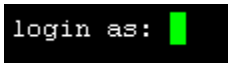
With SSH or Telnet

You can remotely log in to the command line interface (CLI) using an SSH or Telnet client, such as PuTTY.

Note: PuTTY is a free program you can download from the Internet. See PuTTY's documentation for details on configuration.

To log in using SSH or Telnet:

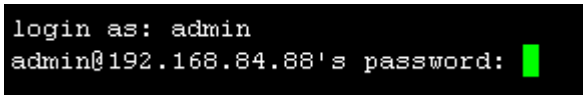
1. Ensure SSH or Telnet has been enabled. See ***Modifying Network Service Settings*** (on page 140) in the User Guide.
2. Launch an SSH or Telnet client and open a console window. A login prompt appears.



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 # or > system prompt appears. See ***Different CLI Modes and Prompts*** (on page 363) in the User Guide for more information.

Tip: The "Last Login" information, including the date and time, is also displayed if the same user profile was used to log in to this product's web interface or CLI.

6. You are now logged in to the command line interface and can begin administering the PX.

With an Analog Modem

The PX supports remote access to the CLI via a connected analog modem. This feature is especially useful when the LAN access is not available.

To connect to the PX via the modem:

1. Make sure the PX has an analog modem connected. See ***Connecting an Analog Modem*** (on page 64).
2. Make sure the computer you are using has an appropriate modem connected.
3. Launch a terminal emulation program, and configure its baud rate settings according to the baud rate set for the analog modem connected to the PX. See ***Configuring the Serial Port*** (on page 153).
4. Type the following AT command to make a connection with the PX.

   ```
   ATD<modem phone number>
   ```

5. The CLI login prompt appears after the connection is established successfully. Then type the user name and password to log in to the CLI.

To disconnect from the PX:

1. Return to the modem's command mode using the escape code +++.
2. After the OK prompt appears, type the following AT command to disconnect from the PX.

   ```
   ATH
   ```

Different CLI Modes and Prompts

Depending on the login name you use and the mode you enter, the system prompt in the CLI varies.

- User Mode: When you log in as a normal user, who may not have full permissions to configure the PX device, the **>** prompt appears.
- Administrator Mode: When you log in as an administrator, who has full permissions to configure the PX device, the # prompt appears.
- Configuration Mode: You can enter the configuration mode from the administrator or user mode. In this mode, the prompt changes to **config:#** or **config:>** and you can change PX device and network configurations. See ***Entering Configuration Mode*** (on page 397).
- 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 522).

Closing a Local Connection

Close the window or terminal emulation program when you finish accessing a PX device over the local connection.

When accessing or upgrading multiple PX devices, do not transfer the local connection cable from one device to another without closing the local connection window first.

Help Command

The help (?) command shows a list of main CLI commands available for the current mode. This is helpful when you are not familiar with CLI commands.

- **Help command under the administrator mode:**

  ```
  #          ?
  ```

- **Help command under the configuration mode:**

  ```
  config:#    ?
  ```

- **Help command under the diagnostic mode:**

  ```
  diag:#      ?
  ```

Press Enter after typing the help command, and a list of main commands for the current mode is displayed.

Tip: You can check what parameters are available for a specific CLI command by adding the help command to the end of the queried command. See **Querying Available Parameters for a Command** *(on page 365).*

Querying Available Parameters for a Command

If you are not sure what commands or parameters are available for a particular type of CLI command or its syntax, you can have the CLI show them by adding a space and the help command (?) to the end of that command. A list of available parameters and their descriptions will be displayed.

The following shows a few query examples.

- **To query available parameters for the "show" command:**

```
#           show ?
```

- **To query available parameters for the "show user" command:**

```
#           show user ?
```

- **To query available network configuration parameters:**

```
config:#    network ?
```

- **To query available role configuration parameters:**

```
config:#    role ?
```

- **To query available parameters for the "role create" command:**

```
config:#    role create ?
```

Showing Information

You can use the show commands to view current settings or the status of the PX 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 363).*

Network Configuration

This command shows all network configuration, such as the IP address, networking mode, and MAC address.

```
#        show network
```

IP Configuration

This command shows the IP-related configuration only, such as IPv4 and IPv6 configuration, address(es), gateway, and subnet mask.

```
#        show network ip <option>
```

Variables:

- <option> is one of the options: *all*, *v4* or *v6*.

Option	Description
all	This options shows both IPv4 and IPv6 settings. *Tip: You can also type the command without adding this option "all" to get the same data.*
v4	This option shows the IPv4 settings only.
v6	This option shows the IPv6 settings only.

LAN Interface Settings

This command shows the LAN interface information only, including LAN interface speed, duplex mode, current LAN interface status and LAN interface MAC address.

```
#        show network interface
```

Networking Mode

This command shows whether the current networking mode is wired or wireless.

```
#       show network mode
```

Note: If the PX is a slave device connected to the LAN via the master PX device, the `show network mode` *command displays* wired(USB) *instead of* wired*.*

Wireless Configuration

This command only shows the wireless configuration of the PX device, such as the SSID parameter.

```
#       show network wireless
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show network wireless details
```

Network Service Settings

This command shows the network service settings only, including the Telnet setting, TCP ports for HTTP, HTTPS, SSH and Modbus/TCP services, and SNMP settings.

```
#       show network services <option>
```

Variables:

- <option> is one of the options: *all*, *http*, *https*, *telnet*, *ssh*, *snmp*, *modbus* and *zeroconfig*.

Option	Description
all	Displays the settings of all network services, including HTTP, HTTPS, Telnet, SSH and SNMP. *Tip: You can also type the command without adding this option "all" to get the same data.*
http	Only displays the TCP port for the HTTP service.

Option	Description
https	Only displays the TCP port for the HTTPS service.
telnet	Only displays the settings of the Telnet service.
ssh	Only displays the settings of the SSH service.
snmp	Only displays the SNMP settings.
modbus	Only displays the settings of the Modbus/TCP service.
zeroconfig	Only displays the settings of the zero configuration advertising.

PDU Configuration

This command shows the PDU configuration, such as the device name, firmware version and model type.

```
#        show pdu
```

To show detailed information, add the parameter "details" to the end of the command.

```
#        show pdu details
```

Outlet Information

This command syntax shows the outlet information.

```
#       show outlets <n>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show outlets <n> details
```

Variables:

- <n> is one of the options: *all*, or a number.

Option	Description
all	Displays the information for all outlets. *Tip: You can also type the command without adding this option "all" to get the same data.*
A specific outlet number	Displays the information for the specified outlet only.

Displayed information:

- Without the parameter "details," only the outlet name and state are displayed.
- With the parameter "details," more outlet information is displayed in addition to the state, such as rated current, voltage, active power, active energy, and outlet settings.

Inlet Information

This command syntax shows the inlet information.

```
#       show inlets <n>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show inlets <n> details
```

Variables:

- <n> is one of the options: *all*, or a number.

Option	Description
all	Displays the information for all inlets. *Tip: You can also type the command without adding this option "all" to get the same data.*
A specific inlet number	Displays the information for the specified inlet only. An inlet number needs to be specified only when there are more than 1 inlet on your PDU.

Displayed information:

- Without the parameter "details," only the inlet's name and RMS current are displayed.
- With the parameter "details," more inlet information is displayed in addition to the inlet name and RMS current, such as the inlet's RMS voltage, active power and active energy.

Overcurrent Protector Information

This command is only available for models with overcurrent protectors for protecting outlets.

This command syntax shows the overcurrent protector information, such as a circuit breaker or a fuse.

```
#        show ocp <n>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#        show ocp <n> details
```

Variables:

- <n> is one of the options: *all*, or a number.

Option	Description
all	Displays the information for all overcurrent protectors. *Tip: You can also type the command without adding this option "all" to get the same data.*
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 PX device.

```
#       show time
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show time details
```

Default Measurement Units

This command shows the default measurement units applied to the PX web and CLI interfaces across all users, especially those users authenticated through remote authentication servers.

```
#       show user defaultPreferences
```

Note: If a user has set his/her own preferred measurement units or the administrator has changed any user's preferred units, the web and CLI interfaces show the preferred measurement units for that user instead of the default ones after that user logs in to the PX. See **Existing User Profiles** *(on page 385) for the preferred measurement units for a specific user.*

Environmental Sensor Information

This command syntax shows the environmental sensor's information.

```
#       show externalsensors <n>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show externalsensors <n> details
```

```
External sensor 3 ('Temperature 1')
Sensor type: Temperature
Reading:    31.8 deg C (normal)

Serial number:        AEI0950133
Description:          Not configured
Location:            X Not configured
                    Y Not configured
                    Z Not configured
Position:             Port 1
Using default thresholds: yes
```

Variables:

- <n> is one of the options: *all*, or a number.

Option	Description
all	Displays the information of all environmental sensors. *Tip: You can also type the command without adding this option "all" to get the same data.*
A specific environmental sensor number*	Displays the information for the specified environmental sensor only.

* The environmental sensor number is the ID number assigned to the sensor, which can be found on the Peripheral Devices page of the PX web interface.

Displayed information:

- Without the parameter "details," only the sensor ID, sensor type and reading are displayed.

  Note: A discrete (on/off) sensor displays the sensor state instead of the numeric reading.

- With the parameter "details," more information is displayed in addition to the ID number and sensor reading, such as the serial number, sensor position, and X, Y, and Z coordinates.

Note: DPX sensor packages do not provide chain position information..

Environmental Sensor Package Information

Different from the "`show externalsensors`" commands, which show the reading, status and configuration of an individual environmental sensor, the following command shows the information of all connected environmental sensor packages, each of which may contain more than one sensor or actuator.

```
#       show peripheralDevicePackages
```

Information similar to the following is displayed. An environmental sensor package is a peripheral device package.

```
Peripheral Device Package 1
Serial Number:    AEI7A00022
Package Type:     DPX-T1H1
Position:         Port 1
Package State:    operational
Firmware Version: Not available

Peripheral Device Package 2
Serial Number:    AEI7A00021
Package Type:     DPX-T3H1
Position:         Port 1
Package State:    operational
Firmware Version: Not available
```

Actuator Information

This command syntax shows an actuator's information.

```
#       show actuators <n>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show actuators <n> details
```

Variables:

- <n> is one of the options: *all*, or a number.

Option	Description
all	Displays the information for all actuators. *Tip: You can also type the command without adding this option "all" to get the same data.*
A specific actuator number*	Displays the information for the specified actuator only.

* The actuator number is the ID number assigned to the actuator. The ID number can be found using the PX 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.

Outlet Sensor Threshold Information

This command syntax shows the specified outlet sensor's threshold-related information.

```
#       show sensor outlet <n> <sensor type>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show sensor outlet <n> <sensor type> details
```

Variables:

- <n> is the number of the outlet whose sensors you want to query.
- <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
lineFrequency	Line frequency sensor

Displayed information:

- Without the parameter "details," only the sensor reading, state, threshold, deassertion hysteresis and assertion timeout settings of the specified outlet 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.

Outlet Pole Sensor Threshold Information

This command is available for an in-line monitor only, including PX2-3000 and PX3-3000 series.

This command syntax shows the specified outlet pole sensor's threshold-related information.

```
#       show sensor outletpole <n> <p> <sensor type>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show sensor outletpole <n> <p> <sensor type> details
```

Variables:

- <n> is the number of the outlet whose pole sensors you want to query.
- <p> is the label of the outlet pole whose sensors you want to query.

Pole	Label <p>	Current sensor	Voltage sensor
1	**L1**	L1	L1 - L2
2	**L2**	L2	L2 - L3
3	**L3**	L3	L3 - L1

- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor

Displayed information:

- Without the parameter "details," only the reading, state, threshold, deassertion hysteresis and assertion delay settings of the specified outlet 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.

Inlet Sensor Threshold Information

This command is NOT available for an in-line monitor (PX3-3000 series).

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 the number 1.
- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor
unbalancedCurrent	Unbalanced load sensor
lineFrequency	Line frequency sensor

Displayed information:

- Without the parameter "details," only the reading, state, threshold, deassertion hysteresis and assertion timeout settings of the specified inlet sensor are displayed.
- With the parameter "details," more sensor information is displayed, including resolution and range.
- If the requested sensor type is not supported, the "Sensor is not available" message is displayed.

Inlet Pole Sensor Threshold Information

This command is only available for a three-phase PDU except for an in-line monitor (PX3-3000 series).

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 the number 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

Sensor type	Description
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor

Displayed information:

- Without the parameter "details," only the reading, state, threshold, deassertion hysteresis and assertion timeout settings of the specified inlet pole sensor are displayed.
- With the parameter "details," more sensor information is displayed, including resolution and range.
- If the requested sensor type is not supported, the "Sensor is not available" message is displayed.

Overcurrent Protector Sensor Threshold Information

This command is only available for models with overcurrent protectors for protecting outlets.

This command syntax shows the specified overcurrent protector sensor's threshold-related information.

```
#       show sensor ocp <n> <sensor type>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show sensor ocp <n> <sensor type> details
```

Variables:

- <n> is the number of the overcurrent protector whose sensors you want to query.
- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor

Displayed information:

- Without the parameter "details," only the reading, state, threshold, deassertion hysteresis and assertion timeout settings of the specified overcurrent protector sensor are displayed.
- With the parameter "details," more sensor information is displayed, including resolution and range.

Environmental Sensor Threshold Information

This command syntax shows the specified environmental sensor's threshold-related information.

```
#       show sensor externalsensor <n>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show sensor externalsensor <n> details

External sensor 3 (Temperature):
Reading: 31.8 deg C
State:   normal

Active Thresholds: Sensor specific thresholds

Default Thresholds for Temperature sensors:
Lower critical threshold: 10.0 deg C
Lower warning threshold:  15.0 deg C
Upper warning threshold:  30.0 deg C
Upper critical threshold: 35.0 deg C
Deassertion hysteresis:   1.0 deg C
Assertion timeout:       0 samples

Sensor Specific Thresholds:
Lower critical threshold: 8.0 deg C
Lower warning threshold:  13.0 deg C
Upper warning threshold:  28.0 deg C
Upper critical threshold: 33.0 deg C
Deassertion hysteresis:   1.0 deg C
Assertion timeout:       0 samples
```

Variables:

- <n> is the environmental sensor number. The environmental sensor number is the ID number assigned to the sensor, which can be found on the Peripheral Devices page of the PX web interface.

Displayed information:

- Without the parameter "details," only the reading, threshold, deassertion hysteresis and assertion timeout settings of the specified environmental sensor are displayed.
- With the parameter "details," more sensor information is displayed, including resolution and range.

Note: For a discrete (on/off) sensor, the threshold-related and accuracy-related data is NOT available.

Environmental Sensor Default Thresholds

This command syntax shows a certain sensor type's default thresholds, which are the initial thresholds applying to the specified type of sensor.

```
#       show defaultThresholds <sensor type>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show defaultThresholds <sensor type> details
```

Variables:

- <sensor type> is one of the following numeric sensor types:

Sensor types	Description
absoluteHumidity	Absolute humidity sensors
relativeHumidity	Relative humidity sensors
temperature	Temperature sensors
airPressure	Air pressure sensors
airFlow	Air flow sensors
vibration	Vibration sensors
all	All of the above numeric sensors *Tip: You can also type the command without adding this option "all" to get the same data.*

Displayed information:

- Without the parameter "details," only the default upper and lower thresholds, deassertion hysteresis and assertion timeout settings of the specified sensor type are displayed.
- With the parameter "details," the threshold range is displayed in addition to default thresholds settings.

Security Settings

This command shows the security settings of the PX.

```
#       show security
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show security details
```

Displayed information:

- Without the parameter "details," the information including IP access control, role-based access control, password policy, and HTTPS encryption is displayed.
- With the parameter "details," more security information is displayed, such as user blocking time, user idle timeout and front panel permissions (if supported by your model).

Existing User Profiles

This command shows the data of one or all existing user profiles.

```
#       show user <user_name>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show user <user_name> details
```

Variables:

- <user_name> is the name of the user whose profile you want to query. The variable can be one of the options: *all* or a user's name.

Option	Description
all	This option shows all existing user profiles. *Tip: You can also type the command without adding this option "all" to get the same data.*
a specific user's name	This option shows the profile of the specified user only.

Displayed information:

- Without the parameter "details," only four pieces of user information are displayed: user name, user "Enabled" status, SNMP v3 access privilege, and role(s).
- With the parameter "details," more user information is displayed, such as the telephone number, e-mail address, preferred measurement units and so on.

Existing Roles

This command shows the data of one or all existing roles.

```
#       show roles <role_name>
```

Variables:

- <role_name> is the name of the role whose permissions you want to query. The variable can be one of the following options:

Option	Description
all	This option shows all existing roles. *Tip: You can also type the command without adding this option "all" to get the same data.*
a specific role's name	This option shows the data of the specified role only.

Displayed information:

- Role settings are displayed, including the role description and privileges.

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 402).*

Serial Port Settings

This command shows the baud rate setting of the serial port labeled CONSOLE / MODEM on the PX device.

```
#       show serial
```

EnergyWise Settings

This command shows the PX device's current configuration for Cisco® EnergyWise.

```
#       show energywise
```

USB-Cascading Configuration Information

This command shows the USB-cascading configuration, such as the cascading mode and device position.

```
#       show cascading
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show cascading details
```

Asset Sensor Settings

This command shows the asset sensor settings, such as the total number of rack units (tag ports), asset sensor state, numbering mode, orientation, available tags and LED color settings.

```
#       show assetStrip <n>
```

Variables:

- <n> is one of the options: *all*, or a number.

Option	Description
all	Displays all asset sensor information. *Tip: You can also type the command without adding this option "all" to get the same data.*

Option	Description
A specific asset sensor number	Displays the settings of the asset sensor connected to the specified FEATURE port number. For the PX device with only one FEATURE port, the valid number is always 1.

Rack Unit Settings of an Asset Sensor

For the Raritan asset sensor, a rack unit refers to a tag port. This command shows the settings of a specific rack unit or all rack units on an asset sensor, such as a rack unit's LED color and LED mode.

```
#       show rackUnit <n> <rack_unit>
```

Variables:

- <n> is the number of the FEATURE port where the selected asset sensor is physically connected. For the PX device with only one FEATURE port, the number is always 1.
- <rack_unit> is one of the options: *all* or a specific rack unit's index number.

Option	Description
all	Displays the settings of all rack units on the specified asset sensor. *Tip: You can also type the command without adding this option "all" to get the same data.*
A specific number	Displays the settings of the specified rack unit on the specified asset sensor. Use the index number to specify the rack unit. The index number of each rack unit is available on the Asset Strip page of the web interface.

Blade Extension Strip Settings

This command shows the information of a blade extension strip, including the total number of tag ports, and if available, the ID (barcode) number of any connected tag.

```
#       show bladeSlot <n> <rack_unit> <blade_slot>
```

Variables:

- <n> is the number of the FEATURE port where the selected asset sensor is physically connected. For the PX device with only one FEATURE port, the number is always 1.
- <rack_unit> is the index number of the desired rack unit (tag port) on the selected asset sensor. The index number of each rack unit is available on the Asset Strip page of the web interface.
- <blade_slot> is one of the options: *all* or a specific number of a tag port on the blade extension strip.

Option	Description
all	Displays the information of all tag ports on the specified blade extension strip connected to a particular rack unit. *Tip: You can also type the command without adding this option "all" to get the same data.*
A specific number	Displays the information of the specified tag port on the blade extension strip connected to a particular rack unit. The number of each tag port on the blade extension strip is available on the Asset Strip page.

Event Log

The command used to show the event log begins with `show eventlog`. You can add either the *limit* or *class* parameters or both to show specific events.

- **Show the last 30 entries:**

```
#       show eventlog
```

- **Show a specific number of last entries in the event log:**

```
#       show eventlog limit <n>
```

- **Show a specific type of events only:**

```
#       show eventlog class <event_type>
```

- **Show a specific number of last entries associated with a specific type of events only:**

```
#       show eventlog limit <n> class <event_type>
```

Variables:

- <n> is one of the options: *all* or a number.

Option	Description
all	Displays all entries in the event log.
An integer number	Displays the specified number of last entries in the event log. The number ranges between 1 to 10,000.

- <event_type> is one of the following event types.

Event type	Description
all	All events.
device	Device-related events, such as system starting or firmware upgrade event.
userAdministration	User management events, such as a new user profile or a new role.
userActivity	User activities, such as login or logout.
pdu	Displays PDU-related events, such as entry or exit of the load shedding mode.

Event type	Description
sensor	Internal or external sensor events, such as state changes of any sensors.
serverMonitor	Server-monitoring records, such as a server being declared reachable or unreachable.
assetManagement	Raritan asset management events, such as asset tag connections or disconnections.
lhx	Schroff® LHX/SHX heat exchanger events.
modem	Modem-related events.
timerEvent	Scheduled action events.
webcam	Events for webcam management, if available.
cardReader	Events for card reader management, if available.
energywise	Cisco EnergyWise-related events, such as enabling the support of the EnergyWise function.

Wireless LAN Diagnostic Log

This command shows the diagnostic log for the wireless LAN connection.

```
#       show wlanlog
```

Server Reachability Information

This command shows all server reachability information with a list of monitored servers and status.

```
#       show serverReachability
```

Server Reachability Information for a Specific Server

To show the server reachability information for a certain IT device only, use the following command.

```
#       show serverReachability server <n>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show serverReachability server <n> details
```

Variables:

- <n> is a number representing the sequence of the IT device in the monitored server list.

  You can find each IT device's sequence number using the CLI command of `show serverReachability` as illustrated below.

```
-------------------------------------------------------------------
#  IP address       Enabled  Status
-------------------------------------------------------------------
1  192.168.84.126   Yes      Waiting for reliable connection
2  www.raritan.com  Yes      Waiting for reliable connection
```

Displayed information:

- Without the parameter "details," only the specified device's IP address, monitoring enabled/disabled state and current status are displayed.
- With the parameter "details," more settings for the specified device are displayed, such as number of pings and wait time prior to the next ping.

Command History

This command syntax shows the command history for current connection session.

```
#       show history
```

Displayed information:

- A list of commands that were previously entered in the current session is displayed.

History Buffer Length

This command syntax shows the length of the history buffer for storing history commands.

```
#       show history bufferlength
```

Displayed information:

- The current history buffer length is displayed.

Reliability Data

This command shows the reliability data.

```
#       show reliability data
```

Reliability Error Log

This command shows the reliability error log.

```
#       show reliability errorlog <n>
```

Variables:

- <n> is one of the options: *0* (zero) or any other integer number.

Option	Description
0	Displays all entries in the reliability error log. *Tip: You can also type the command without adding this option "0" to get all data.*
A specific integer number	Displays the specified number of last entries in the reliability error log.

Examples

This section provides examples of the show command.

Example 1 - Basic Security Information

The diagram shows the output of the *show security* command.

```
# show security
IPv4 access control: Disabled

IPv6 access control: Disabled

Role based access control for IPv4: Disabled

Role based access control for IPv6: Disabled

Password aging: Disabled

Prevent concurrent user login:   No

Strong passwords: Disabled

Enforce HTTPS for web access: Yes

Restricted Service Agreement: disabled
```

Example 2 - In-Depth Security Information

More information is displayed when typing the *show security details* command.

```
# show security details
IPv4 access control: Disabled

IPv6 access control: Disabled


Role based access control for IPv4: Disabled

Role based access control for IPv6: Disabled

Password aging: Disabled

Prevent concurrent user login:   No
Maximum number of failed logins: 3
User block time:                 10 minutes

User idle timeout: 1440 minutes

Strong passwords: Disabled

Enforce HTTPS for web access: Yes

Restricted Service Agreement: disabled
Restricted Service Agreement Banner Content:
Unauthorized access prohibited; all access and activities not explicitly authori
zed by management are unauthorized. All activities are monitored and logged. The
re is no privacy on this system. Unauthorized access and activities or any crimi
nal activity will be reported to appropriate authorities.
```

Example 3 - Basic PDU Information

The diagram shows the output of the *show pdu* command.

```
# show pdu
PDU 'my PX'
Model:            PX3-XXXX
Firmware Version: 2.X.0.5-40956
```

Example 4 - In-Depth PDU Information

More information is displayed when typing the *show pdu details* command. Displayed information varies depending on the model you purchased.

```
# show pdu details
PDU 'my PX'
Model:            PX3-XXXX
Firmware Version: 2.X.0.5-40956
Serial Number:    QGZ3792136
Board Revision:   0x01

Voltage rating:   200-240V
Current rating:   16A
Frequency rating: 50/60Hz
Power rating:     3.2-3.8kVA

Sensor data retrieval:      Enabled
Measurements per log entry: 60

External sensor Z coordinate format: Rack units
Device altitude:                     0 m
```

Clearing Information

You can use the clear commands to remove unnecessary data from the PX.

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 363).*

Clearing Event Log

This command removes all data from the event log.

```
#       clear eventlog
```

-- OR --

```
#       clear eventlog /y
```

If you entered the command without "`/y`," a message appears, prompting you to confirm the operation. Type `y` to clear the event log or `n` to abort the operation.

If you type `y`, a message "Event log was cleared successfully" is displayed after all data in the event log is deleted.

Clearing WLAN Log

This command removes all data from the diagnostic log for the wireless LAN (WLAN) connection.

```
#       clear wlanlog
```

-- OR --

```
#       clear wlanlog /y
```

If you entered the command without "/y," a message appears, prompting you to confirm the operation. Type y to clear the WLAN log or n to abort the operation.

If you type y, a message "WLAN log was cleared successfully" is displayed to indicate all data in the WLAN log has been deleted.

Configuring the PX Device and Network

To configure the PX 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 363).*

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 398).

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 363).

PDU Configuration Commands

A PDU configuration command begins with *pdu*. You can use the PDU configuration commands to change the settings that apply to the whole PX device.

Changing the PDU Name

This command changes the PX device's name.

```
config:#   pdu name "<name>"
```

Variables:

- <name> is a string comprising up to 32 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.

Setting the Outlet Relay Behavior

This section applies to outlet-switching capable models only.

This command syntax determines the relay behavior of all outlets on a PX model.

```
config:#   pdu relayBehaviorOnPowerLoss <option>
```

Variables:

- <option> is one of the options: *latching* or *nonLatching*.

Note: For more information on the outlet relay behavior, see **PX3 Latching Relay Behavior** *(on page 206).*

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 PX device 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.

Note: Power-on sequencing is disabled in the latching mode. See **PX3 Latching Relay Behavior** *(on page 206).*

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.

Note: Power-on sequencing is disabled in the latching mode. See **PX3 Latching Relay Behavior** *(on page 206).*

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 PX device powers up.

Option	Description
on	Switches ON all outlets when the PX device powers up.
lastKnownState	Restores all outlets to the previous status before powering down the PX device when the PDU powers up again.

Note: This feature does NOT take effect and cannot be configured on a PX3 device after the outlet relay is set to the "Latching" mode. See **Setting the Outlet Relay Behavior** *(on page 207).*

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 ***Setting the Initialization Delay*** (on page 217) for information on outlet initialization delay.

```
config:#   pdu outletInitializationDelayOnDeviceStartup <timing>
```

Variables:

- <timing> is a delay time between 1 and 3600 seconds.

Note: This feature does NOT take effect and cannot be configured on a PX3 device after the outlet relay is set to the "Latching" mode. See **Setting the Outlet Relay Behavior** *(on page 207).*

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 ***Setting Non-Critical Outlets and Load Shedding Mode*** (on page 220).

```
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 161).

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 161).

Specifying the Device Altitude

This command specifies your PX device's altitude above sea level (in meters). You must specify the PX device's altitude above sea level if a Raritan's DPX differential air pressure sensor is attached. This is because the device's altitude is associated with the altitude correction factor. See ***Altitude Correction Factors*** (on page 677).

```
config:#   pdu deviceAltitude <altitude>
```

Variables:

- <altitude> is an integer between 1 and 3000 meters.

Setting the Z Coordinate Format for Environmental Sensors

This command enables or disables the use of rack units for specifying the height (Z coordinate) of environmental sensors.

```
config:#   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 481).*

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 ***Disabling the Automatic Management Function*** (on page 312).

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 PX.

```
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.

Setting the Networking Mode

If your PX device is implemented with both wired and wireless networking mechanisms, you must determine which mechanism is enabled for network connectivity before further configuring networking parameters.

This command enables the wired or wireless networking mode.

```
config:#   network mode <mode>
```

Variables:

- <mode> is one of the modes: *wired* or *wireless*.

Mode	Description
wired	Enables the wired networking mode.
wireless	Enables the wireless networking mode.

Note: If you enable the wireless networking mode, and the PX does not detect any wireless USB LAN adapter or the connected wireless USB LAN adapter is not supported, the message "Supported Wireless device not found" is displayed.

Configuring IP Protocol Settings

By default, only the IPv4 protocol is enabled. You can enable both the IPv4 and IPv6 protocols, or only the IPv6 protocol for your PX device.

An IP protocol configuration command begins with *network ip*.

Enabling IPv4 or IPv6

This command determines which IP protocol is enabled on the PX.

```
config:#   network ip proto <protocol>
```

Variables:

- <protocol> is one of the options: *v4Only*, *v6Only* or *both*.

Mode	Description
v4Only	Enables IPv4 only on all interfaces. This is the default.
v6Only	Enables IPv6 only on all interfaces.
both	Enables both IPv4 and IPv6 on all interfaces.

Selecting IPv4 or IPv6 Addresses

This command determines which IP address is used when the DNS server returns both of IPv4 and IPv6 addresses. You need to configure this setting only after both IPv4 and IPv6 protocols are enabled on the PX.

```
config:#   network ip dnsResolverPreference <resolver>
```

Variables:

- <resolver> is one of the options: *preferV4* or *preferV6.*

Option	Description
preferV4	Use the IPv4 addresses returned by the DNS server.
preferV6	Use the IPv6 addresses returned by the DNS server.

Setting Wireless Parameters

You must configure wireless parameters, including Service Set Identifier (SSID), authentication method, Pre-Shared Key (PSK), and Basic Service Set Identifier (BSSID) after the wireless networking mode is enabled.

A wireless configuration command begins with *network wireless*.

Note: If current networking mode is not wireless, the SSID, PSK and BSSID values are not applied until the networking mode is changed to "wireless." In addition, a message appears, indicating that the active network interface is not wireless.

Setting the SSID

This command specifies the SSID string.

```
config:#   network wireless SSID <ssid>
```

Variables:

- <ssid> is the name of the wireless access point, which consists of:
  - Up to 32 ASCII characters
  - No spaces
  - ASCII codes 0x20 ~ 0x7E

Setting the Authentication Method

This command sets the wireless authentication method to either PSK or Extensible Authentication Protocol (EAP).

```
config:#   network wireless authMethod <method>
```

Variables:

- <method> is one of the authentication methods: *PSK* or *EAP*.

Method	Description
PSK	The wireless authentication method is set to PSK.
EAP	The wireless authentication method is set to EAP.

Setting the PSK

If the Pre-Shared Key (PSK) authentication method is selected, you must assign a PSK passphrase by using this command.

```
config:#   network wireless PSK <psk>
```

Variables:

- <psk> is a string or passphrase that consists of:
  - 8 to 63 characters
  - No spaces
  - ASCII codes 0x20 ~ 0x7E

Setting EAP Parameters

When the wireless authentication method is set to EAP, you must configure EAP authentication parameters, including outer authentication, inner authentication, EAP identity, password, and CA certificate.

- **Determine the outer authentication protocol:**

```
config:#   network wireless eapOuterAuthentication <outer_auth>
```

- **Determine the inner authentication protocol:**

```
config:#   network wireless eapInnerAuthentication <inner_auth>
```

- **Set the EAP identity:**

```
config:#   network wireless eapIdentity <identity>
```

- **Set the EAP password:**

```
config:#   network wireless eapPassword
```

After performing the above command, the PX prompts you to enter the password. Then type the password and press Enter.

- **Provide a CA TLS certificate:**

```
config:#   network wireless eapCACertificate
```

After performing the above command, the system prompts you to enter the CA certificate's contents. For details, see ***EAP CA Certificate Example*** (on page 412).

- **Enable or disable verification of the TLS certificate chain:**

```
config:#   network wireless enableCertVerification <option1>
```

- **Allow expired and not yet valid TLS certificates:**

```
config:#   network wireless allowOffTimeRangeCerts <option2>
```

- **Allow wireless network connection with incorrect system time:**

```
config:#   network wireless allowConnectionWithIncorrectClock <option3>
```

Variables:

- The value of <outer_auth> is *PEAP* because PX only supports Protected Extensible Authentication Protocol (PEAP) as the outer authentication.
- The value of <inner_auth> is *MSCHAPv2* because PX only supports Microsoft's Challenge Authentication Protocol Version 2 (MSCHAPv2) as the inner authentication.
- <identity> is your user name for the EAP authentication.
- <option1> is one of the options: *true* or *false*.

Option	Description
true	Enables the verification of the TLS certificate chain.
false	Disables the verification of the TLS certificate chain.

- <option2> is one of the options: *true* or *false*.

Option	Description
true	Always make the wireless network connection successful even though the TLS certificate chain contains any certificate which is outdated or not valid yet.
false	The wireless network connection is NOT successfully established when the TLS certificate chain contains any certificate which is outdated or not valid yet.

- <option3> is one of the options: *true* or *false*.

Option	Description
true	Make the wireless network connection successful when the PX system time is earlier than the firmware build before synchronizing with the NTP server, causing the TLS certificate to become invalid.
false	The wireless network connection is NOT successfully established when the PX finds that the TLS certificate is not valid due to incorrect system time.

EAP CA Certificate Example

This section provides a CA certificate example only. Your CA certificate contents should be different from the contents displayed in this example.

To provide a CA certificate:

1. Make sure you have entered the configuration mode. See ***Entering Configuration Mode*** (on page 397).
2. Type the following command and press Enter.

   ```
   config:#   network wireless eapCACertificate
   ```

3. The system prompts you to enter the contents of the CA certificate.
4. Open a CA certificate using a text editor. You should see certificate contents similar to the following.

```
--- BEGIN CERTIFICATE ---
MIICjTCCAfigAwIBAgIEMaYgRzALBgkqhkiG9w0BAQQwRTELMAkGA1UEBhMCVVMx
NjA0BgNVBAoTLU5hdGlvbmFsIEFlcm9uYXV0aWNzIGFuZCBTcGFjZSBBZG1pbmlz
dHJhdGlvbjAmFxE5NjA1MjgxMzQ5MDUrMDgwMBcROTgwNTI4MTM0OTA1KzA4MDAw
ZzELMAkGA1UEBhMCVVMxNjA0BgNVBAoTLU5hdGlvbmFsIEFlcm9uYXV0aWNzIGFu
ZCBTcGFjZSBBZG1pbmlzdHJhdGlvbjEgMAkGA1UEBRMCMTYwEwYDVQQDEwxTdGV2
ZSBTY2hvY2gwWDALBgkqhkiG9w0BAQEDSQAwRgJBALrAwyYdgxmzNP/ts0Uyf6Bp
miJYktU/w4NG67ULaN4B5CnEz7k57s9o3YY3LecETgQ5iQHmkwlYDTL2fTgVfw0C
AQOjgaswgagwZAYDVR0ZAQH/BFowWDBWMFQxCzAJBgNVBAYTAlVTMTYwNAYDVQQK
Ey1OYXRpb25hbCBBZXJvbmF1dGljcyBhbmQgU3BhY2UgQWRtaW5pc3RyYXRpb24x
DTALBgNVBAMTBENSTDEwFwYDVR0BAQH/BA0wC4AJODMyOTcwODEwMBgGA1UdAgQR
MA8ECTgzMjk3MDgyM4ACBSAwDQYDVR0KBAYwBAMCBkAwCwYJKoZIhvcNAQEEA4GB
AH2y1VCEw/A4zaXzSYZJTTUi3uawbbFiS2yxHvgf28+8Js0OHXk1H1w2d6qOHH21
X82tZXd/0JtG0g1T9usFFBDvYK8O0ebgz/P5ELJnBL2+atObEuJy1ZZ0pBDWINR3
WkDNLCGiTkCKp0F5EWIrVDwh54NNevkCQRZita+z4IBO
--- END CERTIFICATE ---
```

5. Select and copy the contents as illustrated below, excluding the starting line containing "BEGIN CERTIFICATE" and the ending line containing "END CERTIFICATE."

```
MIICjTCCAfigAwIBAgIEMaYgRzALBgkqhkiG9w0BAQQwRTELMAk
GA1UEBhMCVVMxNjA0BgNVBAoTLU5hdGlvbmFsIEFlcm9uYXV0aW
NzIGFuZCBTcGFjZSBBZG1pbmlzdHJhdGlvbjAmFxE5NjA1MjgxM
zQ5MDUrMDgwMBcROTgwNTI4MTM0OTA1KzA4MDAwZzELMAkGA1UE
BhMCVVMxNjA0BgNVBAoTLU5hdGlvbmFsIEFlcm9uYXV0aWNzIGF
uZCBTcGFjZSBBZG1pbmlzdHJhdGlvbjEgMAkGA1UEBRMCMTYwEw
YDVQQDEwxTdGV2ZSBTY2hvY2gwWDALBgkqhkiG9w0BAQEDSQAwR
gJBALrAwyYdgxmzNP/ts0Uyf6BpmiJYktU/w4NG67ULaN4B5CnE
z7k57s9o3YY3LecETgQ5iQHmkwlYDTL2fTgVfw0CAQOjgaswgag
wZAYDVR0ZAQH/BFowWDBWMFQxCzAJBgNVBAYTAlVTMTYwNAYDVQ
QKEy1OYXRpb25hbCBBZXJvbmF1dGljcyBhbmQgU3BhY2UgQWRta
W5pc3RyYXRpb24xDTALBgNVBAMTBENSTDEwFwYDVR0BAQH/BA0w
C4AJODMyOTcwODEwMBgGA1UdAgQRMA8ECTgzMjk3MDgyM4ACBSA
wDQYDVR0KBAYwBAMCBkAwCwYJKoZIhvcNAQEEA4GBAH2y1VCEw/
A4zaXzSYZJTTUi3uawbbFiS2yxHvgf28+8Js0OHXk1H1w2d6qOH
H21X82tZXd/0JtG0g1T9usFFBDvYK8O0ebgz/P5ELJnBL2+atOb
EuJy1ZZ0pBDWINR3WkDNLCGiTkCKp0F5EWIrVDwh54NNevkCQRZ
ita+z4IBO
```

6. Paste the contents in the terminal.
7. Press Enter.
8. Verify whether the system shows the following command prompt, indicating the provided CA certificate is valid.

   ```
   config:#
   ```

Setting the BSSID

This command specifies the BSSID.

```
config:#   network wireless BSSID <bssid>
```

Variables:

- <bssid> is either the MAC address of the wireless access point or *none* for automatic selection.

Configuring IPv4 Parameters

An IPv4 configuration command begins with *network ipv4*.

Configuration commands are case sensitive so ensure you capitalize them correctly.

Setting the IPv4 Configuration Mode

This command determines the IP configuration mode.

```
config:#   network ipv4 ipConfigurationMode <mode>
```

Variables:

- <mode> is one of the modes: *dhcp* or *static*.

Mode	Description
dhcp	The IPv4 configuration mode is set to DHCP.
static	The IPv4 configuration mode is set to static IP address.

Setting the IPv4 Preferred Host Name

After selecting DHCP as the IPv4 configuration mode, you can specify the preferred host name, which is optional. The following is the command:

```
config:#   network ipv4 preferredHostName <name>
```

Variables:

- <name> is a host name which:
  - Consists of alphanumeric characters and/or hyphens
  - Cannot begin or end with a hyphen
  - Cannot contain more than 63 characters
  - Cannot contain punctuation marks, spaces, and other symbols

Setting the IPv4 Address

After selecting the static IP configuration mode, you can use this command to assign a permanent IP address to the PX device.

```
config:#   network ipv4 ipAddress <ip address>
```

Variables:

- <ip address> is the IP address being assigned to your PX device. The value ranges from 0.0.0.0 to 255.255.255.255.

Setting the IPv4 Subnet Mask

After selecting the static IP configuration mode, you can use this command to define the subnet mask.

```
config:#   network ipv4 subnetMask <netmask>
```

Variables:

- <netmask> is the subnet mask address. The value ranges from 0.0.0.0 to 255.255.255.255.

Setting the IPv4 Gateway

After selecting the static IP configuration mode, you can use this command to specify the gateway.

```
config:#   network ipv4 gateway <ip address>
```

Variables:

- <ip address> is the IP address of the gateway. The value ranges from 0.0.0.0 to 255.255.255.255.

Setting the IPv4 Primary DNS Server

After selecting the static IP configuration mode, use this command to specify the primary DNS server. If you have selected the DHCP configuration mode, you still can manually specify DNS servers with this command and then override the DHCP-assigned DNS servers. See ***Overriding the IPv4 DHCP-Assigned DNS Server*** (on page 416).

```
config:#   network ipv4 primaryDNSServer <ip address>
```

Variables:

- <ip address> is the IP address of the primary DNS server. The value ranges from 0.0.0.0 to 255.255.255.255.

Setting the IPv4 Secondary DNS Server

After selecting the static IP configuration mode, you can use this command to specify the secondary DNS server. If you have selected the DHCP configuration mode, you still can manually specify DNS servers with this command and then override the DHCP-assigned DNS servers. See ***Overriding the IPv4 DHCP-Assigned DNS Server*** (on page 416).

```
config:#   network ipv4 secondaryDNSServer <ip address>
```

Variables:

- <ip address> is the IP address of the secondary DNS server. The value ranges from 0.0.0.0 to 255.255.255.255.

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

Overriding the IPv4 DHCP-Assigned DNS Server

After specifying the primary/secondary DNS server, you can use this command to override the DHCP-assigned DNS server with the one you specified.

```
config:#   network ipv4 overrideDNS <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	This option overrides the DHCP-assigned DNS server with the primary/secondary DNS server you assign.
disable	This option resumes using the DHCP-assigned DNS server.

Setting IPv4 Static Routes

If the IPv4 network mode is set to static IP and your local network contains two subnets, you can configure static routes to enable or disable communications between the PX and devices in the other subnet.

These commands are prefixed with *network ipv4 staticRoutes*.

- **Add a static route:**

```
config:#   network ipv4 staticRoutes add <dest-1> <hop>
```

- **Delete an existing static route:**

```
config:#   network ipv4 staticRoutes delete <route_ID>
```

- **Modify an existing static route:**

```
config:#   network ipv4 staticRoutes modify <route_ID> <dest-2> <hop>
```

Variables:

- <dest-1> is a combination of the IP address and subnet mask of the other subnet. The format is *IP address/subnet mask*.
- <hop> is the IP address of the next hop router.
- <route_ID> is the ID number of the route setting which you want to delete or modify.
- <dest-2> is a modified route setting that will replace the original route setting. Its format is *IP address/subnet mask*. You can modify either the IP address or the subnet mask or both.

Configuring IPv6 Parameters

An IPv6 configuration command begins with *network ipv6*.

Configuration commands are case sensitive so ensure you capitalize them correctly.

Setting the IPv6 Configuration Mode

This command determines the IP configuration mode.

```
config:#   network ipv6 ipConfigurationMode <mode>
```

Variables:

- <mode> is one of the modes: *automatic* or *static*.

Mode	Description
automatic	The IPv6 configuration mode is set to automatic.
static	The IPv6 configuration mode is set to static IP address.

Setting the IPv6 Preferred Host Name

After selecting DHCP as the IPv6 configuration mode, you can specify the preferred host name, which is optional. The following is the command:

```
config:#   network ipv6 preferredHostName <name>
```

Variables:

- <name> is a host name which:
  - Consists of alphanumeric characters and/or hyphens
  - Cannot begin or end with a hyphen
  - Cannot contain more than 63 characters
  - Cannot contain punctuation marks, spaces, and other symbols

Setting the IPv6 Address

After selecting the static IP configuration mode, you can use this command to assign a permanent IP address to the PX device.

```
config:#   network ipv6 ipAddress <ip address>
```

Variables:

- <ip address> is the IP address being assigned to your PX device. This value uses the IPv6 address format. Note that you must add */xx*, which indicates a prefix length of bits such as /64, to the end of this IPv6 address.

Setting the IPv6 Gateway

After selecting the static IP configuration mode, you can use this command to specify the gateway.

```
config:#   network ipv6 gateway <ip address>
```

Variables:

- <ip address> is the IP address of the gateway. This value uses the IPv6 address format.

Setting the IPv6 Primary DNS Server

After selecting the static IP configuration mode, use this command to specify the primary DNS server. If you have selected the automatic configuration mode, you still can manually specify DNS servers with this command and then override the DHCP-assigned DNS servers. See ***Overriding the IPv6 DHCP-Assigned DNS Server*** (on page 420).

```
config:#   network ipv6 primaryDNSServer <ip address>
```

Variables:

- <ip address> is the IP address of the primary DNS server. This value uses the IPv6 address format.

Setting the IPv6 Secondary DNS Server

After selecting the static IP configuration mode, you can use this command to specify the secondary DNS server. If you have selected the automatic configuration mode, you still can manually specify DNS servers with this command and then override the DHCP-assigned DNS servers. See ***Overriding the IPv6 DHCP-Assigned DNS Server*** (on page 420).

```
config:#   network ipv6 secondaryDNSServer <ip address>
```

Variables:

- <ip address> is the IP address of the secondary DNS server. This value uses the IPv6 address format.

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

Overriding the IPv6 DHCP-Assigned DNS Server

After specifying the primary/secondary DNS server, you can use this command to override the DHCP-assigned DNS server with the one you specified.

```
config:#   network ipv6 overrideDNS <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	This option overrides the DHCP-assigned DNS server with the primary/secondary DNS server you assign.
disable	This option resumes using the DHCP-assigned DNS server.

Setting IPv6 Static Routes

If the IPv6 network mode is set to static IP and your local network contains two subnets, you can configure static routes to enable or disable communications between the PX and devices in the other subnet.

These commands are prefixed with *network ipv6 staticRoutes*.

- **Add a static route:**

```
config:#   network ipv6 staticRoutes add <dest-1> <hop>
```

- **Delete a static route**

```
config:#   network ipv6 staticRoutes delete <route_ID>
```

- **Modify an existing static route:**

```
config:#   network ipv6 staticRoutes modify <route_ID> <dest-2> <hop>
```

Variables:

- <dest-1> is the IP address and prefix length of the subnet where the PX belongs. The format is *IP address/prefix length*.
- <hop> is the IP address of the next hop router.
- <route_ID> is the ID number of the route setting which you want to delete or modify.
- <dest-2> is a modified route setting that will replace the original route setting. Its format is *IP address/prefix length*. You can modify either the IP address or the prefix length or both.

Setting LAN Interface Parameters

A LAN interface configuration command begins with *network interface*.

Changing the LAN Interface Speed

This command determines the LAN interface speed.

```
config:#   network interface LANInterfaceSpeed <option>
```

Variables:

- <option> is one of the options: *auto*, *10Mbps*, and *100Mbps*.

Option	Description
auto	System determines the optimum LAN speed through auto-negotiation.
10Mbps	The LAN speed is always 10 Mbps.
100Mbps	The LAN speed is always 100 Mbps.

Changing the LAN Duplex Mode

This command determines the LAN interface duplex mode.

```
config:#   network interface LANInterfaceDuplexMode <mode>
```

Variables:

- <mode> is one of the modes: *auto*, *half* or *full*.

Option	Description
auto	The PX selects the optimum transmission mode through auto-negotiation.
half	Half duplex: Data is transmitted in one direction (to or from the PX device) at a time.
full	Full duplex: Data is transmitted in both directions simultaneously.

Setting Network Service Parameters

A network service command begins with *network services*.

Setting the HTTP Port

The commands used to configure the HTTP port settings begin with *network services http*.

Change the HTTP port:

```
config:#   network services http port <n>
```

Enable or disable the HTTP port:

```
config:#   network services http enabled <option>
```

Variables:

- <n> is a TCP port number between 1 and 65535. The default HTTP port is 80.
- <option> is one of the options: *true* or *false*.

Option	Description
true	The HTTP port is enabled.
false	The HTTP port is disabled.

Setting the HTTPS Port

The commands used to configure the HTTPS port settings begin with *network services https*.

Change the HTTPS port:

```
config:#   network services https port <n>
```

Enable or disable the HTTPS access:

```
config:#   network services https enabled <option>
```

Variables:

- <n> is a TCP port number between 1 and 65535. The default HTTPS port is 443.
- <option> is one of the options: *true* or *false*.

Option	Description
true	Forces any access to the PX via HTTP to be redirected to HTTPS.
false	No HTTP access is redirected to HTTPS.

Changing the Telnet Configuration

You can enable or disable the Telnet service, or change its TCP port using the CLI commands.

A Telnet command begins with *network services telnet*.

Enabling or Disabling Telnet

This command enables or disables the Telnet service.

```
config:#   network services telnet enabled <option>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	The Telnet service is enabled.

Option	Description
false	The Telnet service is disabled.

Changing the Telnet Port

This command changes the Telnet port.

```
config:#   network services telnet port <n>
```

Variables:

- <n> is a TCP port number between 1 and 65535. The default Telnet port is 23.

Changing the SSH Configuration

You can enable or disable the SSH service, or change its TCP port using the CLI commands.

An SSH command begins with *network services ssh*.

Enabling or Disabling SSH

This command enables or disables the SSH service.

```
config:#   network services ssh enabled <option>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	The SSH service is enabled.
false	The SSH service is disabled.

Changing the SSH Port

This command changes the SSH port.

```
config:#   network services ssh port <n>
```

Variables:

- <n> is a TCP port number between 1 and 65535. The default SSH port is 22.

Determining the SSH Authentication Method

This command syntax determines the SSH authentication method.

```
config:#   network services ssh authentication <auth_method>
```

Variables:

- <option> is one of the options: *passwordOnly*, *publicKeyOnly* or *passwordOrPublicKey*.

Option	Description
passwordOnly	Enables the password-based login only.
publicKeyOnly	Enables the public key-based login only.
passwordOrPublicKey	Enables both the password- and public key-based login. This is the default.

If the public key authentication is selected, you must type a valid SSH public key for each user profile to log in over the SSH connection. See Specifying the SSH Public Key.

Setting the SNMP Configuration

You can enable or disable the SNMP v1/v2c or v3 agent, configure the read and write community strings, or set the MIB-II parameters, such as sysContact, using the CLI commands.

An SNMP command begins with *network services snmp*.

Enabling or Disabling SNMP v1/v2c

This command enables or disables the SNMP v1/v2c protocol.

```
config:#   network services snmp v1/v2c <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	The SNMP v1/v2c protocol is enabled.
disable	The SNMP v1/v2c protocol is disabled.

Enabling or Disabling SNMP v3

This command enables or disables the SNMP v3 protocol.

```
config:#   network services snmp v3 <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	The SNMP v3 protocol is enabled.
disable	The SNMP v3 protocol is disabled.

Setting the SNMP Read Community

This command sets the SNMP read-only community string.

```
config:#   network services snmp readCommunity <string>
```

Variables:

- <string> is a string comprising 4 to 64 ASCII printable characters.
- The string CANNOT include spaces.

Setting the SNMP Write Community

This command sets the SNMP read/write community string.

```
config:#   network services snmp writeCommunity <string>
```

Variables:

- <string> is a string comprising 4 to 64 ASCII printable characters.
- The string CANNOT include spaces.

Setting the sysContact Value

This command sets the SNMP MIB-II sysContact value.

```
config:#   network services snmp sysContact <value>
```

Variables:

- <value> is a string comprising 0 to 255 alphanumeric characters.

Setting the sysName Value

This command sets the SNMP MIB-II sysName value.

```
config:#   network services snmp sysName <value>
```

Variables:

- <value> is a string comprising 0 to 255 alphanumeric characters.

Setting the sysLocation Value

This command sets the SNMP MIB-II sysLocation value.

```
config:#   network services snmp sysLocation <value>
```

Variables:

<value> is a string comprising 0 to 255 alphanumeric characters.

Changing the Modbus Configuration

You can enable or disable the Modbus agent, configure its read-only capability, or change its TCP port.

A Modbus command begins with *network services modbus*.

Enabling or Disabling Modbus

This command enables or disables the Modbus protocol.

```
config:#   network services modbus enabled <option>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	The Modbus agent is enabled.
false	The Modbus agent is disabled.

Enabling or Disabling the Read-Only Mode

This command enables or disables the read-only mode for the Modbus agent.

```
config:#   network services modbus readonly <option>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	The read-only mode is enabled.
false	The read-only mode is disabled.

Changing the Modbus Port

This command changes the Modbus port.

```
config:#   network services modbus port <n>
```

Variables:

- <n> is a TCP port number between 1 and 65535. The default Modbus port is 502.

Enabling or Disabling the Service Advertisement

This command enables or disables the zero configuration protocol, which enables advertising or auto discovery of network services. See ***Enabling Service Advertisement*** (on page 145) for details.

```
config:#   network services zeroconfig enabled <option>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	The zero configuration protocol is enabled.
false	The zero configuration protocol is disabled.

Examples

This section illustrates several network configuration examples.

Example 1 - Networking Mode

The following command enables the wired networking mode.

```
config:#   network mode wired
```

Example 2 - Enabling Both IP Protocols

The following command determines that both IPv4 and IPv6 protocols are enabled.

```
config:#   network ip proto both
```

Example 3 - Wireless Authentication Method

The following command sets the wireless authentication method to PSK.

```
config:#   network wireless authMethod PSK
```

Example 4 - Static IPv4 Configuration

The following command enables the Static IP configuration mode.

```
config:#   network ipv4 ipConfigurationMode static
```

Time Configuration Commands

A time configuration command begins with *time*.

Determining the Time Setup Method

This command determines the method to configure the system date and time.

```
config:#   time method <method>
```

Variables:

- <method> is one of the time setup options: *manual* or *ntp*.

Mode	Description
manual	The date and time settings are customized.
ntp	The date and time settings synchronize with a specified NTP server.

Setting NTP Parameters

A time configuration command that is used to set the NTP parameters begins with *time ntp*.

Specifying the Primary NTP Server

This command specifies the primary time server if synchronization with the NTP server is enabled.

```
config:#   time ntp firstServer <first_server>
```

Variables:

- The <first_server> is the IP address or host name of the primary NTP server.

Specifying the Secondary NTP Server

This command specifies the primary time server if synchronization with the NTP server is enabled.

```
config:#   time ntp secondServer <second_server>
```

Variables:

- The <second_server> is the IP address or host name of the secondary NTP server.

Overriding DHCP-Assigned NTP Servers

This command determines whether the customized NTP server settings override the DHCP-specified NTP servers.

```
config:#   time ntp overrideDHCPProvidedServer <option>
```

Variables:

- <option> is one of these options: *true* or *false*.

Mode	Description
true	Customized NTP server settings override the DHCP-specified NTP servers.
false	Customized NTP server settings do NOT override the DHCP-specified NTP servers.

Setting the Time Zone

The CLI has a list of time zones to configure the date and time for the PX.

```
config:#   time zone
```

After a list of time zones is displayed, type the index number of the time zone or press Enter to cancel.

Example

To set the time zone:

1. Type the time zone command as shown below and press Enter.

   ```
   config:#   time zone
   ```

2. The system shows a list of time zones. Type the index number of the desired time zone and press Enter.
3. Type `apply` for the selected time zone to take effect.

Customizing the Date and Time

If intending to manually configure the date and time, use the following CLI commands to specify them.

Note: You shall set the time configuration method to "manual" prior to customizing the date and time. See **Determining the Time Setup Method** *(on page 431).*

- **Assign the date:**

```
config:#   time set date <yyyy-mm-dd>
```

- **Assign the time:**

```
config:#   time set time <hh:mm:ss>
```

Variables:

Variable	Description
<yyyy-mm-dd>	Type the date in the format of yyyy-mm-dd. For example, type *2015-11-30* for November 30, 2015.
<hh:mm:ss>	Type the time in the format of hh:mm:ss in the 24-hour format. For example, type *13:50:20* for 1:50:20 pm.

Setting the Automatic Daylight Savings Time

This command determines whether the daylight savings time is applied to the time settings.

```
config:#   time autoDST <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Mode	Description
enable	Daylight savings time is enabled.
disable	Daylight savings time is disabled.

Examples

This section illustrates several time configuration examples.

Example 1 - Time Setup Method

The following command sets the date and time settings by using the NTP servers.

```
config:#   time method ntp
```

Example 2 - Primary NTP Server

The following command sets the primary time server to 192.168.80.66.

```
config:#   time ntp firstServer 192.168.80.66
```

Checking the Accessibility of NTP Servers

This command verifies the accessibility of NTP servers specified manually on your PX and then shows the result. For instructions on specifying NTP servers via CLI, see ***Setting NTP Parameters*** (on page 431).

To perform this command successfully, you must:

- Own the "Change Date/Time Settings" permission.
- Customize NTP servers. See ***Setting NTP Parameters*** (on page 431).
- Make the customized NTP servers override the DHCP-assigned ones. See ***Overriding DHCP-Assigned NTP Servers*** (on page 432).

This command is available either in the administrator/user mode or in the configuration mode. See ***Different CLI Modes and Prompts*** (on page 363).

- **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 PX device from a specific or a range of IP addresses.

- An IPv4 firewall configuration command begins with *security ipAccessControl ipv4*.
- An IPv6 firewall configuration command begins with *security ipAccessControl ipv6*.

Modifying Firewall Control Parameters

There are different commands for modifying firewall control parameters.

- *IPv4 commands*

▶ **Enable or disable the IPv4 firewall control feature:**

```
config:#   security ipAccessControl ipv4 enabled <option>
```

▶ **Determine the default IPv4 firewall control policy for inbound traffic:**

```
config:#   security ipAccessControl ipv4 defaultPolicyIn <policy>
```

▶ **Determine the default IPv4 firewall control policy for outbound traffic:**

```
config:#   security ipAccessControl ipv4 defaultPolicyOut <policy>
```

- *IPv6 commands*

▶ **Enable or disable the IPv6 firewall control feature:**

```
config:#   security ipAccessControl ipv6 enabled <option>
```

▶ **Determine the default IPv6 firewall control policy for inbound traffic:**

```
config:#   security ipAccessControl ipv6 defaultPolicyIn <policy>
```

▶ **Determine the default IPv6 firewall control policy for outbound traffic:**

```
config:#   security ipAccessControl ipv6 defaultPolicyOut <policy>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	Enables the IP access control feature.
false	Disables the IP access control feature.

- <policy> is one of the options: *accept, drop* or *reject*.

Option	Description
accept	Accepts traffic from all IP addresses.
drop	Discards traffic from all IP addresses, without sending any failure notification to the source host.
reject	Discards traffic from all IP addresses, and an ICMP message is sent to the source host for failure notification.

Tip: You can combine both commands to modify all firewall control parameters at a time. See **Multi-Command Syntax** *(on page 511).*

Managing Firewall Rules

You can add, delete or modify firewall rules using the CLI commands.

- An IPv4 firewall control rule command begins with *security ipAccessControl ipv4 rule*.
- An IPv6 firewall control rule command begins with *security ipAccessControl ipv6 rule*.

Adding a Firewall Rule

Depending on where you want to add a new firewall rule in the list, the command for adding a rule varies.

- *IPv4 commands*

▶ **Add a new rule to the bottom of the IPv4 rules list:**

```
config:#    security ipAccessControl ipv4 rule add <direction> <ip_mask> <policy>
```

▶ **Add a new IPv4 rule by inserting it above or below a specific rule:**

```
config:#    security ipAccessControl ipv4 rule add <direction> <ip_mask> <policy> <insert>
            <rule_number>
```

-- OR --

```
config:#    security ipAccessControl ipv4 rule add <direction> <insert> <rule_number>
            <ip_mask> <policy>
```

- *IPv6 commands*

▶ **Add a new rule to the bottom of the IPv6 rules list:**

```
config:#    security ipAccessControl ipv6 rule add <direction> <ip_mask> <policy>
```

▶ **Add a new IPv6 rule by inserting it above or below a specific rule:**

```
config:#    security ipAccessControl ipv6 rule add <direction> <ip_mask> <policy> <insert>
            <rule_number>
```

-- OR --

```
config:#    security ipAccessControl ipv6 rule add <direction> <insert> <rule_number>
            <ip_mask> <policy>
```

Variables:

- <direction> is one of the options: *in* or *out*.

Direction	Description
in	Inbound traffic.
out	Outbound traffic.

- <ip_mask> is the combination of the IP address and subnet mask values (or prefix length), which are separated with a slash. For example, an IPv4 combination looks like this: *192.168.94.222/24*.
- <policy> is one of the options: *accept, drop* or *reject*.

Policy	Description
accept	Accepts traffic from/to the specified IP address(es).
drop	Discards traffic from/to the specified IP address(es), without sending any failure notification to the source or destination host.
reject	Discards traffic from/to the specified IP address(es), and an ICMP message is sent to the source or destination host for failure notification.

- <insert> is one of the options: *insertAbove* or *insertBelow*.

Option	Description
insertAbove	Inserts the new rule above the specified rule number. Then: *new rule's number = the specified rule number*
insertBelow	Inserts the new rule below the specified rule number. Then: *new rule's number = the specified rule number + 1*

- <rule_number> is the number of the existing rule which you want to insert the new rule above or below.

Modifying a Firewall Rule

Depending on what to modify in an existing rule, the command varies.

- *IPv4 commands*

▶ **Modify an IPv4 rule's IP address and/or subnet mask:**

```
config:#   security ipAccessControl ipv4 rule modify <direction> <rule_number> ipMask
           <ip_mask>
```

▶ **Modify an IPv4 rule's policy:**

```
config:#   security ipAccessControl ipv4 rule modify <direction> <rule_number> policy
           <policy>
```

▶ **Modify all contents of an existing IPv4 rule:**

```
config:#   security ipAccessControl ipv4 rule modify <direction> <rule_number> ipMask
           <ip_mask> policy <policy>
```

- *IPv6 commands*

Modify an IPv6 rule's IP address and/or prefix length:

```
config:#   security ipAccessControl ipv6 rule modify <direction> <rule_number> ipMask
           <ip_mask>
```

Modify an IPv6 rule's policy:

```
config:#   security ipAccessControl ipv6 rule modify <direction> <rule_number> policy
           <policy>
```

Modify all contents of an IPv6 existing rule:

```
config:#   security ipAccessControl ipv6 rule modify <direction> <rule_number> ipMask
           <ip_mask> policy <policy>
```

Variables:

- <direction> is one of the options: *in* or *out*.

Direction	Description
in	Inbound traffic.
out	Outbound traffic.

- <rule_number> is the number of the existing rule that you want to modify.
- <ip_mask> is the combination of the IP address and subnet mask values (or prefix length), which are separated with a slash. For example, an IPv4 combination looks like this: *192.168.94.222/24*.
- <policy> is one of the options: *accept, drop* or *reject*.

Option	Description
accept	Accepts traffic from/to the specified IP address(es).
drop	Discards traffic from/to the specified IP address(es), without sending any failure notification to the source or destination host.

Option	Description
reject	Discards traffic from/to the specified IP address(es), and an ICMP message is sent to the source or destination host for failure notification.

Deleting a Firewall Rule

The following commands remove a specific IPv4 or IPv6 rule from the list.

- IPv4 commands

```
config:#   security ipAccessControl ipv4 rule delete <direction> <rule_number>
```

- IPv6 commands

```
config:#   security ipAccessControl ipv6 rule delete <direction> <rule_number>
```

Variables:

- <direction> is one of the options: *in* or *out*.

Direction	Description
in	Inbound traffic.
out	Outbound traffic.

- <rule_number> is the number of the existing rule that you want to remove.

Restricted Service Agreement

The CLI command used to set the Restricted Service Agreement feature begins with `security restrictedServiceAgreement`,

Enabling or Disabling the Restricted Service Agreement

This command activates or deactivates the Restricted Service Agreement.

```
config:#   security restrictedServiceAgreement enabled <option>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	Enables the Restricted Service Agreement feature.
false	Disables the Restricted Service Agreement feature.

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

- In the web interface, select the checkbox labeled "I understand and accept the Restricted Service Agreement."

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

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

Specifying the Agreement Contents

This command allows you to create or modify contents of the Restricted Service Agreement.

```
config:#   security restrictedServiceAgreement bannerContent
```

After performing the above command, do the following:

1. Type the text comprising up to 10,000 ASCII characters when the CLI prompts you to enter the content.
2. To end the content:
   a. Press Enter.
   b. Type `--END--` to indicate the end of the content.
   c. Press Enter again.

If the content is successfully entered, the CLI displays this message "Successfully entered Restricted Service Agreement" followed by the total number of entered characters in parentheses.

Note: The new content of Restricted Service Agreement is saved only after typing the `apply` command. See **Quitting Configuration Mode** *(on page 398).*

Example

The following example illustrates how to specify the content of the Restricted Service Agreement.

1. Type the following command and press Enter to start entering the content.

   ```
   config:#   security restrictedServiceAgreement bannerContent
   ```

2. Type the following content when the CLI prompts you to enter the content.

   ```
   IMPORTANT!! You are accessing a PDU. If you are not the
   system administrator, do NOT power off or power cycle
   any outlet without the permission of the system
   administrator.
   ```

3. Press Enter.
4. Type the following:

   ```
   --END--
   ```

5. Press Enter again.
6. Verify that the message "Successfully entered Restricted Service Agreement" is displayed, indicating that the content input is successful.

Login Limitation

The login limitation feature controls login-related limitations, such as password aging, simultaneous logins using the same user name, and the idle time permitted before forcing a user to log out.

A login limitation command begins with *security loginLimits*.

You can combine multiple commands to modify various login limitation parameters at a time. See ***Multi-Command Syntax*** (on page 511).

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 PX 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 511).

▶ **Determine the maximum number of failed logins before blocking a user:**

```
config:#   security userBlocking maximumNumberOfFailedLogins <value1>
```

▶ **Determine how long a user is blocked:**

```
config:#   security userBlocking blockTime <value2>
```

Variables:

- <value1> is an integer between 3 and 10, or *unlimited*, which sets no limit on the maximum number of failed logins and thus disables the user blocking function.
- <value2> is a numeric value ranging from 1 to 1440 minutes (one day), or *infinite*, which blocks the user all the time until the user is unblocked manually.

Strong Passwords

The strong password commands determine whether a strong password is required for login, and what a strong password should contain at least.

A strong password command begins with `security strongPasswords`.

You can combine multiple strong password commands to modify different parameters at a time. See ***Multi-Command Syntax*** (on page 511).

Enabling or Disabling Strong Passwords

This command enables or disables the strong password feature.

```
config:#   security strongPasswords enabled <option>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	Enables the strong password feature.
false	Disables the strong password feature.

Minimum Password Length

This command determines the minimum length of the password.

```
config:#   security strongPasswords minimumLength <value>
```

Variables:

- <value> is an integer between 8 and 32.

Maximum Password Length

This command determines the maximum length of the password.

```
config:#   security strongPasswords maximumLength <value>
```

Variables:

- <value> is an integer between 16 and 64.

Lowercase Character Requirement

This command determines whether a strong password includes at least a lowercase character.

```
config:#    security strongPasswords enforceAtLeastOneLowerCaseCharacter <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	At least one lowercase character is required.
disable	No lowercase character is required.

Uppercase Character Requirement

This command determines whether a strong password includes at least a uppercase character.

```
config:#    security strongPasswords enforceAtLeastOneUpperCaseCharacter <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	At least one uppercase character is required.
disable	No uppercase character is required.

Numeric Character Requirement

This command determines whether a strong password includes at least a numeric character.

```
config:#    security strongPasswords enforceAtLeastOneNumericCharacter <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	At least one numeric character is required.

Option	Description
disable	No numeric character is required.

Special Character Requirement

This command determines whether a strong password includes at least a special character.

```
config:#   security strongPasswords enforceAtLeastOneSpecialCharacter <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	At least one special character is required.
disable	No special character is required.

Maximum Password History

This command determines the number of previous passwords that CANNOT be repeated when changing the password.

```
config:#   security strongPasswords passwordHistoryDepth <value>
```

Variables:

- <value> is an integer between 1 and 12.

Role-Based Access Control

In addition to firewall access control based on IP addresses, you can configure other access control rules that are based on both IP addresses and users' roles.

- An IPv4 role-based access control command begins with *security roleBasedAccessControl ipv4*.
- An IPv6 role-based access control command begins with *security roleBasedAccessControl ipv6*.

Modifying Role-Based Access Control Parameters

There are different commands for modifying role-based access control parameters.

- *IPv4 commands*

▶ **Enable or disable the IPv4 role-based access control feature:**

```
config:#   security roleBasedAccessControl ipv4 enabled <option>
```

▶ **Determine the IPv4 role-based access control policy:**

```
config:#   security roleBasedAccessControl ipv4 defaultPolicy <policy>
```

- *IPv6 commands*

▶ **Enable or disable the IPv6 role-based access control feature:**

```
config:#   security roleBasedAccessControl ipv6 enabled <option>
```

▶ **Determine the IPv6 role-based access control policy:**

```
config:#   security roleBasedAccessControl ipv6 defaultPolicy <policy>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	Enables the role-based access control feature.
false	Disables the role-based access control feature.

- <policy> is one of the options: *allow* or *deny*.

Policy	Description
allow	Accepts traffic from all IP addresses regardless of the user's role.
deny	Drops traffic from all IP addresses regardless of the user's role.

Tip: You can combine both commands to modify all role-based access control parameters at a time. See **Multi-Command Syntax** *(on page 511).*

Managing Role-Based Access Control Rules

You can add, delete or modify role-based access control rules.

- An IPv4 role-based access control command for managing rules begins with *security roleBasedAccessControl ipv4 rule*.
- An IPv6 role-based access control command for managing rules begins with *security roleBasedAccessControl ipv6 rule*.

Adding a Role-Based Access Control Rule

Depending on where you want to add a new rule in the list, the command syntax for adding a rule varies.

- *IPv4 commands*

▶ **Add a new rule to the bottom of the IPv4 rules list:**

```
config:#  security roleBasedAccessControl ipv4 rule add <start_ip> <end_ip> <role>
          <policy>
```

▶ **Add a new IPv4 rule by inserting it above or below a specific rule:**

```
config:#  security roleBasedAccessControl ipv4 rule add <start_ip> <end_ip> <role>
          <policy> <insert> <rule_number>
```

- *IPv6 commands*

▶ **Add a new rule to the bottom of the IPv6 rules list:**

```
config:#  security roleBasedAccessControl ipv6 rule add <start_ip> <end_ip> <role>
          <policy>
```

▶ **Add a new IPv6 rule by inserting it above or below a specific rule:**

```
config:#   security roleBasedAccessControl ipv6 rule add <start_ip> <end_ip> <role>
           <policy> <insert> <rule_number>
```

Variables:

- <start_ip> is the starting IP address.
- <end_ip> is the ending IP address.
- <role> is the role for which you want to create an access control rule.
- <policy> is one of the options: *allow* or *deny*.

Policy	Description
allow	Accepts traffic from the specified IP address range when the user is a member of the specified role
deny	Drops traffic from the specified IP address range when the user is a member of the specified role

- <insert> is one of the options: *insertAbove* or *insertBelow*.

Option	Description
insertAbove	Inserts the new rule above the specified rule number. Then: *new rule's number = the specified rule number*
insertBelow	Inserts the new rule below the specified rule number. Then: *new rule's number = the specified rule number + 1*

- <rule_number> is the number of the existing rule which you want to insert the new rule above or below.

Modifying a Role-Based Access Control Rule

Depending on what to modify in an existing rule, the command syntax varies.

- *IPv4 commands*

▶ **Modify a rule's IPv4 address range:**

```
config:#   security roleBasedAccessControl ipv4 rule modify <rule_number>
           startIpAddress <start_ip> endIpAddress <end_ip>
```

▶ **Modify an IPv4 rule's role:**

```
config:#  security roleBasedAccessControl ipv4 rule modify <rule_number> role <role>
```

▶ **Modify an IPv4 rule's policy:**

```
config:#  security roleBasedAccessControl ipv4 rule modify <rule_number> policy
          <policy>
```

▶ **Modify all contents of an existing IPv4 rule:**

```
config:#  security roleBasedAccessControl ipv4 rule modify <rule_number>
          startIpAddress <start_ip> endIpAddress <end_ip> role <role> policy <policy>
```

- *IPv6 commands*

▶ **Modify a rule's IPv6 address range:**

```
config:#  security roleBasedAccessControl ipv6 rule modify <rule_number>
          startIpAddress <start_ip> endIpAddress <end_ip>
```

▶ **Modify an IPv6 rule's role:**

```
config:#  security roleBasedAccessControl ipv6 rule modify <rule_number> role <role>
```

▶ **Modify an IPv6 rule's policy:**

```
config:#  security roleBasedAccessControl ipv6 rule modify <rule_number> policy
          <policy>
```

▶ **Modify all contents of an existing IPv6 rule:**

```
config:#    security roleBasedAccessControl ipv6 rule modify <rule_number>
            startIpAddress <start_ip> endIpAddress <end_ip> role <role> policy <policy>
```

Variables:

- <rule_number> is the number of the existing rule that you want to modify.
- <start_ip> is the starting IP address.
- <end_ip> is the ending IP address.
- <role> is one of the existing roles.
- <policy> is one of the options: *allow* or *deny*.

Policy	Description
allow	Accepts traffic from the specified IP address range when the user is a member of the specified role
deny	Drops traffic from the specified IP address range when the user is a member of the specified role

Deleting a Role-Based Access Control Rule

These commands remove a specific rule from the list.

▶ IPv4 commands

```
config:#    security roleBasedAccessControl ipv4 rule delete <rule_number>
```

▶ IPv6 commands

```
config:#    security roleBasedAccessControl ipv6 rule delete <rule_number>
```

Variables:

- <rule_number> is the number of the existing rule that you want to remove.

Enabling or Disabling Front Panel Outlet Switching

This section applies to outlet-switching capable models only.

The following CLI commands control whether you can turn on or off an outlet by operating the front panel display.

- **To enable the front panel outlet control feature:**

```
config:#   security frontPanelPermissions add switchOutlet
```

- **To disable the front panel outlet control feature:**

```
config:#   security frontPanelPermissions remove switchOutlet
```

Enabling or Disabling Front Panel Actuator Control

This section applies to PX3 phase II models only. A PX3 phase I model does NOT support this feature.

The following CLI commands control whether you can turn on or off a connected actuator by operating the front panel LCD display.

- **To enable the front panel actuator control feature:**

```
config:#   security frontPanelPermissions add switchActuator
```

- **To disable the front panel actuator control feature:**

```
config:#   security frontPanelPermissions remove switchActuator
```

Tip: If your PDU supports multiple front panel permissions, you can combine them into one command by adding a semicolon (;) between different permissions. For example, the following CLI command enables both front panel actuator control and outlet switching functions simultaneously.

```
security frontPanelPermissions add
switchActuator;switchOutlet
```

Examples

This section illustrates several security configuration examples.

Example 1 - IPv4 Firewall Control Configuration

The following command sets up two parameters of the IPv4 access control feature.

```
config:#   security ipAccessControl ipv4 enabled true defaultPolicyIn accept
           defaultPolicyOut accept
```

Results:

- The IPv4 access control feature is enabled.
- The default policy for inbound traffic is set to "accept."
- The default policy for outbound traffic is set to "accept."

Example 2 - Adding an IPv4 Firewall Rule

The following command adds a new IPv4 access control rule and specifies its location in the list.

```
config:#   security ipAccessControl ipv4 rule add 192.168.84.123/24 accept
           insertAbove 5
```

Results:

- A new IPv4 firewall control rule is added to accept all packets sent from the IPv4 address 192.168.84.123.
- The newly-added rule is inserted above the 5th rule. That is, the new rule becomes the 5th rule, and the original 5th rule becomes the 6th rule.

Example 3 - User Blocking

The following command sets up two user blocking parameters.

```
config:#   security userBlocking maximumNumberOfFailedLogins 5 blockTime 30
```

Results:

- The maximum number of failed logins is set to 5.
- The user blocking time is set to 30 minutes.

Example 4 - Adding an IPv4 Role-based Access Control Rule

The following command creates a newIPv4 role-based access control rule and specifies its location in the list.

```
config:#   security roleBasedAccessControl ipv4 rule add 192.168.78.50 192.168.90.100
admin deny insertAbove 3
```

Results:

- A new IPv4 role-based access control rule is added, dropping all packets from any IPv4 address between 192.168.78.50 and 192.168.90.100 when the user is a member of the role "admin."
- The newly-added IPv4 rule is inserted above the 3rd rule. That is, the new rule becomes the 3rd rule, and the original 3rd rule becomes the 4th rule.

Outlet Configuration Commands

An outlet configuration command begins with *outlet*. Such a command allows you to configure an individual outlet.

Changing the Outlet Name

This command names an outlet.

```
config:#   outlet <n> name "<name>"
```

Variables:

- <n> is the number of the outlet that you want to configure.
- <name> is a string comprising up to 32 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 PX 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 400).*

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 401).*

Example - Outlet Naming

The following command assigns the name "Win XP" to outlet 8.

```
config:#   outlet 8 name "Win XP"
```

Inlet Configuration Commands

An inlet configuration command begins with *inlet*. You can configure an inlet by using the inlet configuration command.

Changing the Inlet Name

This command syntax names an inlet.

```
config:#   inlet <n> name "<name>"
```

Variables:

- <n> is the number of the inlet that you want to configure. For a single-inlet PDU, <n> is always the number 1. The value is an integer between 1 and 50.
- <name> is a string comprising up to 32 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.

Enabling or Disabling 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 the number 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 PX device contains multiple inlets, this command names the 1st inlet.

```
config:#   inlet 1 name "AC source"
```

Overcurrent Protector Configuration Commands

An overcurrent protector configuration command begins with *ocp*. The command configures an individual circuit breaker or fuse which protects outlets.

Changing the Overcurrent Protector Name

This command names a circuit breaker or a fuse which protects outlets on your PX.

```
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 32 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 PX 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 511).*

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, PX 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 397).
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 511).

Change a user's full name:

```
config:#   user modify <name> fullName "<full_name>"
```

Change a user's telephone number:

```
config:#   user modify <name> telephoneNumber "<phone_number>"
```

Change a user's email address:

```
config:#   user modify <name> eMailAddress <email_address>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <full_name> is a string comprising up to 32 ASCII printable characters. The <full_name> variable must be enclosed in quotes when it contains spaces.
- <phone_number> is the phone number that can reach the specified user. The <phone_number> variable must be enclosed in quotes when it contains spaces.
- <email_address> is the email address of the specified user.

Enabling or Disabling a User Profile

This command enables or disables a user profile. A user can log in to the PX device only after that user's user profile is enabled.

```
config:#   user modify <name> enabled <option>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option> is one of the options: *true* or *false*.

Option	Description
true	Enables the specified user profile.
false	Disables the specified user profile.

Forcing a Password Change

This command determines whether the password change is forced when a user logs in to the specified user profile next time.

```
config:#   user modify <name> forcePasswordChangeOnNextLogin <option>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option> is one of the options: *true* or *false*.

Option	Description
true	A password change is forced on the user's next login.
false	No password change is forced on the user's next login.

Modifying SNMPv3 Settings

There are different commands to modify the SNMPv3 parameters of a specific user profile. You can combine all of the following commands to modify the SNMPv3 parameters at a time. See ***Multi-Command Syntax*** (on page 511).

Enable or disable the SNMP v3 access to PX for the specified user:

```
config:#   user modify <name> snmpV3Access <option1>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option1> is one of the options: *enable* or *disable*.

Option	Description
enable	Enables the SNMP v3 access permission for the specified user.
disable	Disables the SNMP v3 access permission for the specified user.

Determine the security level:

```
config:#   user modify <name> securityLevel <option2>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option2> is one of the options: *noAuthNoPriv*, *authNoPriv* or *authPriv*.

Option	Description
noAuthNoPriv	No authentication and no privacy.
authNoPriv	Authentication and no privacy.
authPriv	Authentication and privacy.

Determine whether the authentication passphrase is identical to the password:

```
config:#    user modify <name> userPasswordAsAuthenticationPassphrase <option3>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option3> is one of the options: *true* or *false*.

Option	Description
true	Authentication passphrase is identical to the password.
false	Authentication passphrase is different from the password.

Determine the authentication passphrase:

```
config:#    user modify <name> authenticationPassPhrase <authentication_passphrase>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <authentication_passphrase> is a string used as an authentication passphrase, comprising 8 to 32 ASCII printable characters.

Determine whether the privacy passphrase is identical to the authentication passphrase:

```
config:#    user modify <name> useAuthenticationPassPhraseAsPrivacyPassPhrase <option4>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option4> is one of the options: *true* or *false*.

Option	Description
true	Privacy passphrase is identical to the authentication passphrase.
false	Privacy passphrase is different from the authentication passphrase.

Determine the privacy passphrase:

```
config:#   user modify <name> privacyPassPhrase <privacy_passphrase>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <privacy_passphrase> is a string used as a privacy passphrase, comprising 8 to 32 ASCII printable characters.

Determine the authentication protocol:

```
config:#   user modify <name> authenticationProtocol <option5>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option5> is one of the options: *MD5* or *SHA-1*.

Option	Description
MD5	MD5 authentication protocol is applied.
SHA-1	SHA-1 authentication protocol is applied.

Determine the privacy protocol:

```
config:#   user modify <name> privacyProtocol <option6>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option6> is one of the options: *DES* or *AES-128*.

Option	Description
DES	DES privacy protocol is applied.
AES-128	AES-128 privacy protocol is applied.

Changing the Role(s)

This command changes the role(s) of a specific user.

```
config:#   user modify <name> roles <roles>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <roles> is a role or a list of comma-separated roles assigned to the specified user profile. See ***All Privileges*** (on page 474).

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 511).

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 PX user interfaces for all users via CLI, see **Setting Default Measurement Units** *(on page 470).*

Set the preferred temperature unit:

```
config:#   user modify <name> preferredTemperatureUnit <option1>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option1> is one of the options: *C* or *F*.

Option	Description
C	This option displays the temperature in Celsius.
F	This option displays the temperature in Fahrenheit.

Set the preferred length unit:

```
config:#   user modify <name> preferredLengthUnit <option2>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option2> is one of the options: *meter* or *feet*.

Option	Description
meter	This option displays the length or height in meters.
feet	This option displays the length or height in feet.

Set the preferred pressure unit:

```
config:#   user modify <name> preferredPressureUnit <option3>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option3> is one of the options: *pascal* or *psi*.

Option	Description
pascal	This option displays the pressure value in Pascals (Pa).
psi	This option displays the pressure value in psi.

Changing the SSH Public Key

This command changes the role(s) of a specific user.

```
config:#   user modify <name> sshPublicKey
```

After performing the above command, you are prompted to enter the SSH public key. You can either enter the new SSH public key or simply press Enter without entering any SSH public key to remove the existing SSH public key.

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 397).
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 PX 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 397).
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 PX 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 511).

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

Tip: To change the preferred measurement units displayed in the PX user interfaces for a specific user via CLI, see **Changing Measurement Units** *(on page 467)*.

▶ **Set the default temperature unit:**

```
config:#   user defaultpreferences preferredTemperatureUnit <option1>
```

Variables:

- <option1> is one of the options: *C* or *F*.

Option	Description
C	This option displays the temperature in Celsius.
F	This option displays the temperature in Fahrenheit.

▶ **Set the default length unit:**

```
config:#   user defaultpreferences preferredLengthUnit <option2>
```

Variables:

- <option2> is one of the options: *meter* or *feet*.

Option	Description
meter	This option displays the length or height in meters.
feet	This option displays the length or height in feet.

Set the default pressure unit:

```
config:#   user defaultpreferences preferredPressureUnit <option3>
```

Variables:

- <option3> is one of the options: *pascal* or *psi*.

Option	Description
pascal	This option displays the pressure value in Pascals (Pa).
psi	This option displays the pressure value in psi.

Examples

This section illustrates several user configuration examples.

Example 1 - Creating a User Profile

The following command creates a new user profile and sets two parameters for the new user.

```
config:#   user create May enable admin
```

Results:

- A new user profile "May" is created.
- The new user profile is enabled.
- The **admin** role is assigned to the new user profile.

Example 2 - Modifying a User's Roles

The following command assigns two roles to the user "May."

```
config:#   user modify May roles admin,tester
```

Results:

- The user May has the union of all privileges of "admin" and "tester."

Example 3 - Default Measurement Units

The following command sets all default measurement units at a time.

```
config:#    user defaultpreferences preferredTemperatureUnit F preferredLengthUnit feet
            preferredPressureUnit psi
```

Results:

- The default temperature unit is set to Fahrenheit.
- The default length unit is set to feet.
- The default pressure unit is set to psi.

Role Configuration Commands

A role configuration command begins with *role*.

Creating a Role

This command creates a new role, with a list of semicolon-separated privileges assigned to the role.

```
config:#    role create <name> <privilege1>;<privilege2>;<privilege3>...
```

If a specific privilege contains any arguments, that privilege should be followed by a colon and the argument(s).

```
config:#    role create <name> <privilege1>:<argument1>,<argument2>...;
            <privilege2>:<argument1>,<argument2>...;
            <privilege3>:<argument1>,<argument2>...;
            ...
```

Variables:

- <name> is a string comprising up to 32 ASCII printable characters.
- <privilege1>, <privilege2>, <privilege3> and the like are names of the privileges assigned to the role. Separate each privilege with a semi-colon. See ***All Privileges*** (on page 474).
- <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
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)
switchOutlet*	Switch Outlet
switchActuator**	Switch Actuator
switchTransferSwitch	Switch Transfer Switch
viewEventSetup	View Event Settings
viewEverything	Unrestricted View Privileges

Privilege	Description
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 "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 "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 PX web interface. It is an integer between 1 and 32.

Modifying a Role

You can modify diverse parameters of an existing role, including its privileges.

Modify a role's description:

```
config:#   role modify <name> description "<description>"
```

Variables:

- <name> is a string comprising up to 32 ASCII printable characters.
- <description> is a description comprising alphanumeric characters. The <description> variable must be enclosed in quotes when it contains spaces.

Add more privileges to a specific role:

```
config:#   role modify <name> addPrivileges
           <privilege1>;<privilege2>;<privilege3>...
```

If a specific privilege contains any arguments, add a colon and the argument(s) after that privilege.

```
config:#   role modify <name> addPrivileges
           <privilege1>:<argument1>,<argument2>...;
           <privilege2>:<argument1>,<argument2>...;
           <privilege3>:<argument1>,<argument2>...;
           ...
```

Variables:

- <name> is a string comprising up to 32 ASCII printable characters.
- <privilege1>, <privilege2>, <privilege3> and the like are names of the privileges assigned to the role. Separate each privilege with a semi-colon. See ***All Privileges*** (on page 474).
- <argument1>, <argument2> and the like are arguments set for a particular privilege. Separate a privilege and its argument(s) with a colon, and separate arguments with a comma if there are more than one argument for a privilege.

Remove specific privileges from a role:

```
config:#   role modify <name> removePrivileges
           <privilege1>;<privilege2>;<privilege3>...
```

If a specific privilege contains any arguments, add a colon and the argument(s) after that privilege.

```
config:#   role modify <name> removePrivileges
           <privilege1>:<argument1>,<argument2>...;
           <privilege2>:<argument1>,<argument2>...;
           <privilege3>:<argument1>,<argument2>...;
           ...
```

Note: When removing privileges from a role, make sure the specified privileges and arguments (if any) exactly match those assigned to the role. Otherwise, the command fails to remove specified privileges that are not available.

Variables:

- <name> is a string comprising up to 32 ASCII printable characters.
- <privilege1>, <privilege2>, <privilege3> and the like are names of the privileges assigned to the role. Separate each privilege with a semi-colon. See ***All Privileges*** (on page 474).
- <argument1>, <argument2> and the like are arguments set for a particular privilege. Separate a privilege and its argument(s) with a colon, and separate arguments with a comma if there are more than one argument for a privilege.

Deleting a Role

This command deletes an existing role.

```
config:#   role delete <name>
```

Example - Creating a Role

The following command creates a new role and assigns privileges to the role.

```
config:#   role create tester firmwareUpdate;viewEventSetup
```

Results:

- A new role "tester" is created.
- Two privileges are assigned to the role: firmwareUpdate (Firmware Update) and viewEventSetup (View Event Settings).

Environmental Sensor Configuration Commands

An environmental sensor configuration command begins with *externalsensor*. You can configure the name and location parameters of an individual environmental sensor.

Note: To configure an actuator, see **Actuator Configuration Commands** *(on page 495).*

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 PX web interface or using the command "`show externalsensors <n>`" in the CLI. It is an integer between 1 and 32.
- <name> is a string comprising up to 32 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.

Note: To name an actuator, see **Actuator Configuration Commands** *(on page 495).*

Specifying the CC Sensor Type

Raritan's contact closure sensor (DPX-CC2-TR) supports the connection of diverse third-party or Raritan's detectors/switches. You must specify the type of connected detector/switch for proper operation. Use this command when you need to specify the sensor type.

```
config:#   externalsensor <n> sensorSubType <sensor_type>
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is available in the PX web interface or using the command "`show externalsensors <n>`" in the CLI. It is an integer between 1 and 32.
- <sensor_type> is one of these types: *contact*, *smokeDetection*, *waterDetection* or *vibration*.

Type	Description
contact	The connected detector/switch is for detection of door lock or door closed/open status.
smokeDetection	The connected detector/switch is for detection of the smoke presence.
waterDetection	The connected detector/switch is for detection of the water presence.
vibration	The connected detector/switch is for detection of the vibration.

Setting the X Coordinate

This command specifies the X coordinate of an environmental sensor.

```
config:#   externalsensor <n> xlabel "<coordinate>"
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is available in the PX web interface or using the command "`show externalsensors <n>`" in the CLI. It is an integer between 1 and 32.
- <coordinate> is a string comprising up to 24 ASCII printable characters, and it must be enclosed in quotes.

Setting the Y Coordinate

This command specifies the Y coordinate of an environmental sensor.

```
config:#   externalsensor <n> ylabel "<coordinate>"
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is available in the PX web interface or using the command "`show externalsensors <n>`" in the CLI. It is an integer between 1 and 32.
- <coordinate> is a string comprising up to 24 ASCII printable characters, and it must be enclosed in quotes.

Setting the Z Coordinate

This command specifies the Z coordinate of an environmental sensor.

```
config:#   externalsensor <n> zlabel "<coordinate>"
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is available in the PX web interface or using the command "`show externalsensors` <n>" in the CLI. It is an integer between 1 and 32.
- Depending on the Z coordinate format you set, there are two types of values for the <coordinate> variable:

Type	Description
Free form	<coordinate> is a string comprising up to 24 ASCII printable characters, and it must be enclosed in quotes.
Rack units	<coordinate> is an integer number in rack units.

Note: To specify the Z coordinate using the rack units, see **Setting the Z Coordinate Format for Environmental Sensors** *(on page 404).*

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 PX web interface or using the command "`show externalsensors` <n>" in the CLI. It is an integer between 1 and 32.
- <description> is a string comprising up to 64 ASCII printable characters, and it must be enclosed in quotes.

Using Default Thresholds

This command determines whether default thresholds, including the deassertion hysteresis and assertion timeout, are applied to a specific environmental sensor.

```
config:#   externalsensor <n> useDefaultThresholds <option>
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is available in the PX web interface or using the command "`show externalsensors <n>`" in the CLI. It is an integer between 1 and 32.
- <option> is one of the options: *true* or *false*.

Option	Description
true	Default thresholds are selected as the threshold option for the specified sensor.
false	Sensor-specific thresholds are selected as the threshold option for the specified sensor.

Setting the Alarmed to Normal Delay for DX-PIR

This command determines the value of the Alarmed to Normal Delay setting for a DX-PIR presence detector.

```
config:#   externalsensor <n> alarmedToNormalDelay <time>
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is available in the PX web interface or using the command "`show externalsensors <n>`" in the CLI. It is an integer between 1 and 32.
- <time> is an integer number in seconds, ranging between 0 and 300.

Examples

This section illustrates several environmental sensor configuration examples.

Example 1 - Environmental Sensor Naming

The following command assigns the name "Cabinet humidity" to the environmental sensor with the ID number 4.

```
config:#   externalsensor 4 name "Cabinet humidity"
```

Example 2 - Sensor Threshold Selection

The following command sets the environmental sensor #1 to use the default thresholds, including the deassertion hysteresis and assertion timeout, as its threshold settings.

```
config:#   externalsensor 1 useDefaultThresholds true
```

Configuring Environmental Sensors' Default Thresholds

You can set the default values of upper and lower thresholds, deassertion hysteresis and assertion timeout on a sensor type basis, including temperature, humidity, air pressure and air flow sensors. The default thresholds automatically apply to all environmental sensors that are newly detected or added.

A default threshold configuration command begins with *defaultThresholds*.

You can configure various default threshold settings for the same sensor type at a time by combining multiple commands. See ***Multi-Command Syntax*** (on page 511).

- **Set the Default Upper Critical Threshold for a specific sensor type:**

```
config:#   defaultThresholds <sensor type> upperCritical <value>
```

- **Set the Default Upper Warning Threshold for a specific sensor type:**

```
config:#   defaultThresholds <sensor type> upperWarning <value>
```

- **Set the Default Lower Critical Threshold for a specific sensor type:**

```
config:#   defaultThresholds <sensor type> lowerCritical <value>
```

- **Set the Default Lower Warning Threshold for a specific sensor type:**

```
config:#    defaultThresholds <sensor type> lowerWarning <value>
```

Set the Default Deassertion Hysteresis for a specific sensor type:

```
config:#    defaultThresholds <sensor type> hysteresis <hy_value>
```

Set the Default Assertion Timeout for a specific sensor type:

```
config:#    defaultThresholds <sensor type> assertionTimeout <as_value>
```

Variables:

- <sensor type> is one of the following numeric sensor types:

Sensor types	Description
absoluteHumidity	Absolute humidity sensors
relativeHumidity	Relative humidity sensors
temperature	Temperature sensors
airPressure	Air pressure sensors
airFlow	Air flow sensors
vibration	Vibration sensors

- <value> is the value for the specified threshold of the specified sensor type. Note that diverse sensor types use different measurement units.

Sensor types	Measurement units
absoluteHumidity	g/m^3 (that is, g/m^3)
relativeHumidity	%
temperature	Degrees Celsius (°C) or Fahrenheit (°F), depending on your measurement unit settings.
airPressure	Pascal (Pa) or psi, depending on your measurement unit settings.
airFlow	m/s
vibration	g

- <hy_value> is the deassertion hysteresis value applied to the specified sensor type.
- <as_value> is the assertion timeout value applied to the specified sensor type. It ranges from 0 to 100 (samples).

Example - Default Upper Thresholds for Temperature

It is assumed that your preferred measurement unit for temperature is set to degrees Celsius. Then the following command sets the default Upper Warning threshold to 20°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:

- Outlets
- 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 Outlet Sensors

A sensor configuration command for outlets begins with *sensor outlet*.

You can configure various outlet sensor threshold settings at a time by combining multiple commands. See ***Multi-Command Syntax*** (on page 511).

Set the Upper Critical threshold for an outlet sensor:

```
config:#   sensor outlet <n> <sensor type> upperCritical <option>
```

Set the Upper Warning threshold for an outlet sensor:

```
config:#   sensor outlet <n> <sensor type> upperWarning <option>
```

Set the Lower Critical threshold for an outlet sensor:

```
config:#    sensor outlet <n> <sensor type> lowerCritical <option>
```

Set the Lower Warning threshold for an outlet sensor:

```
config:#    sensor outlet <n> <sensor type> lowerWarning <option>
```

Set the deassertion hysteresis for an outlet sensor:

```
config:#    sensor outlet <n> <sensor type> hysteresis <hy_value>
```

Set the assertion timeout for an outlet sensor:

```
config:#    sensor outlet <n> <sensor type> assertionTimeout <as_value>
```

Variables:

- <n> is the number of the outlet that you want to configure.
- <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
lineFrequency	Line frequency 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 outlet sensor.
disable	Disables the specified threshold for a specific outlet sensor.

Option	Description
A numeric value	Sets a value for the specified threshold of a specific outlet sensor and enables this threshold at the same time.

- <hy_value> is a numeric value that is assigned to the hysteresis for the specified outlet sensor. See ***"To De-assert" and Deassertion Hysteresis*** (on page 672).
- <as_value> is a number in samples that is assigned to the assertion timeout for the specified outlet sensor. See ***"To Assert" and Assertion Timeout*** (on page 670).

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 511).

▶ **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 the number 1.
- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
peakCurrent	Peak 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
residualCurrent	Residual current 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.
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 672).
- <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 670).

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 511).

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.
- <p> is the label of the inlet pole that you want to configure.

Pole	Label <p>	Current sensor	Voltage sensor
1	**L1**	L1	L1 - L2
2	**L2**	L2	L2 - L3
3	**L3**	L3	L3 - L1

- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor
unbalancedCurrent	Unbalanced load sensor

Note: If the requested sensor type is not supported, the "Sensor is not available" message is displayed.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the specified threshold for the specified inlet pole sensor.
disable	Disables the specified threshold for the specified inlet pole sensor.
A numeric value	Sets a value for the specified threshold of the specified inlet pole sensor and enables this threshold at the same time.

- <hy_value> is a numeric value that is assigned to the hysteresis for the specified inlet pole sensor. See ***"To De-assert" and Deassertion Hysteresis*** (on page 672).
- <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 670).

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 511).

▶ **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.

Option	Description
disable	Disables the specified threshold for the overcurrent protector sensor.
A numeric value	Sets a value for the specified threshold of the overcurrent protector sensor and enables this threshold at the same time.

- <hy_value> is a numeric value that is assigned to the hysteresis for the specified overcurrent protector sensor. See ***"To De-assert" and Deassertion Hysteresis*** (on page 672).
- <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 670).

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 511).

▶ **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 PX web interface or using the command "`show externalsensors <n>`" in the CLI. It is an integer between 1 and 32.
- <sensor type> is one of these sensor types: *temperature, absoluteHumidity, relativeHumidity, airPressure, airFlow* or *vibration*.

Note: If the specified sensor type does not match the type of the specified environmental sensor, this error message appears: "Specified sensor type 'XXX' does not match the sensor's type (<sensortype>)," where XXX is the specified sensor type, and <sensortype> is the correct sensor type.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the specified threshold for a specific environmental sensor.
disable	Disables the specified threshold for a specific environmental sensor.
A numeric value	Sets a value for the specified threshold of a specific environmental sensor and enables this threshold at the same time.

- <hy_value> is a numeric value that is assigned to the hysteresis for the specified environmental sensor. See ***"To De-assert" and Deassertion Hysteresis*** (on page 672).
- <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 670).

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 511).

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 PX web interface or CLI. It is an integer starting at 1.
- <name> is a string comprising up to 32 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.
- <coordinate> is a string comprising up to 24 ASCII printable characters, and it must be enclosed in quotes.
- There are two types of values for the <z_label> variable, depending on the Z coordinate format you set:

Type	Description
Free form	<coordinate> is a string comprising up to 24 ASCII printable characters, and it must be enclosed in quotes.
Rack units	<coordinate> is an integer number in rack units.

Note: To specify the Z coordinate using the rack units, see **Setting the Z Coordinate Format for Environmental Sensors** *(on page 404).*

- <description> is a sentence or paragraph comprising up to 64 ASCII printable characters, and it must be enclosed in quotes.

Example - Actuator Naming

The following command assigns the name "Door lock" to the actuator whose ID number is 9.

```
config:#   actuator 9 name "Door lock"
```

Server Reachability Configuration Commands

You can use the CLI to add or delete an IT device, such as a server, from the server reachability list, or modify the settings for a monitored IT device. A server reachability configuration command begins with *serverReachability*.

Adding a Monitored Device

This command adds a new IT device to the server reachability list.

```
config:#   serverReachability add <IP_host> <enable> <succ_ping>
           <fail_ping> <succ_wait> <fail_wait> <resume> <disable_count>
```

Variables:

- <IP_host> is the IP address or host name of the IT device that you want to add.
- <enable> is one of the options: *true* or *false*.

Option	Description
true	Enables the ping monitoring feature for the newly added device.
false	Disables the ping monitoring feature for the newly added device.

- <succ_ping> is the number of successful pings for declaring the monitored device "Reachable." Valid range is 0 to 200.
- <fail_ping> is the number of consecutive unsuccessful pings for declaring the monitored device "Unreachable." Valid range is 1 to 100.
- <succ_wait> is the wait time to send the next ping after a successful ping. Valid range is 5 to 600 (seconds).
- <fail_wait> is the wait time to send the next ping after a unsuccessful ping. Valid range is 3 to 600 (seconds).
- <resume> is the wait time before the PX 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 PX 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 511).

▶ **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 PX 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 PX 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 PX device is enabled.

```
config:#   energywise enabled <option>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	The Cisco EnergyWise feature is enabled.
false	The Cisco EnergyWise feature is disabled.

Specifying the EnergyWise Domain

This command syntax specifies to which Cisco® EnergyWise domain the PX device belongs.

```
config:#   energywise domain <name>
```

Variables:

- <name> is a string comprising up to 127 ASCII printable characters. Spaces and asterisks are NOT acceptable.

Specifying the EnergyWise Secret

This command syntax specifies the password (secret) to enter the Cisco® EnergyWise domain.

```
config:#   energywise secret <password>
```

Variables:

- <password> is a string comprising up to 127 ASCII printable characters. Spaces and asterisks are NOT acceptable.

Changing the UDP Port

This command syntax specifies the UDP port for communications in the Cisco® EnergyWise domain.

```
config:#   energywise port <port>
```

Variables:

- <port> is the UDP port number ranging between 1 and 65535.

Setting the Polling Interval

This command syntax determines the polling interval at which the Cisco® EnergyWise domain queries the PX device.

```
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 PX is enabled.
- The UDP port is set to 10288.

USB-Cascading Configuration Commands

A USB-cascading configuration command begins with *cascading*. You can set the cascading mode on the master device.

Note: You CANNOT change the cascading mode on slave devices.

Configuring the Cascading Mode

This command determines the cascading mode.

```
config:#   cascading mode <mode>
```

Variables:

- <mode> is one of the following cascading modes:

Mode	Description
bridging	The network bridging mode, where each cascaded device is assigned a unique IP address.
portForwarding	The port forwarding mode, where every cascaded device in the chain shares the same IP address, with diverse port numbers assigned.

Asset Management Commands

You can use the CLI commands to change the settings of the connected asset sensor (if any) or the settings of LEDs on the asset sensor.

Asset Sensor Management

An asset sensor management configuration command begins with `assetStrip`.

Naming an Asset Sensor

This command syntax names or changes the name of an asset sensor connected to the PX device.

```
config:#   assetStrip <n> name "<name>"
```

Variables:

- <n> is the number of the FEATURE port where the selected asset sensor is physically connected. For the PX device with only one FEATURE port, the number is always 1.
- <name> is a string comprising up to 32 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.

Specifying the Number of Rack Units

This command syntax specifies the total number of rack units on an asset sensor connected to the PX device.

```
config:#   assetStrip <n> numberOfRackUnits <number>
```

Note: For the Raritan asset sensor, a rack unit refers to a tag port.

Variables:

- <n> is the number of the FEATURE port where the selected asset sensor is physically connected. For the PX device with only one FEATURE port, the number is always 1.
- <number> is the total number of rack units available on the connected asset sensor. This value ranges from 8 to 64.

Specifying the Rack Unit Numbering Mode

This command syntax specifies the numbering mode of rack units on the asset sensors connected to the PX device. The numbering mode changes the rack unit numbers.

```
config:#   assetStrip <n> rackUnitNumberingMode <mode>
```

Variables:

- <n> is the number of the FEATURE port where the selected asset sensor is physically connected. For the PX device with only one FEATURE port, the number is always 1.
- <mode> is one of the numbering modes: *topDown* or *bottomUp*.

Mode	Description
topDown	The rack units are numbered in the ascending order from the highest to the lowest rack unit.
bottomUp	The rack units are numbered in the descending order from the highest to the lowest rack unit.

Specifying the Rack Unit Numbering Offset

This command syntax specifies the starting number of rack units on the asset sensors connected to the PX device.

```
config:#   assetStrip <n> rackUnitNumberingOffset <number>
```

Variables:

- <n> is the number of the FEATURE port where the selected asset sensor is physically connected. For the PX device with only one FEATURE port, the number is always 1.
- <number> is a starting number for numbering rack units on the connected asset sensor. This value is an integer number.

Specifying the Asset Sensor Orientation

This command syntax specifies the orientation of the asset sensors connected to the PX device. Usually you do not need to perform this command unless your asset sensors do NOT come with the tilt sensor, causing the PX unable to detect the asset sensors' orientation.

```
config:#   assetStrip <n> assetStripOrientation <orientation>
```

Variables:

- <n> is the number of the FEATURE port where the selected asset sensor is physically connected. For the PX device with only one FEATURE port, the number is always 1.
- <orientation> is one of the options: *topConnector* or *bottomConnector*.

Orientation	Description
topConnector	This option indicates that the asset sensor is mounted with the RJ-45 connector located on the top.
bottomConnector	This option indicates that the asset sensor is mounted with the RJ-45 connector located at the bottom.

Setting LED Colors for Connected Tags

This command syntax sets the LED color for all rack units on the asset sensor #1 to indicate the presence of a connected asset tag.

```
config:#   assetStrip <n> LEDColorForConnectedTags <color>
```

Variables:

- <color> is the hexadecimal RGB value of a color in HTML format. The <color> variable ranges from #000000 to #FFFFFF.

Setting LED Colors for Disconnected Tags

This command syntax sets the LED color for all rack units on the connected asset sensor(s) to indicate the absence of a connected asset tag.

```
config:#   assetStrip <n> LEDColorForDisconnectedTags <color>
```

Variables:

- <color> is the hexadecimal RGB value of a color in HTML format. The <color> variable ranges from #000000 to #FFFFFF.

Rack Unit Configuration

For the Raritan asset sensor, a rack unit refers to a tag port. A rack unit configuration command begins with `rackUnit`.

Naming a Rack Unit

This command syntax assigns or changes the name of the specified rack unit on the specified asset sensor.

```
config:#   rackUnit <n> <rack_unit> name "<name>"
```

Variables:

- <n> is the number of the FEATURE port where the selected asset sensor is physically connected. For the PX device with only one FEATURE port, the number is always 1.
- <rack_unit> is the index number of the desired rack unit. The index number of each rack unit is available on the Asset Strip page of the web interface.
- <name> is a string comprising up to 32 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.

Setting the LED Operation Mode

This command syntax determines whether a specific rack unit on the specified asset sensor follows the global LED color settings.

```
config:#   rackUnit <n> <rack_unit> LEDOperationMode <mode>
```

Variables:

- <n> is the number of the FEATURE port where the selected asset sensor is physically connected. For the PX device with only one FEATURE port, the number is always 1.
- <rack_unit> is the index number of the desired rack unit. The index number of each rack unit is available on the Asset Strip page of the web interface.
- <mode> is one of the LED modes: *automatic* or *manual*.

Mode	Description
automatic	This option makes the LED of the specified rack unit follow the global LED color settings. See ***Setting LED Colors for Connected Tags*** (on page 505) and ***Setting LED Colors for Disconnected Tags*** (on page 506). This is the default.
manual	This option enables selection of a different LED color and LED mode for the specified rack unit. When this option is selected, see ***Setting an LED Color for a Rack Unit*** (on page 508) and ***Setting an LED Mode for a Rack Unit*** (on page 508) to set different LED settings.

Setting an LED Color for a Rack Unit

This command syntax sets the LED color for a specific rack unit on the specified asset sensor. You need to set a rack unit's LED color only when the LED operation mode of this rack unit has been set to "manual."

```
config:#   rackUnit <n> <rack_unit> LEDColor <color>
```

Variables:

- <n> is the number of the FEATURE port where the selected asset sensor is physically connected. For the PX device with only one FEATURE port, the number is always 1.
- <rack_unit> is the index number of the desired rack unit. The index number of each rack unit is available on the Asset Strip page of the web interface.
- <color> is the hexadecimal RGB value of a color in HTML format. The <color> variable ranges from #000000 to #FFFFFF.

Note: A rack unit's LED color setting overrides the global LED color setting on it. See **Setting LED Colors for Connected Tags** *(on page 505) and* **Setting LED Colors for Disconnected Tags** *(on page 506).*

Setting an LED Mode for a Rack Unit

This command syntax sets the LED mode for a specific rack unit on the specified asset sensor. You need to set a rack unit's LED mode only when the LED operation mode of this rack unit has been set to "manual."

```
config:#   rackUnit <n> <rack_unit> LEDMode <mode>
```

Variables:

- <n> is the number of the FEATURE port where the selected asset sensor is physically connected. For the PX device with only one FEATURE port, the number is always 1.
- <rack_unit> is the index number of the desired rack unit. The index number of each rack unit is available on the Asset Strip page of the web interface.
- <mode> is one of the LED modes: *on*, *off*, *blinkSlow* or *blinkFast*.

Mode	Description
on	This mode has the LED stay lit permanently.
off	This mode has the LED stay off permanently.
blinkSlow	This mode has the LED blink slowly.

Mode	Description
blinkFast	This mode has the LED blink quickly.

Examples

This section illustrates several asset management examples.

Example 1 - Asset Sensor LED Colors for Disconnected Tags

This command syntax sets the LED color for all rack units on the asset sensor #1 to BLACK (that is, 000000) to indicate the absence of a connected asset tag.

```
config:#   assetStrip 1 LEDColorForDisconnectedTags #000000
```

Note: Black color causes the LEDs to stay off.

Example 2 - Rack Unit Naming

The following command assigns the name "Linux server" to the rack unit whose index number is 25 on the asset sensor#1.

```
config:#   rackUnit 1 25 name "Linux server"
```

Serial Port Configuration Commands

A serial port configuration command begins with *serial*.

Setting the Baud Rates

The following commands set the baud rate (bps) of the serial port labeled CONSOLE / MODEM on the PX device. Change the baud rate before connecting it to the desired device, such as a computer, a Raritan's P2CIM-SER, or a modem, through the serial port, or there are communications errors. If you change the baud rate dynamically after the connection has been made, you must reset the PX or power cycle the connected device for proper communications.

Determine the CONSOLE baud rate:

```
config:#   serial consoleBaudRate <baud_rate>
```

Note: The serial port bit-rate change is needed when the PX works in conjunction with Raritan's Dominion LX KVM switch. The Dominion LX only supports 19200 bps for communications over the serial interface.

Determine the MODEM baud rate:

```
config:#   serial modemBaudRate <baud_rate>
```

Variables:

- <baud_rate> is one of the baud rate options: *1200*, *2400*, *4800*, *9600*, *19200*, *38400*, *57600*, *115200*.

Forcing the Device Detection Mode

This command forces the serial port on the PX to enter a specific device detection mode.

```
config:#   serial deviceDetectionType <mode>
```

Variables:

- <mode> is one of the detection modes: *automatic*, *forceConsole*, *forceAnalogModem,* or *forceGsmModem*.

Option	Description
automatic	The PX automatically detects the device type on the serial port. Select this option unless your PX cannot correctly detect the connected device.
forceConsole	The port enters the local console state.
forceAnalogModem	The port enters the analog modem state.

Option	Description
forceGsmModem	The port enters the GSM modem state.

Example

The following command sets the CONSOLE baud rate of the PX device's serial port to 9600 bps.

```
config:#   serial consoleBaudRate 9600
```

Setting the History Buffer Length

This command syntax sets the history buffer length, which determines the amount of history commands that can be retained in the buffer. The default length is 25.

```
config:#   history length <n>
```

Variables:

- <n> is an integer number between 1 and 250.

Multi-Command Syntax

To shorten the configuration time, you can combine various configuration commands in one command to perform all of them at a time. All combined commands must belong to the same configuration type, such as commands prefixed with *network*, *user modify*, *sensor externalsensor* and so on.

A multi-command syntax looks like this:

```
<configuration type> <setting 1> <value 1> <setting 2>
<value 2> <setting 3> <value 3> ...
```

Example 1 - Combination of IP, Subnet Mask and Gateway Parameters

The following multi-command syntax configures IPv4 address, subnet mask and gateway for the network connectivity simultaneously.

```
config:#    network ipv4 ipAddress 192.168.84.225 subnetMask 255.255.255.0
            gateway 192.168.84.0
```

Results:

- The IP address is set to 192.168.84.225.
- The subnet mask is set to 255.255.255.0.
- The gateway is set to 192.168.84.0.

Example 2 - Combination of Upper Critical and Upper Warning Settings

The following multi-command syntax simultaneously configures Upper Critical and Upper Warning thresholds for the RMS current of the 2nd overcurrent protector.

```
config:#    sensor ocp 2 current upperCritical disable upperWarning 15
```

Results:

- The Upper Critical threshold of the 2nd overcurrent protector's RMS current is disabled.
- The Upper Warning threshold of the 2nd overcurrent protector's RMS current is set to 15A and enabled at the same time.

Example 3 - Combination of SSID and PSK Parameters

This multi-command syntax configures both SSID and PSK parameters simultaneously for the wireless feature.

```
config:#    network wireless SSID myssid PSK encryp_key
```

Results:

- The SSID value is set to myssid.
- The PSK value is set to encryp_key.

Example 4 - Combination of Upper Critical, Upper Warning and Lower Warning Settings

The following multi-command syntax configures Upper Critical, Upper Warning and Lower Warning thresholds for the outlet 5 RMS current simultaneously.

```
config:#    sensor outlet 5 current upperCritical disable upperWarning enable
            lowerWarning 1.0
```

Results:

- The Upper Critical threshold of outlet 5 RMS current is disabled.
- The Upper Warning threshold of outlet 5 RMS current is enabled.
- The Lower Warning threshold of outlet 5 RMS current is set to 1.0A and enabled at the same time.

Load Shedding Configuration Commands

This section applies to outlet-switching capable models only.

A load shedding configuration command begins with *loadshedding*.

Unlike other CLI configuration commands, the load shedding configuration command is performed in the *administrator mode* rather than the configuration mode. See ***Different CLI Modes and Prompts*** (on page 363).

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, PX 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 PX enter the load shedding mode.

```
config:#    loadshedding start
```

Power Control Operations

This section applies to outlet-switching capable models only.

Outlets on the PX device can be turned on or off or power cycled through the CLI.

Besides, you can cancel the power-on process while the PX is powering on ALL outlets.

You must perform this operation in the *administrator mode*. See ***Different CLI Modes and Prompts*** (on page 363).

Turning On the Outlet(s)

This section applies to outlet-switching capable models only.

This command turns on one or multiple outlets.

```
#       power outlets <numbers> on
```

To quicken the operation, you can add the parameter "/y" to the end of the command, which confirms the operation.

```
#       power outlets <numbers> on /y
```

Variables:

- <numbers> is one of the options: *all*, an outlet number, a list or a range of outlets.

Option	Description
all	Switches ON all outlets.
A specific outlet number	Switches ON the specified outlet.
A comma-separated list of outlets	Switches ON multiple, inconsecutive or consecutive outlets. For example, to specify 7 outlets -- 2, 4, 9, 11, 12, 13 and 15, type `outlets 2,4,9,11-13,15`.
A range of outlets with an en dash in between	Switches ON multiple, consecutive outlets. For example, to specify 6 consecutive outlets -- 3, 4, 5, 6, 7, 8, type `outlets 3-8`.

If you entered the command without "/y", a message appears, prompting you to confirm the operation. Then:

- Type y to confirm the operation, OR
- Type n to abort the operation

Turning Off the Outlet(s)

This section applies to outlet-switching capable models only.

This command turns off one or multiple outlets.

```
#       power outlets <numbers> off
```

To quicken the operation, you can add the parameter "/y" to the end of the command, which confirms the operation.

```
#       power outlets <numbers> off /y
```

Variables:

- <numbers> is one of the options: *all*, an outlet number, a list or a range of outlets.

Option	Description
all	Switches OFF all outlets.
A specific outlet number	Switches OFF the specified outlet.
A comma-separated list of outlets	Switches OFF multiple, inconsecutive or consecutive outlets. For example, to specify 7 outlets -- 2, 4, 9, 11, 12, 13 and 15, type `outlets 2,4,9,11-13,15`.
A range of outlets with an en dash in between	Switches OFF multiple, consecutive outlets. For example, to specify 6 consecutive outlets -- 3, 4, 5, 6, 7, 8, type `outlets 3-8`.

If you entered the command without "/y", a message appears, prompting you to confirm the operation. Then:

- Type y to confirm the operation, OR
- Type n to abort the operation

Power Cycling the Outlet(s)

This section applies to outlet-switching capable models only.

This command power cycles one or multiple outlets.

```
#       power outlets <numbers> cycle
```

To quicken the operation, you can add the parameter "/y" to the end of the command, which confirms the operation.

```
#       power outlets <numbers> cycle /y
```

Variables:

- <numbers> is one of the options: *all*, an outlet number, a list or a range of outlets.

Option	Description
all	Power cycles all outlets.
A specific outlet number	Power cycles the specified outlet.
A comma-separated list of outlets	Power cycles multiple, inconsecutive or consecutive outlets. For example, to specify 7 outlets -- 2, 4, 9, 11, 12, 13 and 15, type `outlets 2,4,9,11-13,15`.
A range of outlets with an en dash in between	Power cycles multiple, consecutive outlets. For example, to specify 6 consecutive outlets -- 3, 4, 5, 6, 7, 8, type `outlets 3-8`.

If you entered the command without "/y", a message appears, prompting you to confirm the operation. Then:

- Type y to confirm the operation, OR

- Type n to abort the operation

Canceling the Power-On Process

This section applies to outlet-switching capable models only.

After issuing the command to power on ALL outlets, you can use the following command to stop the power-on process.

```
#       power cancelSequence
```

To quicken the operation, you can add the parameter "/y" to the end of the command, which confirms the operation.

```
#       power cancelSequence /y
```

Example - Power Cycling Specific Outlets

The following command power cycles these outlets: 2, 6, 7, 8, 10, 13, 14, 15 and 16.

```
#     power outlets 2,6-8,10,13-16 cycle
```

Actuator Control Operations

An actuator, which is connected to a dry contact signal channel of a DX sensor, can control a mechanism or system. You can switch on or off that mechanism or system through the actuator control command in the CLI.

Perform these commands in the administrator or user mode. See ***Different CLI Modes and Prompts*** (on page 363).

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 PX web interface or using the show command in the CLI. It is an integer between 1 and 32.

If you entered the command without "/y", a message appears, prompting you to confirm the operation. Then:

- Type y to confirm the operation, OR
- Type n to abort the operation

Switching Off an Actuator

This command syntax turns off one actuator.

```
#       control actuator <n> off
```

To quicken the operation, you can add the parameter "/y" to the end of the command, which confirms the operation.

```
#       control actuator <n> off /y
```

Variables:

- <n> is an actuator's ID number.

  The ID number is available in the PX web interface or using the show command in the CLI. It is an integer between 1 and 32.

If you entered the command without "/y", a message appears, prompting you to confirm the operation. Then:

- Type y to confirm the operation, OR
- Type n to abort the operation

Example - Turning On a Specific Actuator

The following command turns on the actuator whose ID number is 8.

```
#     control actuator 8 on
```

Unblocking a User

If any user is blocked from accessing the PX, you can unblock them at the local console.

To unblock a user:

1. Log in to the CLI interface using any terminal program via a local connection. See ***With HyperTerminal*** (on page 360).
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 PX

You can reset the PX device to factory defaults or simply restart it using the CLI commands.

Restarting the PDU

This command restarts the PX device. It is not a factory default reset.

To restart the PX device:

1. Ensure you have entered administrator mode and the # prompt is displayed.
2. Type either of the following commands to restart the PX device.

```
#     reset unit
```

-- OR --

```
#     reset unit /y
```

3. If you entered the command without "/y" in Step 2, a message appears prompting you to confirm the operation. Type y to confirm the reset.
4. Wait until the Username prompt appears, indicating the reset is complete.

Note: If you are performing this command over a USB connection, re-connect the USB cable after the reset is completed, or the CLI communications are lost.

Resetting Active Energy Readings

You can reset either one active energy sensor or all active energy sensors at a time to restart the energy accumulation process.

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

To reset all active energy readings of the PX:

```
#     reset activeEnergy pdu
```

-- OR --

```
#     reset activeEnergy pdu /y
```

To reset one inlet's active energy readings:

```
#     reset activeEnergy inlet <n>
```

-- OR --

```
#     reset activeEnergy inlet <n> /y
```

To reset one outlet's active energy readings:

```
#     reset activeEnergy outlet <outlet_n>
```

-- OR --

```
#     reset activeEnergy outlet <outlet_n> /y
```

If you entered the command without "/y", a message appears prompting you to confirm the operation. Type y to confirm the reset or n to abort it.

Variables:

- <n> is the inlet number.
- <outlet_n> is an outlet number.

Resetting to Factory Defaults

The following commands restore all settings of the PX device to factory defaults.

To reset PX settings after login, use either command:

```
#     reset factorydefaults
```

-- OR --

```
#     reset factorydefaults /y
```

To reset PX settings before login:

```
Username:   factorydefaults
```

See ***Using the CLI Command*** (on page 581) for details.

Network Troubleshooting

The PX provides 4 diagnostic commands for troubleshooting network problems: *nslookup*, *netstat*, *ping*, and *traceroute*. The diagnostic commands function as corresponding Linux commands and can get corresponding Linux outputs.

Entering Diagnostic Mode

Diagnostic commands function in the diagnostic mode only.

To enter the diagnostic mode:

1. Enter either of the following modes:
   - Administrator mode: The # prompt is displayed.
   - User mode: The > prompt is displayed.
2. Type `diag` and press Enter. The diag# or diag> prompt appears, indicating that you have entered the diagnostic mode.
3. Now you can type any diagnostic commands for troubleshooting.

Quitting Diagnostic Mode

▶ **To quit the diagnostic mode, use this command:**

```
diag>       exit
```

The # or > prompt appears after pressing Enter, indicating that you have entered the administrator or user mode. See ***Different CLI Modes and Prompts*** (on page 363).

Diagnostic Commands

The diagnostic command syntax varies from command to command.

Querying DNS Servers

This command syntax queries Internet domain name server (DNS) information of a network host.

```
diag>       nslookup <host>
```

Variables:

- <host> is the name or IP address of the host whose DNS information you want to query.

Showing Network Connections

This command syntax displays network connections and/or status of ports.

```
diag>       netstat <option>
```

Variables:

- <option> is one of the options: *ports* or *connections*.

Option	Description
ports	Shows TCP/UDP ports.
connections	Shows network connections.

Testing the Network Connectivity

This ping command sends the ICMP ECHO_REQUEST message to a network host for checking its network connectivity. If the output shows the host is responding properly, the network connectivity is good. If not, either the host is shut down or it is not being properly connected to the network.

```
diag>       ping <host>
```

Variables:

- <host> is the host name or IP address whose networking connectivity you want to check.

Options:

- You can include any or all of additional options listed below in the ping command.

Options	Description
count <number1>	Determines the number of messages to be sent. <number1> is an integer number between 1 and 100.
size <number2>	Determines the packet size. <number2> is an integer number in bytes between 1 and 65468.
timeout <number3>	Determines the waiting period before timeout. <number3> is an integer number in seconds ranging from 1 to 600.

The command looks like the following when it includes all options:

```
diag>       ping <host> count <number1> size <number2> timeout <number3>
```

Tracing the Route

This command syntax traces the network route between your PX device and a network host.

```
diag>       traceroute <host>
```

Variables:

- <host> is the name or IP address of the host you want to trace.

Example - Ping Command

The following command checks the network connectivity of the host 192.168.84.222 by sending the ICMP ECHO_REQUEST message to the host for 5 times.

```
diag>       ping 192.168.84.222 count 5
```

Retrieving Previous Commands

If you would like to retrieve any command that was previously typed in the same connection session, press the Up arrow (↑) on the keyboard until the desired command is displayed.

Automatically Completing a Command

A CLI command always consists of several words. You can easily enter a command by typing first word(s) or letter(s) and then pressing Tab or Ctrl+i instead of typing the whole command word by word.

To have a command completed automatically:

1. Type initial letters or words of the desired command. Make sure the letters or words you typed are unique so that the CLI can identify the command you want.
2. Press Tab or Ctrl+i until the complete command appears.

Example 1:

Type the first word and the first letter of the second word of the "`reset factorydefaults`" command, that is, `reset f`. Then press Tab or Ctrl+i to complete the second word.

Example 2:

Type the first word and initial letters of the second word of the "`security enforceHttpsForWebAccess`" command, that is, `security enf`. Then press Tab or Ctrl+i to complete the second word.

Logging out of CLI

After completing your tasks using the CLI, always log out of the CLI to prevent others from accessing the CLI.

To log out of the CLI:

1. Ensure you have entered administrator mode and the # prompt is displayed.
2. Type `exit` and press Enter.

Chapter 9 In-Line Monitors

The model name of a PX in-line monitor follows this format: PX3-3nnn, where n is a number, such as PX3-3411.

Unlike most of PX devices, each inlet of an in-line monitor is connected to an outlet only, so an inlet's rating is the same as an outlet's rating.

In This Chapter

Overview....527
Safety Instructions....527
Flexible Cord Installation Instructions....528
In-Line Monitor's Web Interface....536

Overview

An in-line monitor is implemented with the same number of inlets and outlets. An inlet is connected to a power source for receiving electricity, such as electric distribution panels or branch circuit receptacles. An outlet is connected to a device that draws power, such as a cooling or IT device.

Inlets are located at the side labeled **Line**, and outlets are located at the side labeled **Load**.

Safety Instructions

1. Installation of this product should only be performed by a licensed electrician.
2. Make sure the line cord is disconnected from power before physically mounting or moving the location of this product.
3. This product is intended to be located in an equipment rack in an information technology room. In the United States, installation must comply and be done in accordance with NEC (2011) Article 645 *Information Technology Equipment*.
4. 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.
5. 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.

6. 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.

Flexible Cord Installation Instructions

The following instructions are for Raritan products manufactured to accept user-installed flexible cords. These products are visually identified by the cable gland used to hold the flexible cord.

Important: Complete and the most updated instructions on installing a flexible cord on Raritan PDUs are included in the *Raritan PX Power Cord Installation Guide*, which is available on the Raritan website's *Support page* (*http://www.raritan.com/support/*).

Flexible Cord Selection

- The preferred flexible cable is type SOOW, 600V, 90°C or 105°C. Consult Raritan before using a different flexible cable type.
- The rated ampacity of the flexible cord must be greater than or equal to the Raritan product's rated ampacity marked on its nameplate. In the United States, relevant ampacity ratings for flexible cords can be found in NEC(2011) section 400.5.
- The number of wires in the flexible cord must match the number of terminals (including the ground terminal) inside the Raritan product. See ***Wiring of 3-Phase In-Line Monitors*** (on page 530) for exceptions.
- If a plug is to be attached to the flexible cord, the length of the flexible cord must not exceed 4.5 meters - as specified in UL 60950-1 (2007) and NEC 645.5 (2011).
- The flexible cord may be permanently connected to power subject to local regulatory agency approval. In the United States, relevant electrical regulations can be found in NEC (2011) sections 400.7(A)(8), 400.7(B), 368.56 and table 400.4.

Plug Selection

If a plug is to be attached to the flexible cord, the plug's rated ampacity is chosen as follows:

- In the United States, as specified in UL 60950-1, the plug's rated ampacity must be 125% greater than the Raritan product's rated ampacity. In some Raritan products, such as 35A 3-phase delta wired PDUs, an exactly 125% rated plug is not available. In these cases, choose the closest plug that is more than 125%. For example, a 50A plug is the closest fit for a 35A 3-phase PDU.
- For all other locations, subject to local regulatory agency policy, the plug's rated ampacity is the same as the Raritan products rated ampacity.

Receptacle Selection

For Raritan in-line monitors, any receptacle fitted to the outlet flexible cord must have identical ratings as the plug attached to the inlet flexible cord.

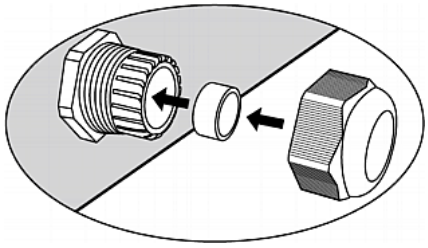
Derating a Raritan Product

Lower rated plugs, receptacles and flexible cords may be connected to a Raritan product. This results in a derated (reduced) ampacity rating for the product.

Derating guidelines:

1. Choose the plug and use its rated ampacity to determine the derated ampacity.
   - In the United States, as specified in UL 60950-1, the derated ampacity is 80% of the plug's rated ampacity. For example, a 30A plug would result in a derated ampacity of 24A.
   - In other geographic locations, subject to local regulatory agency approval, the derated ampacity is the plug's rated ampacity. For example, using a 16A plug would result in a derated ampacity of 16A.
2. The derated ampacity must be marked on the Raritan product so the new reduced rating can be easily identified.
3. For in-line monitors, the receptacles used must have the same voltage and ampacity rating as the plug chosen in step 1.

4. The flexible cord must have a rated ampacity greater than or equal to the derated ampacity. Since the new flexible cord may be smaller diameter, a check must be performed to insure the cable gland nut, when tightened, will securely hold the flexible cord so that it cannot be twisted, pulled or pushed in the cable gland. A sealing ring, for small diameter flexible cords, may have been included with the Raritan product, or one can be requested from Raritan, to reduce the inside diameter of the cable gland.



Wiring of 3-Phase In-Line Monitors

3-phase in-line monitors contain 4-pole wiring terminal blocks (L1, L2, L3, N) to monitor 5-wire (4P+PE) 3-phase wye connections. Delta wired 4-wire (3P+PE) 3-phase connections are also permitted (no wire connected to the terminal block neutral “N”). No additional hardware or firmware configuration is required to specify whether the connection is 5-wire wye or 4-wire delta.

In-Line Monitor Unused Channels

It is not necessary to wire up all channels of multi-channel in-line monitors. The inlet and outlet openings of unused channels must be completely closed off. “Goof plugs” for this purpose may be a good choice if they are available in your country or region.

Step by Step Flexible Cord Installation

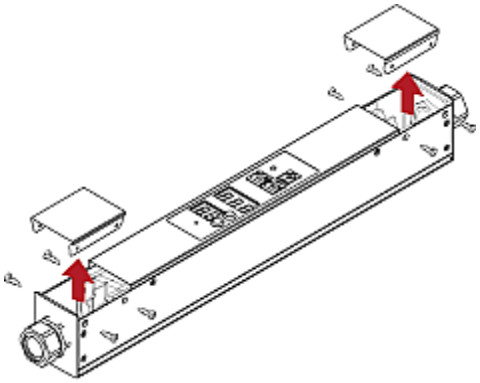
The following items are required to complete the installation:

- Flexible cord(s).
- Insulated ring terminals (one for each wire) and appropriate crimp tool.
- Plug(s) and receptacle(s) (for in-line monitors)
- Torque screwdriver, torque nut driver and torque wrench to tighten the wiring terminal block screws, ground nut and cable gland nut.

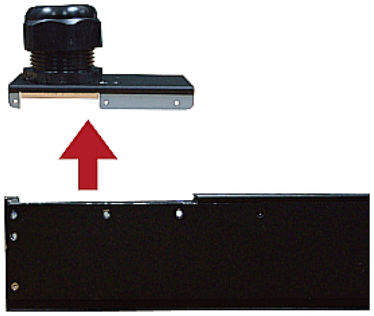
▶ To install a flexible cord:

1. Open the PDU's access panel (or in-line monitor top panel) to expose the power wiring terminal block(s).

One-channel in-line monitor

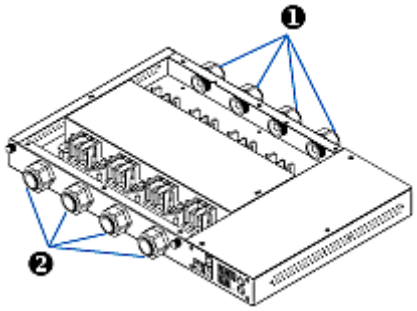


Zero U PDU



Make sure to locate the ground wire mounting stud(s). There is a separate ground wire mounting stud for each terminal block. Each flexible cord MUST have its green (or green/yellow) ground wire bonded to a ground wire mounting stud.

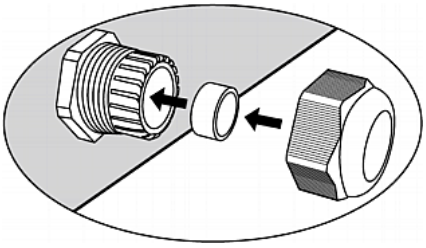
For in-line monitors, make sure to identify the inlet terminal blocks (rear of monitor) and outlet terminal blocks (front of monitor). Each inlet terminal block has a corresponding outlet terminal block.



Number	Description
1	Inlets (labeled LINE)
2	Outlets (labeled LOAD)

2. Strip off the outer jacket of the flexible cord and remove any jute, paper or other fillers. Use the following to help determine how much jacket to remove:
   - In the finished assembly, the outer jacket should protrude inside the Raritan product.
   - The wires will have ring terminals crimped onto them.
   - In the finished assembly, the wires should have some slack and not be taught.
   - In the finished assembly, if the flexible cord slips in the cable gland placing a strain on the cord's wires, the ground wire must be the last wire to take the strain.
3. Crimp an insulated ring terminal onto each wire. A non-insulated ring terminal may be used for the ground wire. Inspect each crimp to insure it is secure and verify no exposed wire protrudes from the rear of an insulated ring terminal.
4. Loosen the cable gland nut and push the flexible cord assembly through the gland.

Temporarily hand tighten the gland nut and verify the cord cannot be twisted or pushed or pulled in the gland. Do not proceed if hand tightening results in a loose cord. In some models, especially in-line monitors, the flexible cord's diameter may be too small for the cable gland. A sealing ring for smaller diameter line cords may have been included with the Raritan product, or can be requested from Raritan, to reduce the inside diameter of the cable gland.



5. Fasten the ring terminal of the green (or green/yellow) ground wire to the chassis's threaded ground stud in this order:
   a. Place the lock washer on the stud.
   b. Place the ground wire ring terminal on the stud.
   c. Place the nut on the stud and tighten with a torque wrench. The appropriate torque settings vary according to the nut size.

Nut size	Torque setting (N·m)	Tolerance
M3	0.49	10%
M4	1.27	8%
M5	1.96	5%
M6	2.94	3.5%
M8	4.9	2%

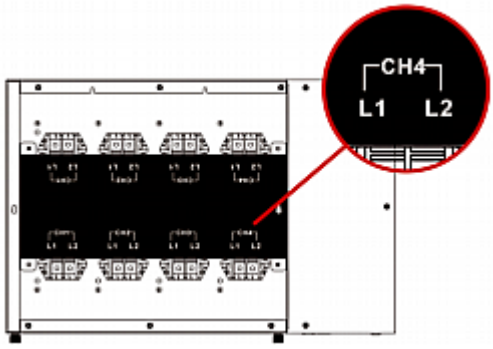
   d. Check the ground wire connection. It should be secure and not move or rotate.

6. Fasten the ring terminals of all remaining wires to the terminal block and tighten each using a torque screwdriver. The appropriate torque settings vary according to the screw size.

Screw size	Torque setting (N·m)	Tolerance
M3	0.49	10%
M4	1.27	8%
M5	1.96	5%
M6	2.94	3.5%
M8	4.9	2%

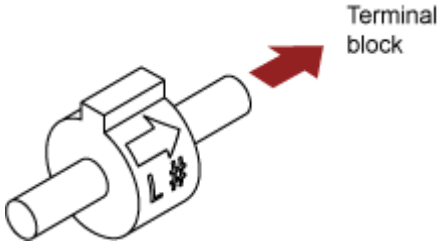
Make sure each ring terminal is firmly fastened and cannot be twisted by hand. Use the following guidelines to help terminal block wiring.

- In single-phase Raritan products with world-wide ratings, the terminals are labeled L1 and L2. L1 is the phase wire. L2 is either the neutral (120/230V installations) or another phase wire (208V installations).



- In all 3-phase products, L1 is phase A, L2 is phase B, L3 is phase C and N is neutral.

- If your PDU is inlet metered, such as PDU models PX2-1nnn and PX2-2nnn (where n is a number), you must pass each line cord wire through the correct CT in the correct direction. Each CT is labeled and contains a direction arrow. Push the ring terminal end of the line cord through the CT in the direction indicated by the arrow. For example, push the L1 line cord wire through the CT labeled L1 and then connect it to the L1 terminal block.



- For Raritan in-line monitors, where there is a one to one correspondence between plug and receptacle, maintain the same wire colors for inlet and outlet flexible cords.

7. Make final adjustments to the cable gland and verify the jacket of the flexible cord extends into the Raritan product. Hand tighten the gland nut and finish tightening with a torque wrench. Appropriate torque settings vary according to the cable gland size.

Cable gland size	Torque setting (N·m)
M12x1.5	0.7 to 0.9
M16x1.5	2.0 to 3.0
M20x1.5	2.7 to 4.0
M25x1.5	5.0 to 7.5
M32x1.5	7.5 to 10.0
M40x1.5	7.5 to 10.0
M50x1.5	7.5 to 10.0
M63x1.5	7.5 to 10.0

Note: The cable gland size is marked on the cable gland body.

After tightening, examine the flexible cord and cable gland for the following:

- Make sure you can see a few remaining threads between the cable gland body and cable gland nut. The gland nut must not bottom out on the gland body.
- Make sure the flexible cord does not move in the cable gland when it is twisted, pushed or pulled.

8. Re-install the PDU wiring access panel or in-line monitor cover plate. This completes internal wiring of the Raritan product.

9. For in-line monitors, fasten the receptacles to the outlet flexible cords following the manufacturer's instructions.
10. Complete the wiring of the inlet flexible cord by performing one of these steps:
    - Assemble the plug following the manufacturer's instructions.
    - Permanently attach and strain relief the flexible cord to a junction box following applicable electrical codes.

In-Line Monitor's Web Interface

An in-line monitor's web interface is similar to a regular PX model's web interface.

See ***Using the Web Interface*** (on page 107) for login instructions and additional information.

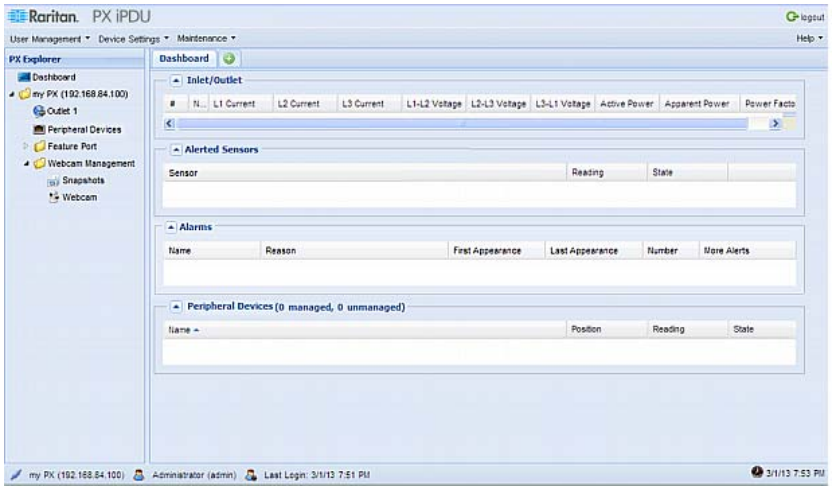
Dashboard Page

After login, the web interface displays the Dashboard page by default. An inline monitor's Dashboard page looks slightly different from a regular PX device's Dashboard page.

The power status of the outlet on a three-phase Y-wired inline monitor is displayed on this page, including:

- Current of L1, L2 and L3
- Voltage of L1-L2, L2-L3, and L3-L1
- Active power
- Apparent power
- Power factor

Note: Depending on your model, elements shown on the same page may appear slightly different from this image.



Outlet Page

An inline monitor's Outlet page displays more information than a regular PX device's Outlet page, including:

- Current per outlet

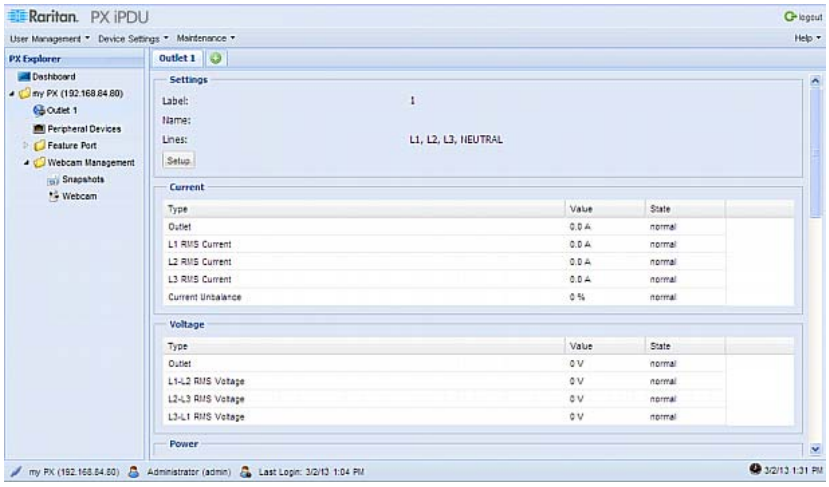
  Current per line (for a three-phase model)
- Voltage per outlet

  Voltage per line (for a three-phase model)
- Power-related readings per outlet

  Power-related readings per line (for a three-phase model)
- Threshold settings per outlet

  Threshold settings per line (for a three-phase model)

Note: Depending on your model, elements shown on the same page may appear slightly different from this image.



Appendix A Specifications

In This Chapter

Maximum Ambient Operating Temperature 539
Serial RS-232 Port Pinouts.....539
Sensor RJ-45 Port Pinouts 539
Feature RJ-45 Port Pinouts 540

Maximum Ambient Operating Temperature

The maximum ambient operating temperature (TMA) for PX varies from 50 to 60 degrees Celsius, depending on the model and certification standard (CE or UL). If necessary, contact Raritan Technical Support for this information for your model.

Specification	Measure
Max Ambient Temperature	50 to 60 degrees Celsius

Serial RS-232 Port Pinouts

RS-232 Pin/signal definition			
Pin No.	Signal	Direction	Description
1	DCD	Input	Data
2	RxD	Input	Receive data (data in)
3	TxD	Output	Transmit data
4	DTR	Output	Data terminal ready
5	GND	—	Signal ground
6	DSR	Input	Data set ready
7	RTS	Output	Request to send
8	CTS	Input	Clear to send
9	RI	Input	Ring indicator

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)
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	—	Used for Feature Port
8	GND	—	Signal Ground

Note: A maximum of 500mA power is permitted for both pin 1 and pin 2 altogether.

Feature RJ-45 Port Pinouts

RJ-45 Pin/signal definition			
Pin No.	Signal	Direction	Description
1	DTR	Output	Reserved
2	GND	—	Signal Ground
3	+5V	—	Power for CIM (200mA, fuse protected) Warning: Pin 3 is only intended for use with Raritan devices.
4	TxD	Output	Transmit Data (Data out)
5	RxD	Input	Receive Data (Data in)
6	+12V	—	Warning: Pin 6 is only intended for use with Raritan devices. Do NOT connect.

RJ-45 Pin/signal definition			
Pin No.	Signal	Direction	Description
7	GND	—	Signal Ground
8	DCD	Input	Reserved

Appendix B Equipment Setup Worksheet

PX Series Model _____

PX Series Serial Number _____

OUTLET 1	OUTLET 2	OUTLET 3
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE
OUTLET 4	**OUTLET 5**	**OUTLET 6**
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE

OUTLET 7	OUTLET 8	OUTLET 9
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE
OUTLET 10	OUTLET 11	OUTLET 12
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE
OUTLET 13	OUTLET 14	OUTLET 15
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE

OUTLET 16	OUTLET 17	OUTLET 18
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE
OUTLET 19	OUTLET 20	OUTLET 21
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE

OUTLET 22	OUTLET 23	OUTLET 24
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE

Types of adapters

_____

Types of cables

_____

Name of software program

_____

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 PX.

- Configuration changes
- Firmware upgrade
- Downloading diagnostic data

Tip: You can also accomplish the same tasks via the TFTP server in a DHCP network. See **Bulk Configuration or Firmware Upgrade via DHCP/TFTP** *(on page 557).*

To use a USB drive to configure the PX or upgrade firmware:

1. Verify that both the USB drive and your PX meet the requirements. See ***System and USB Requirements*** (on page 547).
2. Prepare required configuration files. See ***Configuration Files*** (on page 547).
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 PX.
5. The initial message shown on the front panel display depends on the first task performed by the PX.
   - If no firmware upgrade task will be performed, a happy smiley as shown below is displayed after around 30 seconds.

     =-]
   - If the USB drive contains the firmware upgrade data, the PX first performs the firmware upgrade, showing the upgrade message on the front panel display, and then shows the happy smiley when the firmware upgrade completes successfully. See ***Firmware Upgrade via USB*** (on page 556).
6. After the happy smiley appears, press and hold one of the control buttons next to the front panel display for one second until the display turns blank.
7. Wait for several seconds until the PX resumes normal operation, indicated by the normal message of the front panel display.

Tip: You can remove the USB drive and plug it into another PX for performing the same task(s) once the happy smiley or the firmware upgrade message displays.

If nothing is shown on the display and no task is performed after plugging the USB drive, check the log file in the USB drive.

In This Chapter

System and USB Requirements.....547
Configuration Files.....547
Firmware Upgrade via USB.....556

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.

PX system requirements:

- There is at least one USB-A port available on your Raritan device.
- Your PX must be version 2.2.13 or later.

  Note that the PX interpreted the USB drive contents using the firmware which was running when plugging the USB drive into the PX, not the new firmware after firmware upgrade.

USB drive requirements:

- The drive must contain a single partition formatted as a Windows FAT32 filesystem.
- The drive must contain a configuration file called *fwupdate.cfg* in its root directory. See ***fwupdate.cfg*** (on page 549).

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 549).

- **config.txt:**

  This file is used for configuring device settings. See ***config.txt*** (on page 552).

- **devices.csv:**

  This file is required only when there are device-specific settings to configure for multiple PX devices. See ***devices.csv*** (on page 554).

Raritan provides a Mass Deployment Utility, which helps you to quickly generate all configuration files for your PX. See ***Creating Configuration Files via Mass Deployment Utility*** (on page 555).

fwupdate.cfg

The configuration file, *fwupdate.cfg*, is an ASCII text file containing key-value pairs, one per line.

Each value in the file must be separated by a single = character, without any surrounding spaces. Keys are not case sensitive.

This section only explains common options of the file.

Note: To use any options developed after version 2.2.13, the firmware version running on your PX must be able to support them.

user

- A required option.
- Specify the name of a user account with Administrator Privileges.
- For a PX with factory default configuration, set this option to `admin`.

password

- A required option.
- Specify the password of the specified admin user.
- For a PX with factory default configuration, set this option to `raritan.`

logfile

- Specify the name of a text file where the PX will append the log messages when interpreting the USB drive contents.
- If the specified file does not exist in the USB drive, it will be automatically created.
- If this option is not set, no log message are recorded. The disadvantage is that no feedback is available if the PX detects a problem with the USB drive contents.

firmware

- Specify the name of a firmware binary file used to upgrade your PX.
- The specified firmware file must be compatible with your PX and have an official Raritan signature.
- If the specified firmware file is the same as the current firmware version of your PX, no firmware upgrade is performed unless you have set the option "force_update" to `true`.

force_update

- If this option is set to `true`, the firmware upgrade is always performed even though your PX is running the same firmware version as the specified firmware file.

- This option CANNOT break other constraints like the minimum downgrade version.

config

- Supported as of release 2.4.0.
- Specify the name of the configuration file containing device settings.
- The suggested filename is *config.txt*. See ***config.txt*** (on page 552).

device_list

- Specify the name of the configuration file listing all PX 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 554).

match

- Specify a match condition for identifying a line or a PX 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 PX to search for the MAC address in the 7th column of the "devices.csv" file.
- The default value is `serial:1`, making the PX search for its serial number in the first column.
- This option is used only if the "device_list" option has been set.

collect_diag

- If this option is set to `true`, the diagnostic data of the PX is downloaded to the USB drive.
- The filename of the diagnostic data written into the USB drive varies, depending on the PX firmware version:
  - Filename prior to version 3.0.0: *diag_<unit-serial>.zip*, where <unit-serial> is the serial number of the PX.
  - Filename as of version 3.0.0: *diag_<unit-serial>.tgz*

- The PX utters a short beep when writing the diagnostic data to the USB drive.

factory_reset

- Supported as of release 3.0.0.
- If this option is set to `true`, the PX will be reset to factory defaults.
- If the device configuration will be updated at the same time, the factory reset will be executed before updating the device configuration.

bulk_config_restore

- Supported as of release 3.1.0.
- Specify the name of the bulk configuration file used to configure or restore the PX.

Note: See **Saving the PX Configuration** *(on page 320) for instructions on generating a bulk configuration file.*

- Additional configuration keys set via the *config.txt* file will be applied after performing the bulk restore operation.
- This option CANNOT be used with the option "full_config_restore."
- If a firmware upgrade will be performed at the same time, you must generate the bulk configuration file based on the NEW firmware version instead of the current firmware version.

full_config_restore

- Supported as of release 3.1.0.
- Specify the name of the full configuration backup file used to restore the PX.

Note: See **Backup and Restore of PX Device Settings** *(on page 322) for instructions on generating the full configuration backup file.*

- Additional configuration keys set via the *config.txt* file will be applied after performing the configuration restore operation.
- This option CANNOT be used with the option "bulk_config_restore."
- If a firmware upgrade will be performed at the same time, you must generate the full configuration backup file based on the NEW firmware version instead of the current firmware version.

config.txt

To perform device configuration using a USB drive, you must:

- Copy the device configuration file "config.txt" to the root directory of the USB drive.
- Reference the "config.txt" file in the *config* option of the "fwupdate.cfg" file. See ***fwupdate.cfg*** (on page 549).

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 PX 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 PX model and firmware version.

Regular configuration key syntax:

- Each configuration key and value pair is in a single line as shown below:

  ```
  key=value
  ```

  Note: Each value in the file must be separated by a single = character, without any surrounding spaces.

- As of release 3.1.0, multi-line values are supported by using the *Here Document Syntax* with a user-chosen delimiter.

  The following illustration declares a value in two lines. You can replace the delimiter `EOF` with other delimiter strings.

  ```
  key<<EOF
  value line 1
  value line 2
  EOF
  ```

  Note: The line break before the closing EOF is not part of the value. If a line break is required in the value, insert an additional empty line before the closing EOF.

Special configuration keys:

There are 3 special configuration keys that are prefixed with `magic:`.

- A special key that sets a user account's password without knowing the firmware's internal encryption/hashing algorithms is implemented as of release 2.2.13.

  Example:

  ```
  magic:users[1].cleartext_password=joshua
  ```

- Two special keys that set the SNMPv3 passphrases without knowing the firmware's internal encryption/hashing algorithms are implemented as of release 2.4.0.

  Examples:

  ```
  magic:users[1].snmp_v3.auth_phrase=swordfish
  magic:users[1].snmp_v3.priv_phrase=opensesame
  ```

To configure device-specific settings:

1. Make sure the device list configuration file "devices.csv" is available in the USB drive. See ***devices.csv*** (on page 554)
2. In the "config.txt" file, refer each device-specific configuration key to a specific column in the "devices.csv" file. The syntax is: `${column}`, where "column" is a column number.

   Examples:

   ```
   network.interfaces[eth0].ipaddr=${2}
   pdu.name=${16}
   ```

devices.csv

If there are device-specific settings to configure, you must create a device list configuration file - *devices.csv*, to store unique data of each PX.

This file must be:

- An excel file in the CSV format.
- Copied to the root directory of the USB drive.
- Referenced in the *device_list* option of the "fwupdate.cfg" file. See ***fwupdate.cfg*** (on page 549).

Every PX identifies its entry in the "devicelist.csv" file by comparing its serial number or MAC address to one of the columns in the file.

Determine the column to identify PX devices:

- By default, a PX searches for its serial number in the 1st column.
- To override the default, set the *match* option in the "fwupdate.cfg" file to a different column.

Syntax:

- Prior to release 3.1.0, only single-line values containing NO commas are supported. A comma is considered a field delimiter.

  For example:

  ```
  Value-1,Value-2,Value-3
  ```

- As of release 3.1.0, values containing commas, line breaks or double quotes are all supported. The commas and line breaks to be included in the values must be enclosed in double quotes. Every double quote to be included in the value must be escaped with another double quote.

  For example:

  ```
  Value-1,"Value-2,with,three,commas",Value-3


  Value-1,"Value-2,""with""three""double-quotes",Valu
  e-3


  Value-1,"Value-2
  with a line break", Value-3
  ```

Creating Configuration Files via Mass Deployment Utility

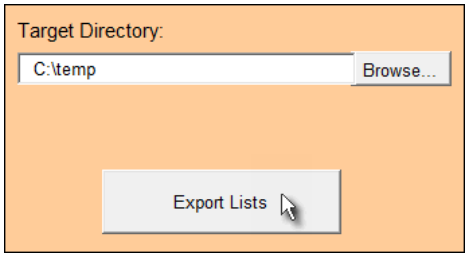
The Mass Deployment Utility is an Excel file that lets you fill in basic information required for the three configuration files, such as the admin account and password.

After entering required information, you can generate all configuration files with only one click, including *fwupdate.cfg*, *config.txt* and *devices.csv*.

To use the Mass Deployment Utility:

1. Download the Mass Deployment Utility from the Raritan website.
   - The utility is named *mass_deployment-xxx* (where xxx is the version number).
   - It is available on the PX section of the ***Support page*** (***http://www.raritan.com/support/***).
2. Make sure Microsoft Excel's security level has been set to Medium or the equivalent for executing unsigned macros of this utility. See the user documentation accompanying your Excel.
3. Launch Excel to open this utility.

   Note: Other office suites, such as OpenOffice and LibreOffice, are not supported.
4. Read the instructions in the 1st spreadsheet of the utility.
5. Enter information in the 2nd and 3rd spreadsheets.
   - The 2nd spreadsheet contains information required for *fwupdate.cfg* and *config.txt*.
   - The 3rd spreadsheet contains device-specific information for *devices.csv*.
6. Return to the 2nd spreadsheet to execute the export macro.
   a. In the Target Directory field, specify the folder where to generate the configuration files. For example, you can specify the connected USB drive.
   b. Click Export Lists to generate configuration files.



7. Verify that at least 3 configuration files are created - *fwupdate.cfg*, *config.txt* and *devices.csv*. You are ready to configure or upgrade any PX with these files. See ***Configuration or Firmware Upgrade with a USB Drive*** (on page 546).

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 PX, 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 549).

To use a USB drive to upgrade the PX:

1. Copy the configuration file "fwupdate.cfg" and an appropriate firmware file to the root directory of the USB drive.
2. Reference the firmware file in the *image* option of the "fwupdate.cfg" file.
3. Plug the USB drive into the USB-A port on the PX.
4. The PX performs the firmware upgrade.
   - On a PX3 Phase II model, the front panel display shows the firmware upgrade percentage.
   - On a PX3 Phase I model, the front panel display shows "FUP."

   Tip: You can remove the USB drive and plug it into another PX for firmware upgrade when the firmware upgrade message displays.
5. It may take one to five minutes to complete the firmware upgrade, depending on your product.
6. When the firmware upgrade finishes, the front panel display indicates the firmware upgrade result.
   - **=-]** (happy smiley): Successful.
   - **=-[** (sad smiley): Failed. Check the log file in the USB drive or contact Raritan Technical Support to look into the failure cause.

Appendix 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 PX devices in the same network.

- Initial deployment
- Configuration changes
- Firmware upgrade
- Downloading diagnostic data

This feature is drastically useful if you have hundreds or even thousands of PX devices to configure or upgrade.

Warning: The feature of bulk configuration or firmware upgrade via DHCP/TFTP only works on standalone PX devices directly connected to the network. This feature does NOT work for slave devices in the USB-cascading configuration.

Tip: For the other alternative, see ***Configuration or Firmware Upgrade with a USB Drive*** (on page 546).

In This Chapter

Bulk Configuration/Upgrade Procedure 557
TFTP Requirements 558
DHCP IPv4 Configuration in Windows 559
DHCP IPv6 Configuration in Windows 569
DHCP IPv4 Configuration in Linux 576
DHCP IPv6 Configuration in Linux 578

Bulk Configuration/Upgrade Procedure

The DHCP/TFTP feature is supported as of release 3.1.0 so make sure that all PX devices which you want to configure or upgrade are running firmware version 3.1.0 or later.

Steps of using DHCP/TFTP for bulk configuration/upgrade:

1. Create configuration files specific to your PX models and firmware versions. See ***Configuration Files*** (on page 547) 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 558).
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 PX.

   Click one or more of the following links for detailed DHCP configuration instructions, based on your system and the IP address type.

   - ***DHCP IPv4 Configuration in Windows*** (on page 559)
   - ***DHCP IPv6 Configuration in Windows*** (on page 569)
   - ***DHCP IPv4 Configuration in Linux*** (on page 576)
   - ***DHCP IPv6 Configuration in Linux*** (on page 578)
5. Make sure all of the desired PX devices use DHCP as the IP configuration method and have been *directly* connected to the network.
6. Re-boot these PX devices. The DHCP server will execute the commands in the "fwupdate.cfg" file on the TFTP server to configure or upgrade those PX 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 557).

If you are going to upload any PX diagnostic file or create a log file in the TFTP server, the first of the following requirements is also required.

- The TFTP server supports the write operation, including file creation and upload.

  In Linux, provide the option "-c" for write support.

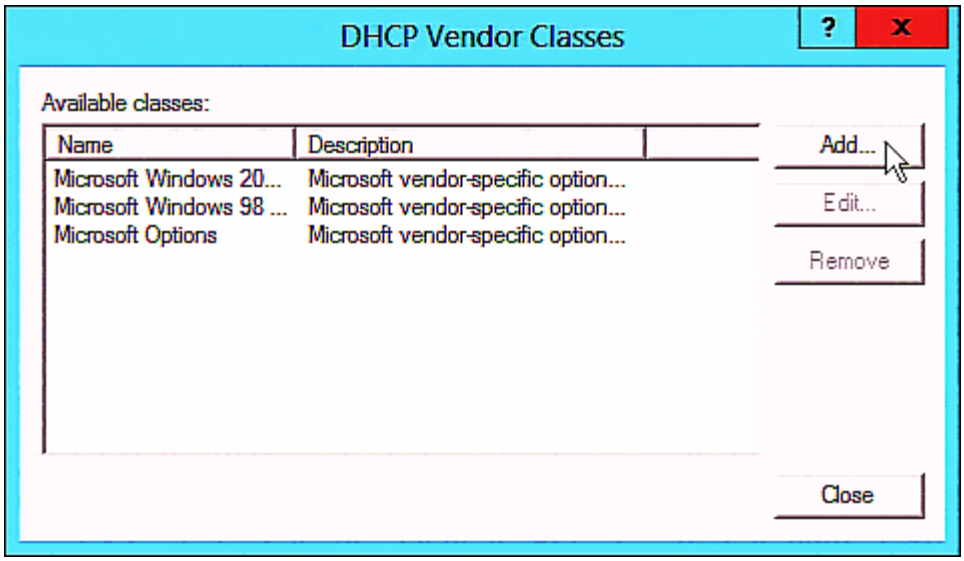
- **Required for uploading the diagnostic file only** - the timeout for file upload is set to one minute or larger.

DHCP IPv4 Configuration in Windows

For those PX devices using IPv4 addresses, follow this procedure to configure your DHCP server. The following illustration is based on Microsoft® Windows Server 2012 system.

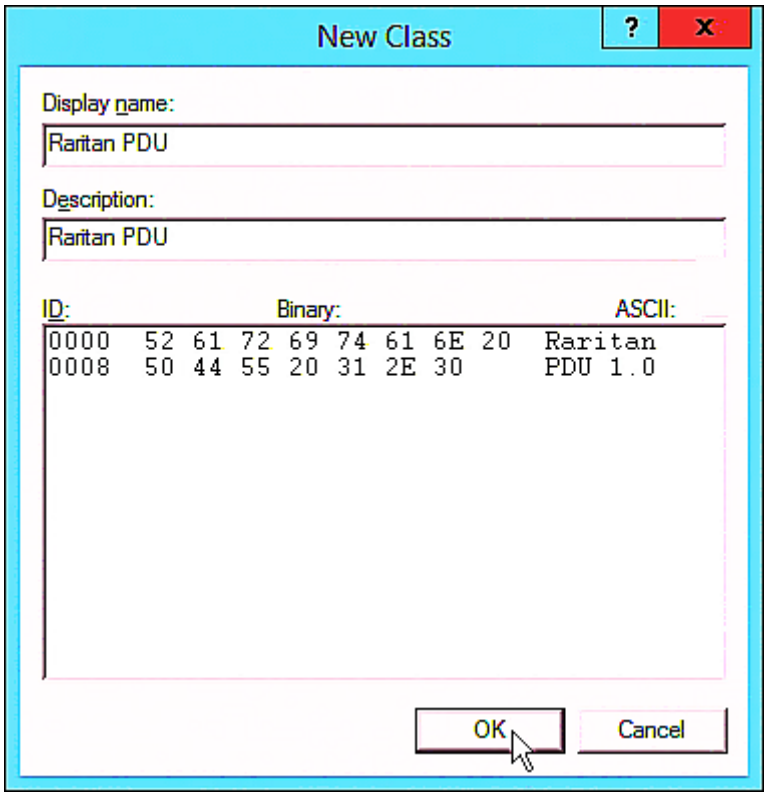
Required Windows IPv4 settings in DHCP:

1. Add a new vendor class for Raritan PX under IPv4.
   a. Right-click the IPv4 node in DHCP to select Define Vendor Classes.
   b. Click Add to add a new vendor class.



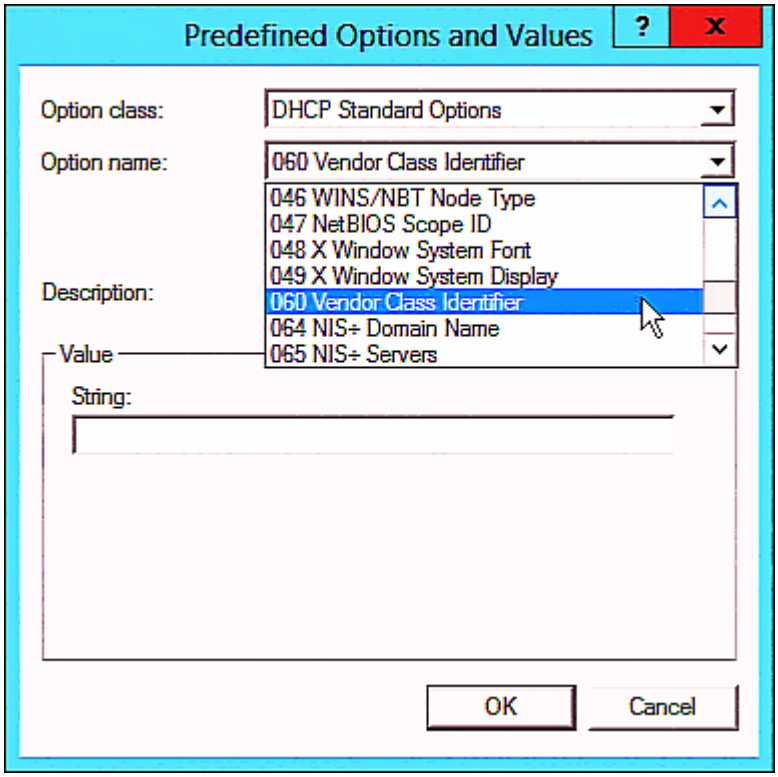
   c. Specify a unique name for this vendor class and type the binary codes of "Raritan PDU 1.0" in the New Class dialog.

The vendor class is named "Raritan PDU" in this illustration.



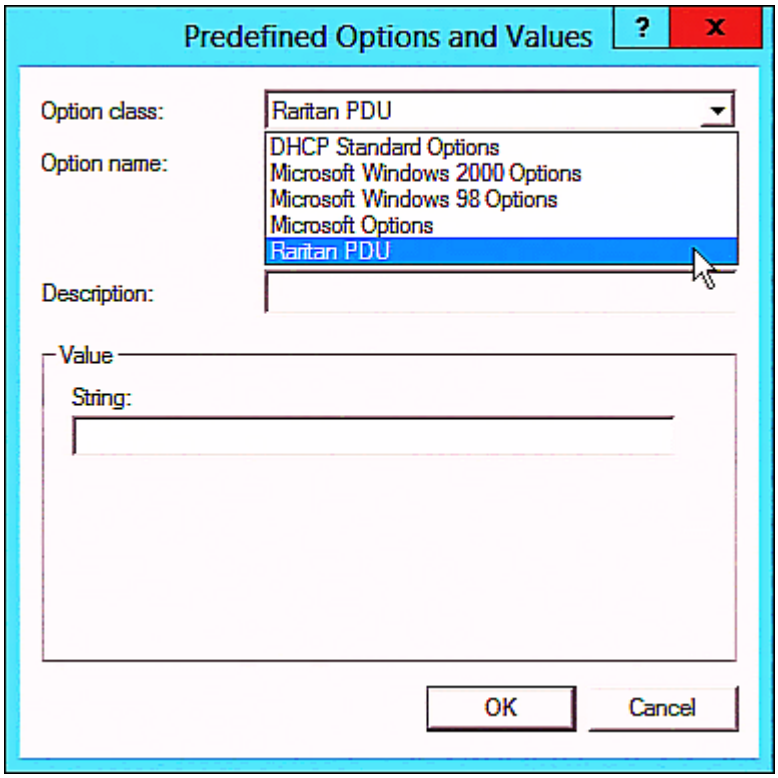
2. Define one DHCP standard option - Vendor Class Identifier.
   a. Right-click the IPv4 node in DHCP to select Set Predefined Options.

b. Select DHCP Standard Options in the "Option class" field, and Vendor Class Identifier in the "Option name" field. Leave the String field blank.

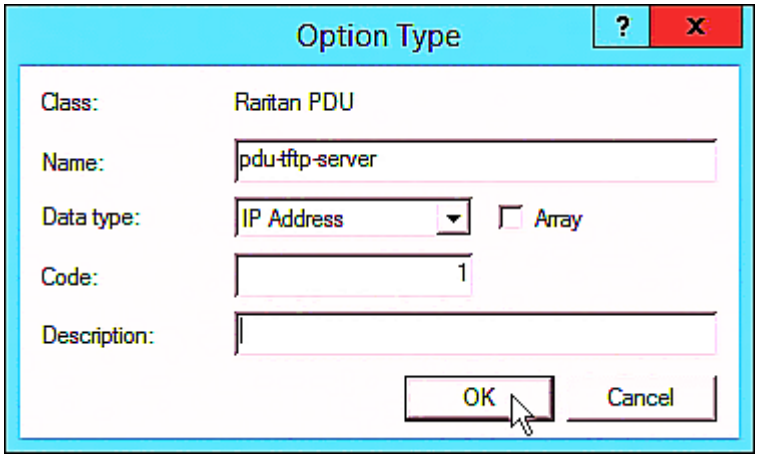


3. Add three options to the new vendor class "Raritan PDU" in the same dialog.

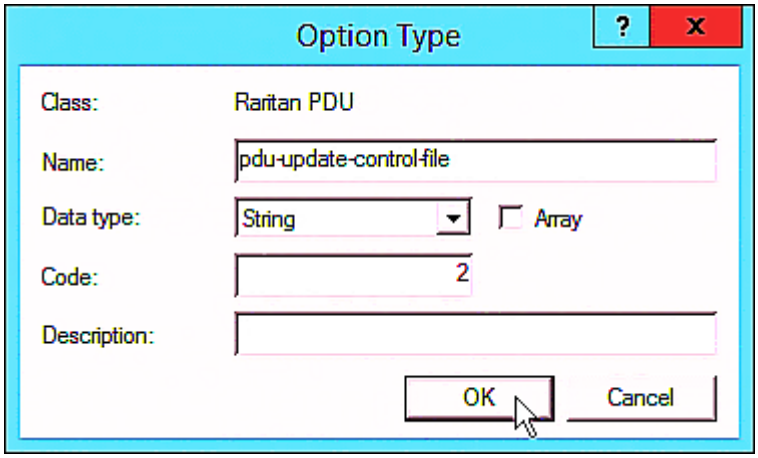
a. Select Raritan PDU in the "Option class" field.



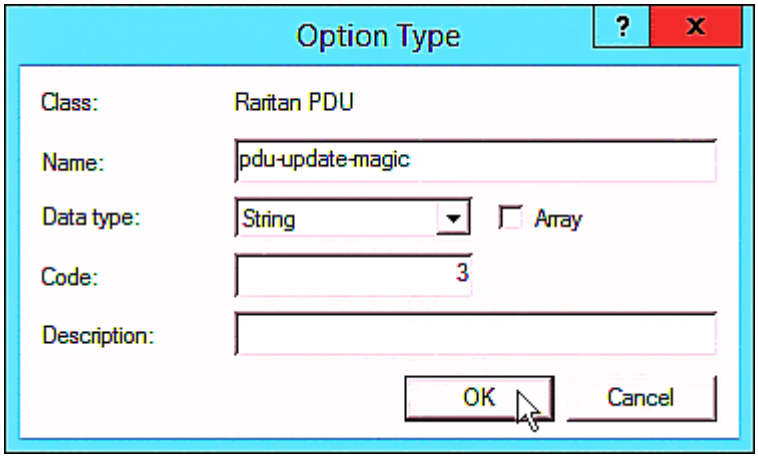
b. Click Add to add the first option. Type "pdu-tftp-server" in the Name field, select IP Address as the data type, and type 1 in the Code field.



c. Click Add to add the second option. Type "pdu-update-control-file" in the Name field, select String as the data type, and type 2 in the Code field.

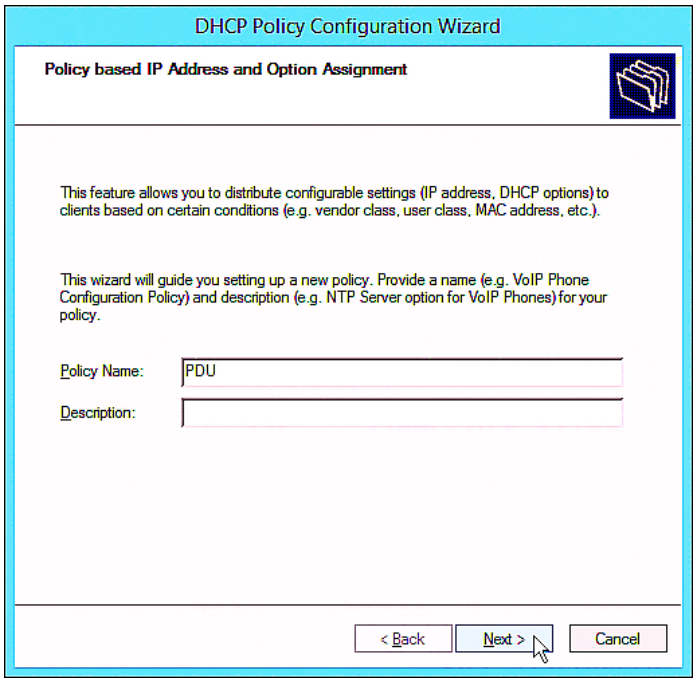


d. Click Add to add the third one. Type "pdu-update-magic" in the Name field, select String as the data type, and type 3 in the Code field.



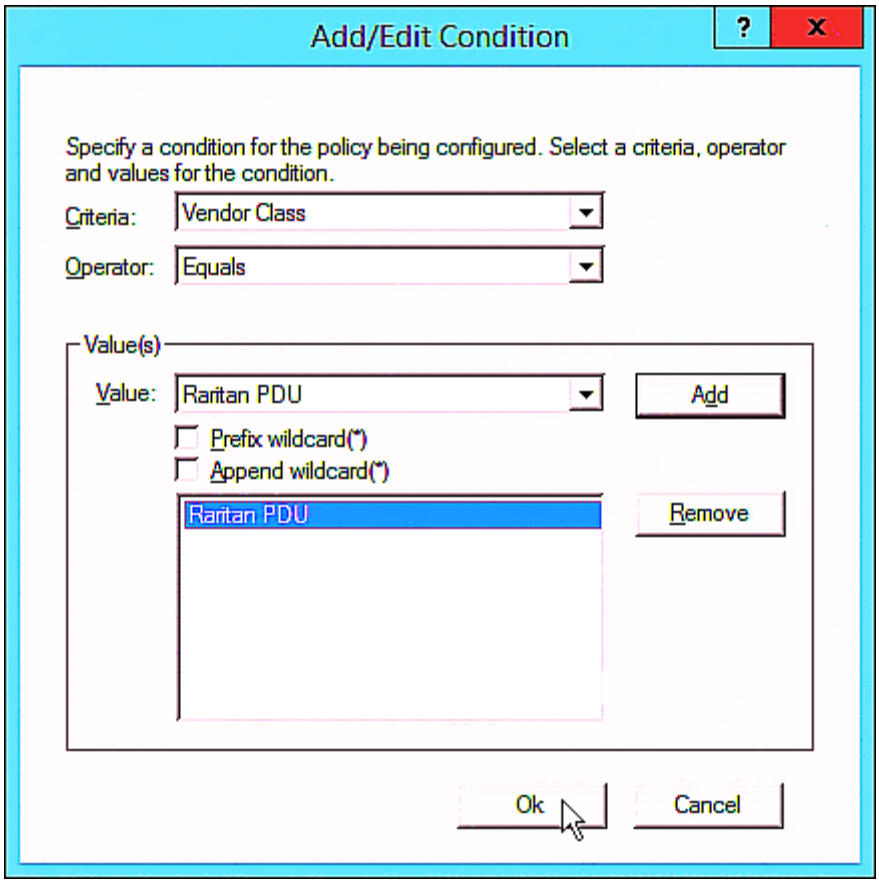
4. Create a new policy associated with the "Raritan PDU" vendor class.
   a. Right-click the Policies node under IPv4 to select New Policy.
   b. Specify a policy name, and click Next.

The policy is named "PDU" in this illustration.



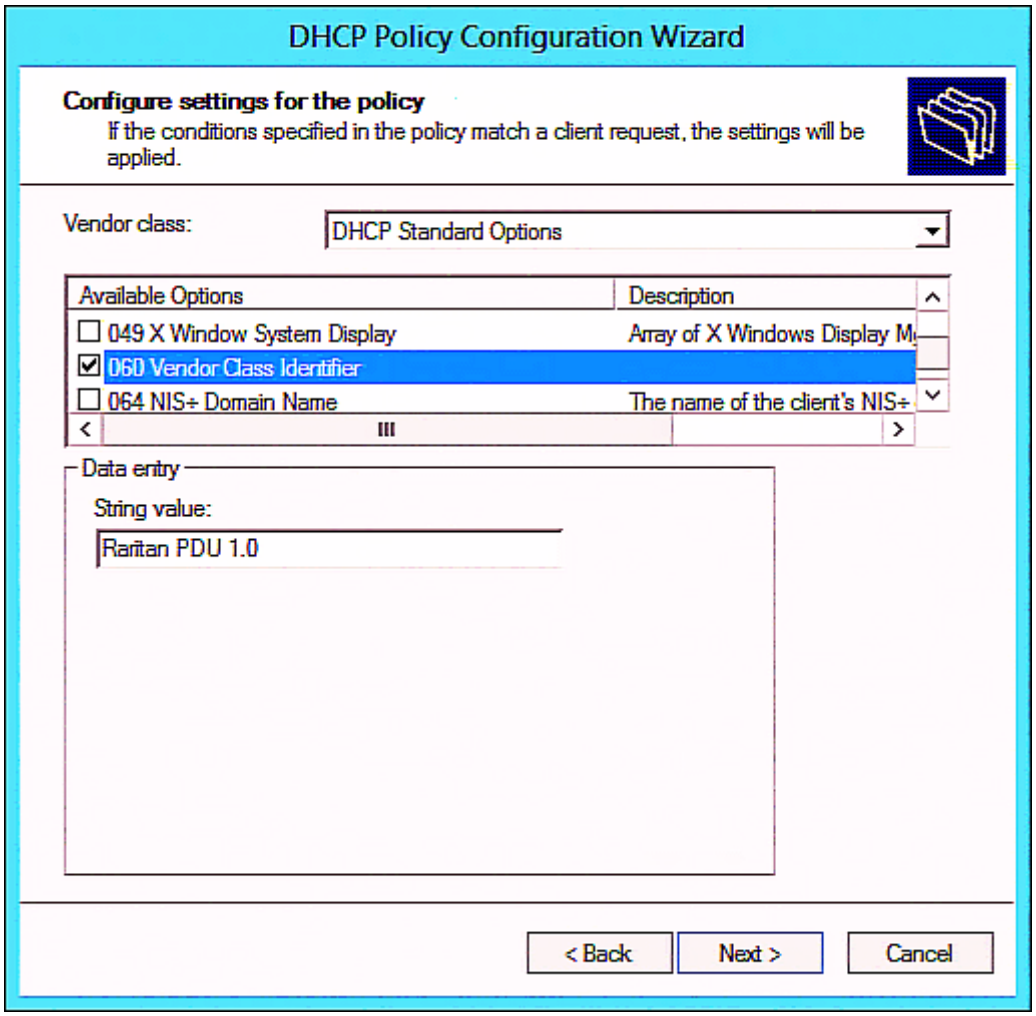
c. Click Add to add a new condition.

d. Select the vendor class "Raritan PDU" in the Value field, click Add and then Ok.

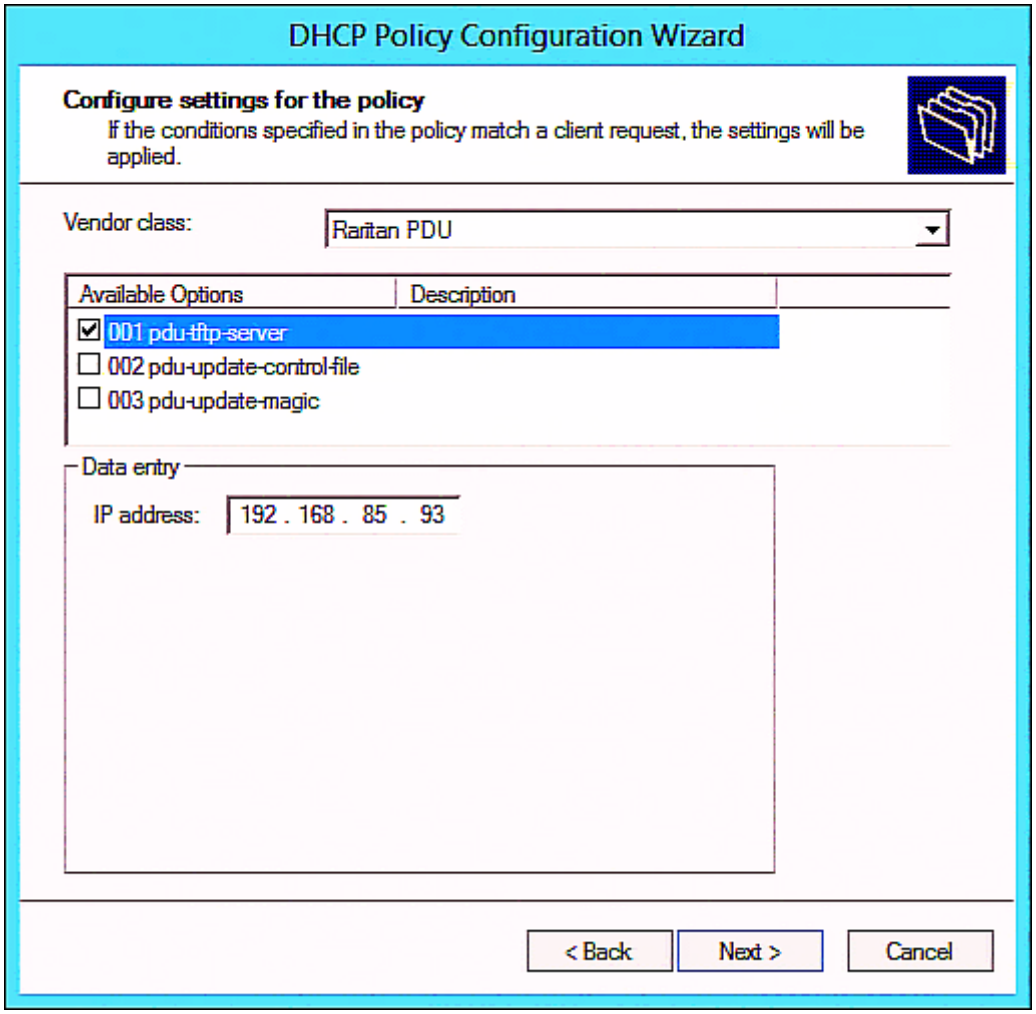


e. Click Next.

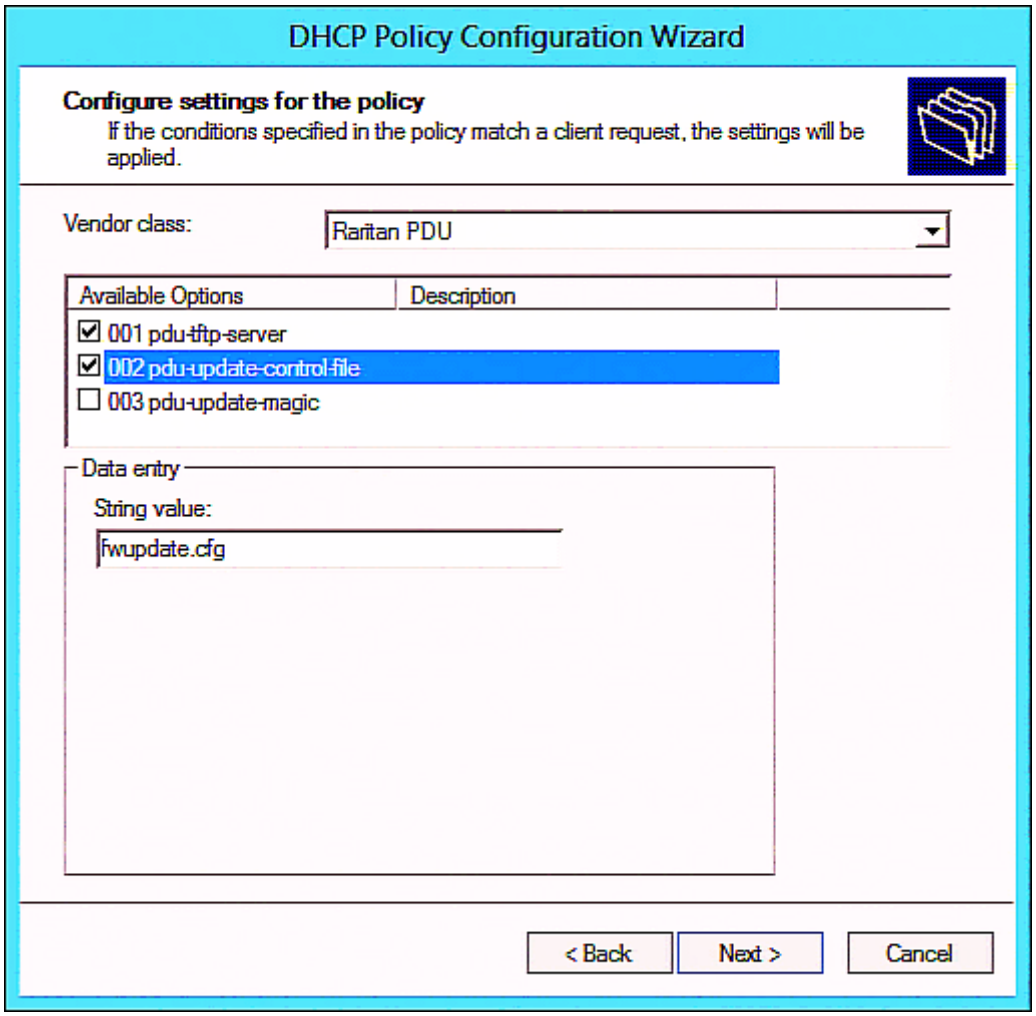
f. Select DHCP Standard Options in the "Vendor class" field, select "060 Vendor Class Identifier" from the Available Options list, and type "Raritan PDU 1.0" in the "String value" field.



g. Select the "Raritan PDU" in the "Vendor class" field, select "001 pdu-tftp-server" from the Available Options list, and type your TFTP server's IPv4 address in the "IP address" field.



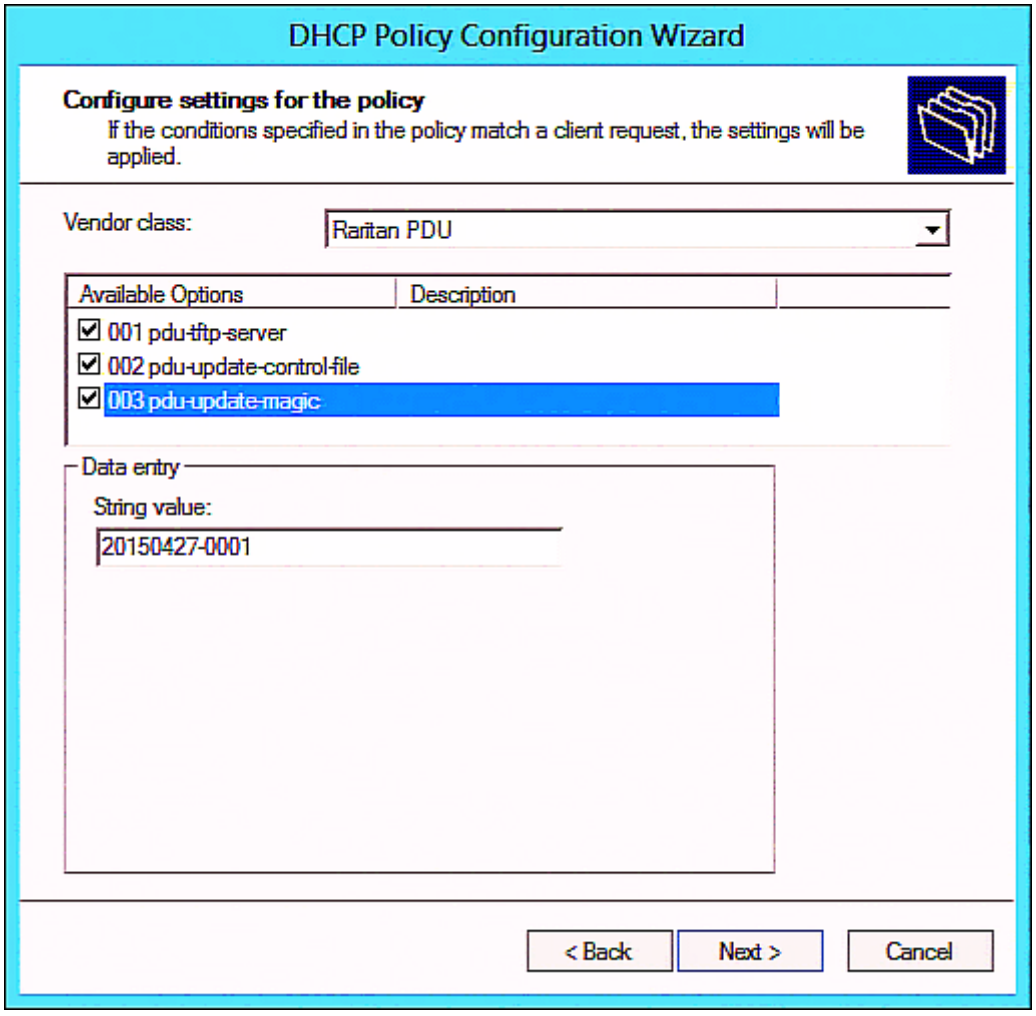
h. Select "002 pdu-update-control-file" from the Available Options list, and type the filename "fwupdate.cfg" in the "String value" field.



i. Select "003 pdu-update-magic" from the Available Options list, and type any string in the "String value" field. This third option/code is the magic cookie to prevent the *fwupdate.cfg* commands from being executed repeatedly. It does NOT matter whether the IPv4 magic cookie is identical to or different from the IPv6 magic cookie.

The magic cookie is a string comprising numerical and/or alphabetical digits in any format. In the following illustration diagram, it is a combination of a date and a serial number.

Important: The magic cookie is transmitted to and stored in PX 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 PX. 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

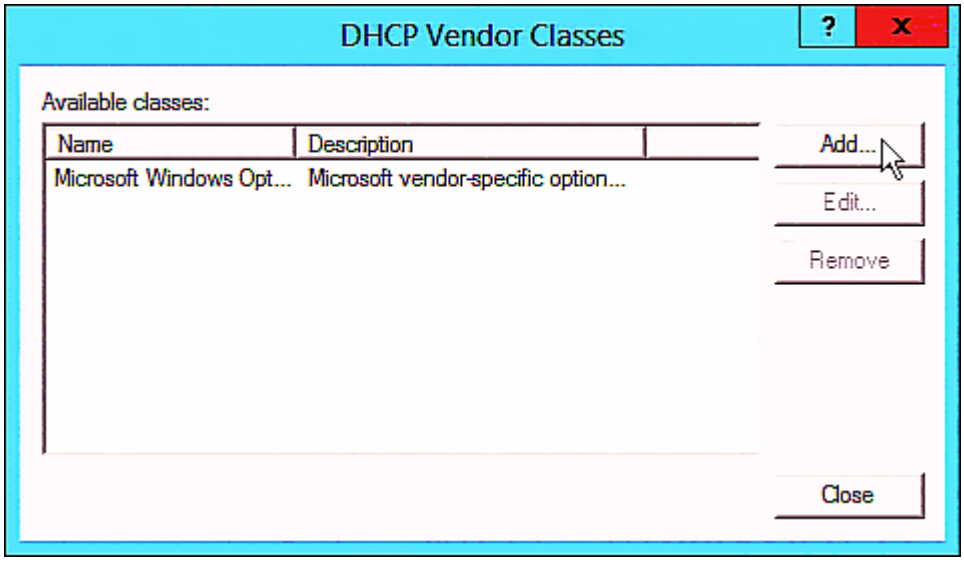
For those PX devices using IPv6 addresses, follow this procedure to configure your DHCP server. The following illustration is based on Microsoft® Windows Server 2012 system.

Required Windows IPv6 settings in DHCP:

1. Add a new vendor class for Raritan PX under IPv6.

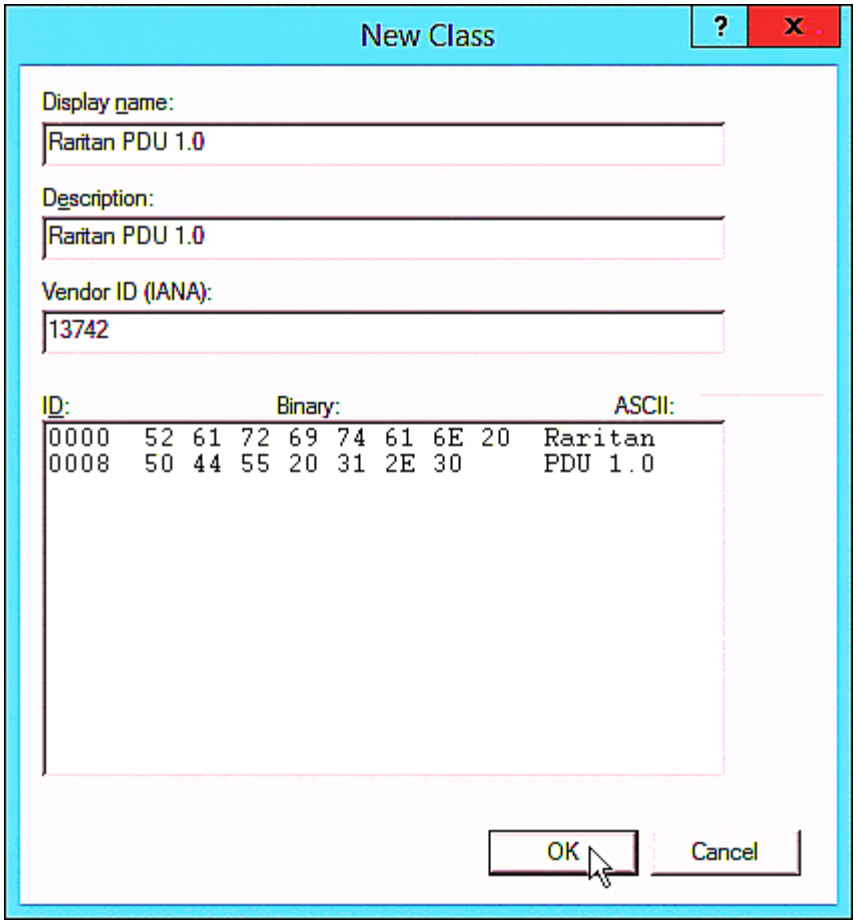
a. Right-click the IPv6 node in DHCP to select Define Vendor Classes.

b. Click Add to add a new vendor class.



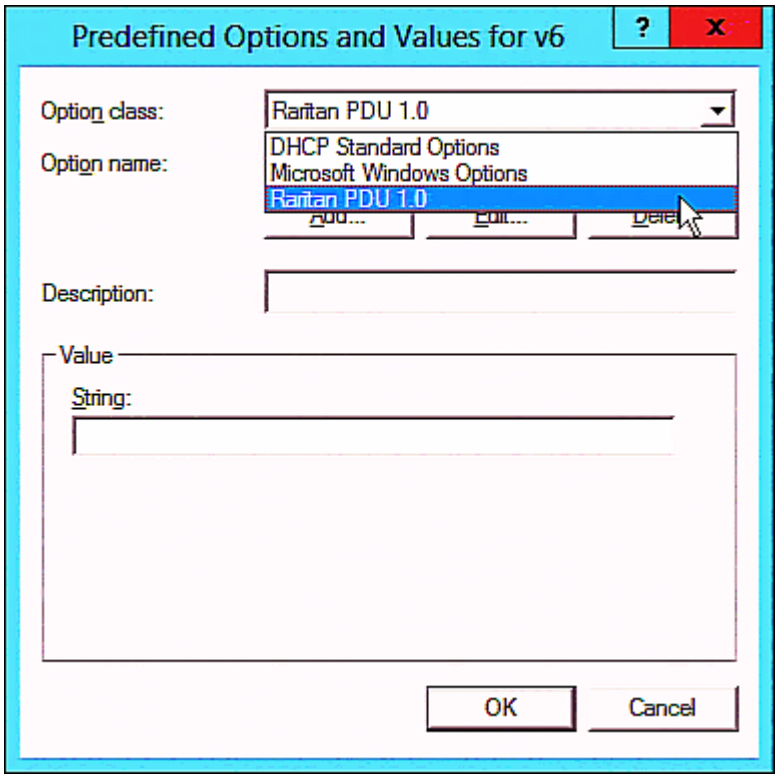
c. Specify a unique name for the vendor class, type "13742" in the "Vendor ID (IANA)" field, and type the binary codes of "Raritan PDU 1.0" in the New Class dialog.

The vendor class is named "Raritan PDU 1.0" in this illustration.

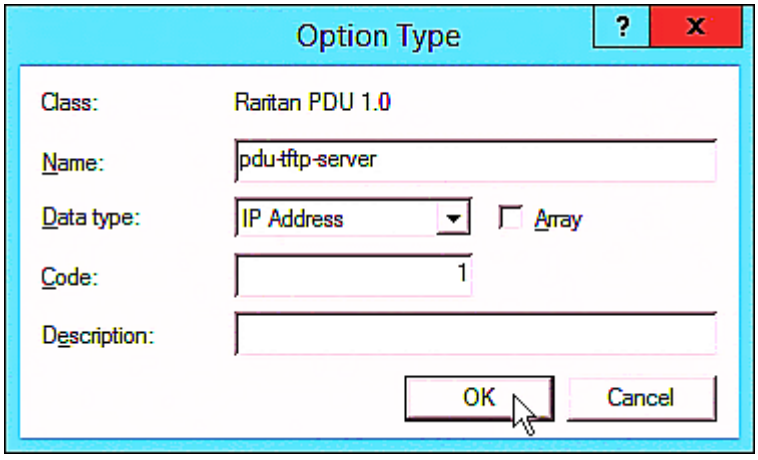


2. Add three options to the "Raritan PDU 1.0" vendor class.
   a. Right-click the IPv6 node in DHCP to select Set Predefined Options.

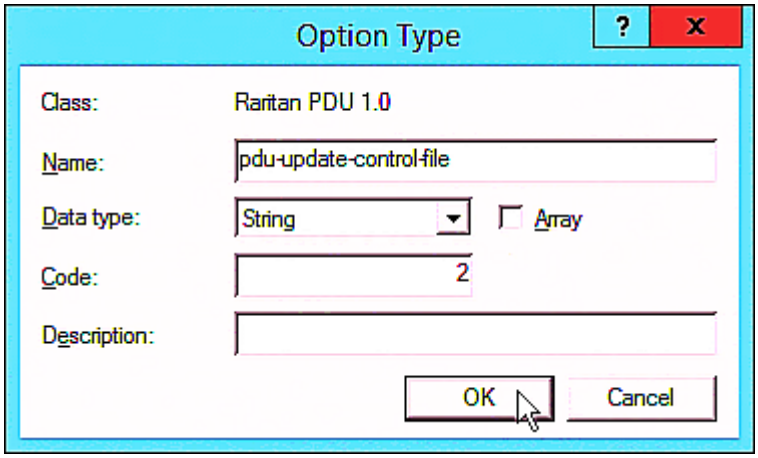
b. Select Raritan PDU 1.0 in the "Option class" field.



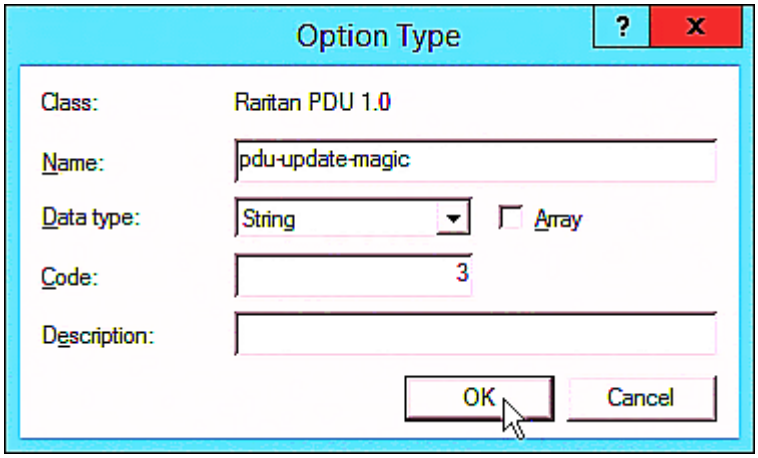
c. Click Add to add the first option. Type "pdu-tftp-server" in the Name field, select IP Address as the data type, and type 1 in the Code field.



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.

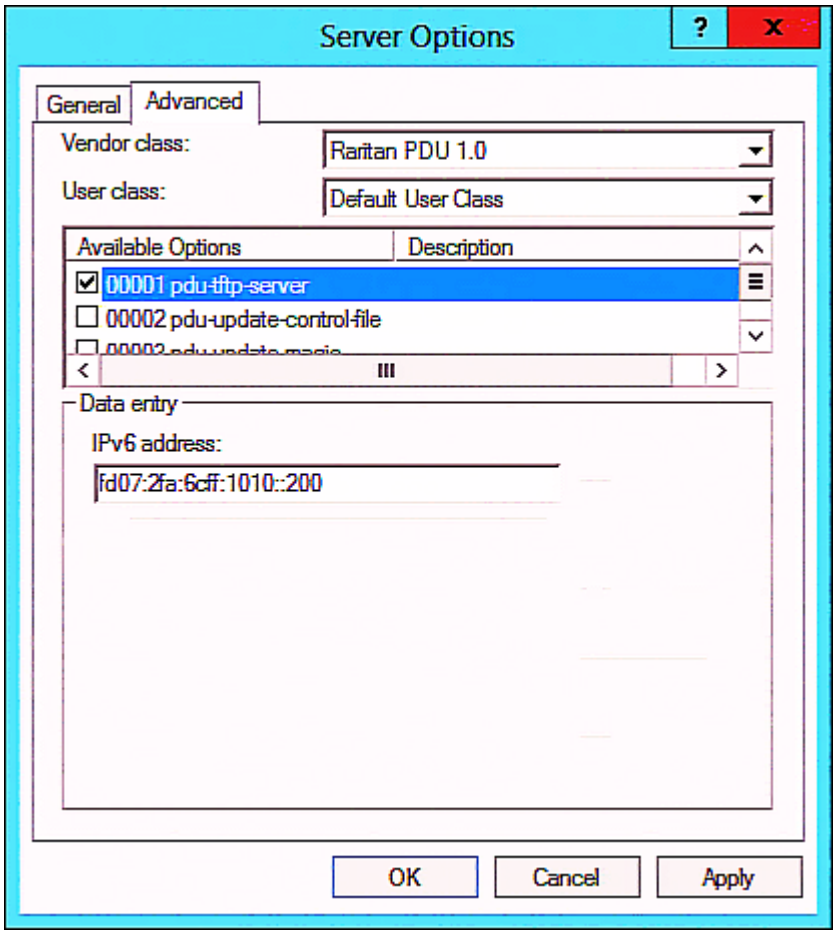


3. Configure server options associated with the "Raritan PDU 1.0" vendor class.

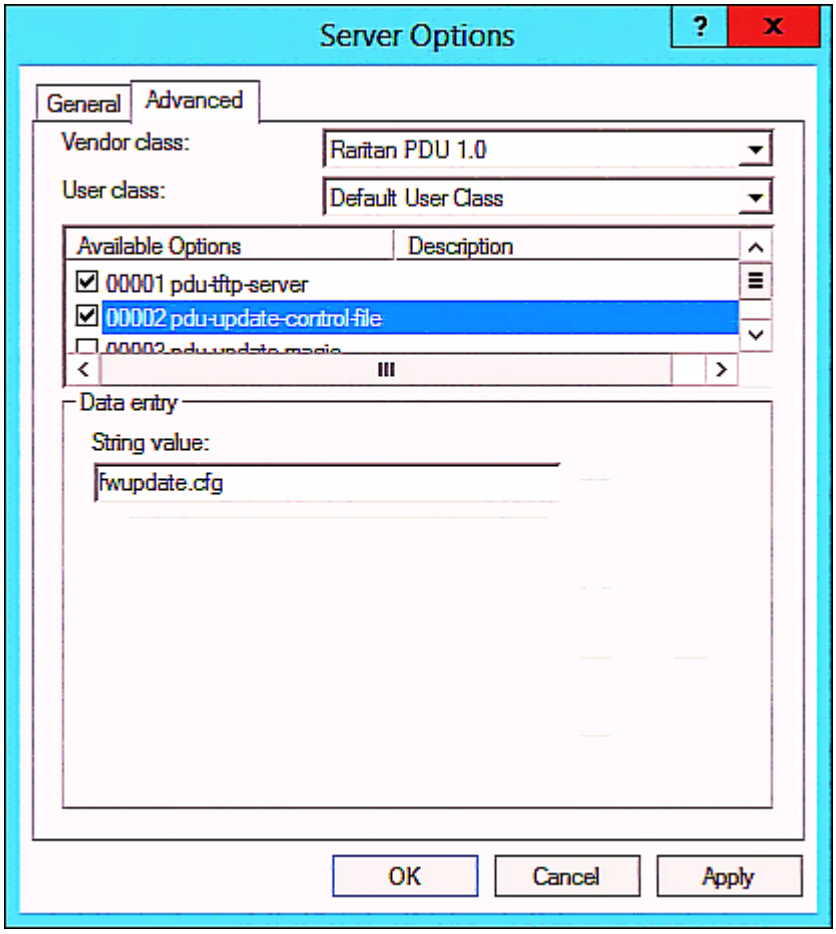
   a. Right-click the Server Options node under IPv6 to select Configure Options.

   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.



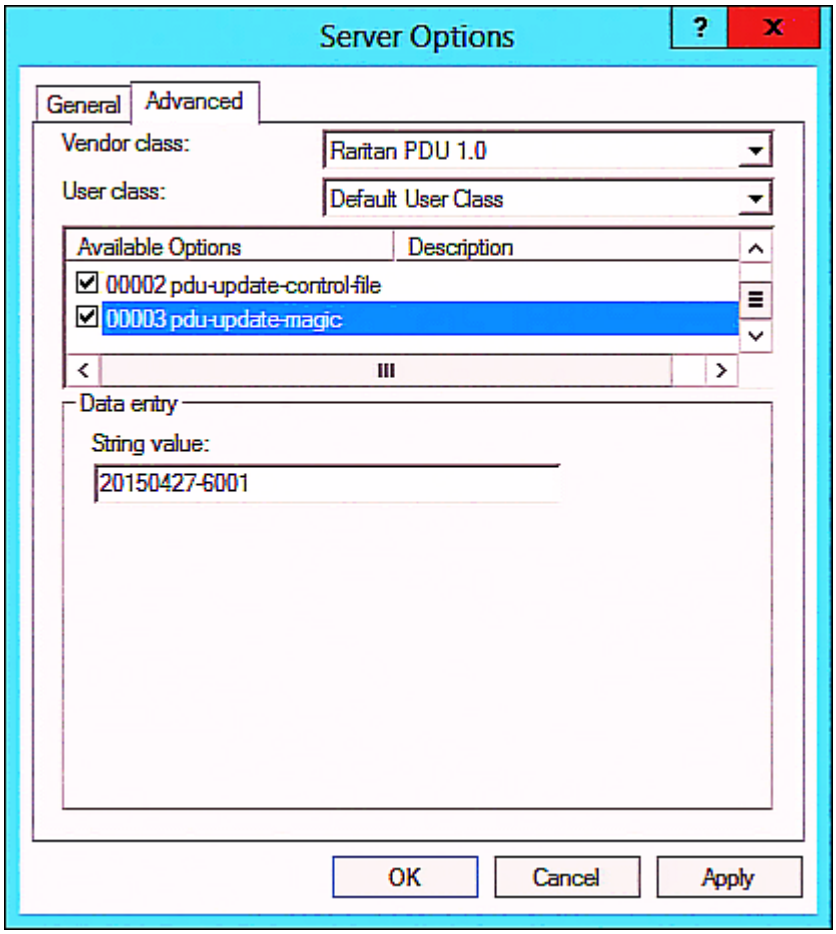
d. Select "00002 pdu-update-control-file" from the Available Options list, and type the filename "fwupdate.cfg" in the "String value" field.



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 PX 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 PX. 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 PX 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 PX 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 PX 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 PX. Therefore, you must modify the magic cookie's value in DHCP when intending to execute the "fwupdate.cfg" commands next time.

▶ **IPv4 illustration example in dhcpd.conf:**

```
[...]

set vendor-string = option vendor-class-identifier;
option space RARITAN code width 1 length width 1 hash size 3;
option RARITAN.pdu-tftp-server code 1 = ip-address;
option RARITAN.pdu-update-control-file code 2 = text;
option RARITAN.pdu-update-magic code 3 = text;


class "raritan" {
    match if option vendor-class-identifier = "Raritan PDU 1.0";
    vendor-option-space          RARITAN;
    option RARITAN.pdu-tftp-server 192.168.1.7;
    option RARITAN.pdu-update-control-file "fwupdate.cfg";
    option RARITAN.pdu-update-magic "20150123-0001";
    option vendor-class-identifier "Raritan PDU 1.0";
}

[...]
```

DHCP IPv6 Configuration in Linux

Modify the "dhcpd6.conf" file for IPv6 settings when your DHCP server is running Linux.

▶ **Required Linux IPv6 settings in DHCP:**

1. Locate and open the "dhcpd6.conf" file of the DHCP server.
2. The PX 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 PX 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 PX. 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 Resetting to Factory Defaults

You can use either the reset button or the command line interface (CLI) to reset the PX.

Important: Exercise caution before resetting the PX 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.

In This Chapter

Using the Reset Button.....580
Using the CLI Command 581

Using the Reset Button

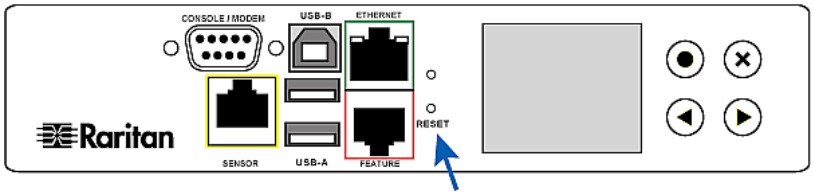
An RS-232 serial connection to a computer is required for using the reset button.

To reset to factory defaults using the reset button:

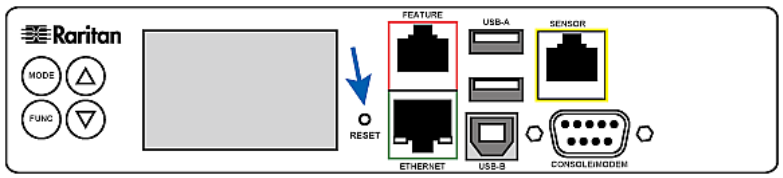
1. Connect a computer to the PX device. See ***Connecting the PX to a Computer*** (on page 18).
2. Launch a terminal emulation program such as HyperTerminal, Kermit, or PuTTY, and open a window on the PX. For information on the serial port configuration, see Step 2 of ***Initial Network Configuration via CLI*** (on page 23).
3. Press (and release) the Reset button of the PX 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 PX to its factory defaults.
5. Wait until the Username prompt appears, indicating the reset is complete.

These diagrams show the reset button on Zero U models.

PX3 Phase II models:



PX3 Phase I models:



Note: HyperTerminal is available on Windows operating systems prior to Windows Vista. For Windows Vista or later versions, you may use PuTTY, which is a free program you can download from the Internet. See PuTTY's documentation for details on configuration.

Using the CLI Command

The Command Line Interface (CLI) provides a reset command for restoring the PX to factory defaults. For information on CLI, see ***Using the Command Line Interface*** (on page 359).

To reset to factory defaults after logging in to the CLI:

1. Connect to the PX device. See ***Logging in to CLI*** (on page 360) or ***Connecting the PX to a Computer*** (on page 18).
2. Launch a terminal emulation program such as HyperTerminal, Kermit, or PuTTY, and open a window on the PX. For information on the serial port configuration, see Step 2 of ***Initial Network Configuration via CLI*** (on page 23).
3. Log in to the CLI by typing the user name "admin" and its password.
4. After the # system prompt appears, type either of the following commands and press Enter.

   ```
   #     reset factorydefaults
   ```

   -- OR --

   ```
   #     reset factorydefaults /y
   ```

5. If you entered the command without "/y" in Step 4, a message appears prompting you to confirm the operation. Type y to confirm the reset.
6. Wait until the Username prompt appears, indicating the reset is complete.

To reset to factory defaults without logging in to the CLI:

The PX provides an easier way to reset the product to factory defaults in the CLI prior to login.

1. Connect to the PX and launch a terminal emulation program as described in the above procedure.
2. At the Username prompt in the CLI, type "factorydefaults" and press Enter.

   ```
   Username:  factorydefaults
   ```

3. Type y on a confirmation message to perform the reset.

Appendix F Available SCP Commands

You can perform a Secure Copy (SCP) command to update the PX firmware, do bulk configuration, or back up and restore the configuration.

In This Chapter

Firmware Update via SCP 583
Bulk Configuration via SCP 584
Backup and Restore via SCP 585

Firmware Update via SCP

Same as any PX firmware update, all user management operations are suspended and all login attempts fail during the SCP firmware update. For details, see ***Firmware Update via Web Interface*** (on page 342).

Warning: Do NOT perform the firmware upgrade over a wireless network connection.

To update the firmware using the SCP command:

1. Type the following SCP command and press Enter.

   ```
   scp <firmware file> <user name>@<device ip>:/fwupdate
   ```

   - *<firmware file>* is the PX firmware's filename. If the firmware file is not in the current directory, you must include the path in the filename.
   - *<user name>* is the "admin" or any user profile with the Firmware Update permission.
   - *<device ip>* is the IP address of the PX that you want to update.
2. When the system prompts you to enter the password for the specified user profile, type it and press Enter.
3. The system transmits the specified firmware file to the PX, and shows the transmission speed and percentage.
4. When the transmission is complete, it shows the following message, indicating that the PX starts to update its firmware now. Wait until the upgrade completes.

   ```
   Starting firmware update. The connection will be closed now.
   ```

SCP command example:

```
scp  pdu-px2-030000-41270.bin
admin@192.168.87.50:/fwupdate
```

Tip: The PSCP works in a similar way to the SCP so the PSCP syntax is similar.
`pscp <firmware file> <user name>@<device ip>:/fwupdate`

Bulk Configuration via SCP

Like performing bulk configuration via the web interface, there are two steps with the bulk configuration using the SCP commands:

a. Save a configuration from a source PX.

b. Copy the configuration file to one or multiple destination PX.

For detailed information on the bulk configuration requirements, see ***Bulk Configuration*** (on page 319).

To save the configuration using the SCP command:

1. Type the following SCP command and press Enter.

   ```
   scp <user name>@<device ip>:/bulk_config.xml
   ```

   - <*user name*> is the "admin" or any user profile with the administrator privileges.
   - <*device ip*> is the IP address of the PX that you want to update.
2. Type the password when the system prompts you to type it.
3. The system saves the configuration from the PX to a file named "bulk_config.xml."

To copy the configuration using the SCP command:

1. Type the following SCP command and press Enter.

   ```
   scp bulk_config.xml <user name>@<device
   ip>:/bulk_restore
   ```

   - <*user name*> is the "admin" or any user profile with the administrator privileges.
   - <*device ip*> is the IP address of the PX that you want to update.
2. Type the password when the system prompts you to type it.

3. The system copies the configuration included in the file "bulk_config.xml" to another PX, and displays the following message.

   ```
   Starting restore operation. The connection will be
   closed now.
   ```

SCP command examples:

- Save operation's example:

  ```
  scp  admin@192.168.87.50:/bulk_config.xml
  ```

- Copy operation's example:

  ```
  scp  bulk_config.xml
  admin@192.168.87.47:/bulk_restore
  ```

Tip: The PSCP works in a similar way to the SCP so its syntax is similar.
Save operation -- `pscp <user name>@<device ip>:/bulk_config.xml`
Copy operation -- `pscp bulk_config.xml <user name>@<device ip>:/bulk_restore`

Backup and Restore via SCP

To back up ALL settings of a PX, including device-specific settings, you should perform the backup operation instead of the bulk configuration.

You can restore all settings to previous ones after a backup file is available.

To back up the settings using the SCP command:

1. Type the following SCP command and press Enter.

   ```
   scp <user name>@<device ip>:/backup_settings.xml
   ```

   - *<user name>* is the "admin" or any user profile with the administrator privileges.
   - *<device ip>* is the IP address of the PX that you want to update.

2. Type the password when the system prompts you to type it.
3. The system saves the settings from the PX to a file named "backup_settings.xml."

To restore the settings using the SCP command:

1. Type the following SCP command and press Enter.

   ```
   scp backup_settings.xml <user name>@<device
   ip>:/settings_restore
   ```

- *<user name>* is the "admin" or any user profile with the administrator privileges.
- *<device ip>* is the IP address of the PX that you want to update.

2. Type the password when the system prompts you to type it.
3. The system copies the configuration included in the file "backup_settings.xml" to the PX, and displays the following message.

```
Starting restore operation. The connection will be
closed now.
```

SCP command examples:

- Backup example:

```
scp  admin@192.168.87.50:/backup_settings.xml
```

- Settings restoration example:

```
scp  backup_settings.xml
admin@192.168.87.50:/settings_restore
```

Tip: The PSCP works in a similar way to the SCP so its syntax is similar.
Backup operation -- `pscp <user name>@<device ip>:/backup_settings.xml`
Restoration operation -- `pscp backup_settings.xml <user name>@<device ip>:/settings_restore`

Appendix G PX Models with Residual Current Monitoring

PX models with residual current monitoring (RCM) detect and report residual current - abnormal flow of current into the protective earth conductor.

Residual current is a safety issue since electrocution is possible if the rack or any device within it is touched.

Warning: PX RCM cannot disconnect power to stop residual current flow. Devices like RCD and GFI disconnect power when residual current is detected, but the PX with RCM are NOT RCD or GFI protected devices.

In This Chapter

RCM Current Sensor 587
RCM State Sensor 588
Compliance with IEC 62020 589
RCM Self-Test 590
Web Interface Operations for RCM 590
Front Panel Operations for RCM 593
RCM SNMP Operations 597
CLI Operations for RCM 598

RCM Current Sensor

The RCM current sensor detects current imbalance which indicates current is flowing to ground. The sensor cannot determine the exact location. It just reports the sum of all residual current in the PDU and devices plugged into it.

Most equipment leaks a small amount of current and the UL/IEC 60950-1 standard for IT equipment permits up to 3mA. The RCM reports the sum so if twenty plugged-in devices - each leaking 1mA, the RCM sensor reports 20mA.

RCM State Sensor

The RCM state sensor reports events based on residual current thresholds or RCM self-test failure.

RCM state	Description
Normal	Residual current is within normal range.
Warning	Residual current is above warning level.
Critical	Residual current is above critical level. In addition to an event, the CRITICAL state causes the PX front panel to display a special error message.
Self-test active	RCM diagnostics are running.
Failure	RCM current sensor has malfunctioned. Contact Raritan Technical Support.

Note: The factory default is to disable the Warning state. To define and enable this state, see **Setting RCM Current Thresholds** *(on page 592).*

Compliance with IEC 62020

IEC 62020 is an international standard for Residual Current Monitors. All PX with RCM are IEC 62020 compliant.

IEC 62020 uses the term *rated residual operating current* (IΔn) to specify residual current, equal to or above which causes an alarm. IEC 62020 recommends preferred values 6mA, 10mA, 30mA, 100mA, 300mA and 500mA. In the PX with RCM, IΔn is specified using the Critical Rated Residual Operating Current threshold.

Note: The PX triggers events when residual current values are above (but not equal to) thresholds. For example, you would set the critical threshold to 29mA to specify the IEC 62020 IΔn of 30mA.

IEC 62020 uses the term *residual non-operating current* (IΔno) to specify residual current, below which does not cause an alarm. IEC 62020 specifies IΔno be no higher than 0.5 IΔn. In PX with RCM, IΔno is set using the RCM Deassertion Hysteresis and this value must be no higher than 0.5 the RCM critical threshold.

PX with RCM allows you to establish an optional WARNING state, which is not part of the IEC 62020 specification. PX RCM remains IEC 62020 compliant when the RCM deassertion hysteresis is configured properly.

IEC 62020 specification	PX with RCM characteristics
Method of operation	Dependent on line voltage. RCM only functions if line voltage is present.
Type of installation	PX with flexible line cords and plugs are for mobile installation and corded connection.
Current paths	1-phase PX are two current paths RCM. 3-phase 3W+PE are three current paths RCM. 3-phase 4W+PE are four current paths RCM.
Ability to adjust residual operating current	Adjustable.
Adjustable time delay	Non-adjustable time delay.
Protection against external influence	Enclosed-type RCM.
Method of mounting	Panel board type RCM.
Method of connection	Not associated with mechanical mounting.
Connection of load conductors	Monitored line is directly connected.
Fault indicating means	Visual, with other output signals.

IEC 62020 specification	PX with RCM characteristics
Ability to directly discriminate	Directionally non-discriminating.
Rated residual operating current	0.5A (highest value).
Residual currents with direct current components	Type A.

RCM Self-Test

PX with RCM have a built-in self-test feature that performs these functions:

- When residual current is less than 3mA, 15mA is momentarily added to determine whether the low reading is due to a faulty sensor. The residual current added is done in a safe manner which does not run current into ground or pose operator risk.
- The RCM state sensor changes to SELF-TEST and then back to its original state if self-test passes, or to the FAILURE state if self-test fails. These state changes are useful to verify your monitoring systems (SNMP, syslog, or email) are correctly set up to receive PX event notifications.

Note: If self-test fails, the FAILURE state persists until another self-test runs and passes.

Web Interface Operations for RCM

The RCM is a PX inlet sensor. To view, configure or run self-test, click the Inlet icon in the PX Explorer pane.

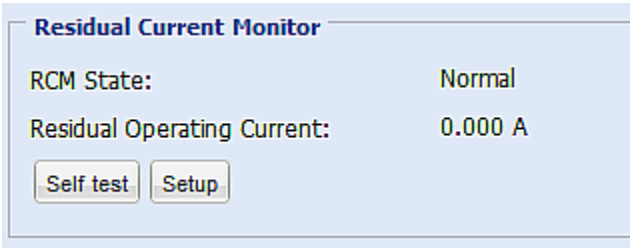
Checking RCM State and Current

A section titled 'Residual Current Monitor' is available on the Inlet page, showing both the present RCM state and residual current.

To check RCM state and current on the Inlet page:

1. Click Inlet I1 in the PX Explorer pane, and the Inlet I1 page opens in the right pane.
2. Locate the Residual Current Monitor section on the Inlet I1 page.
   - RCM State: There are five states - Normal, Warning, Critical, Self-test active and Failure. See ***RCM State Sensor*** (on page 588) for information on these states.

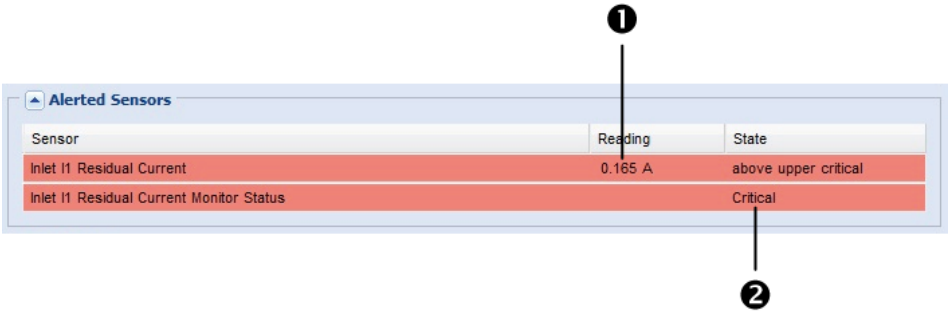
- Residual Operating Current: The magnitude of residual current detected.



Note: To determine the RCM's normal, warning and critical levels, configure the RCM current thresholds. See **Setting RCM Current Thresholds** *(on page 592).*

RCM Critical State Alarm

When a PX device's RCM enters the Critical state, the PX beeps and this alarm is displayed in the Alerted Sensors section of the Dashboard page.

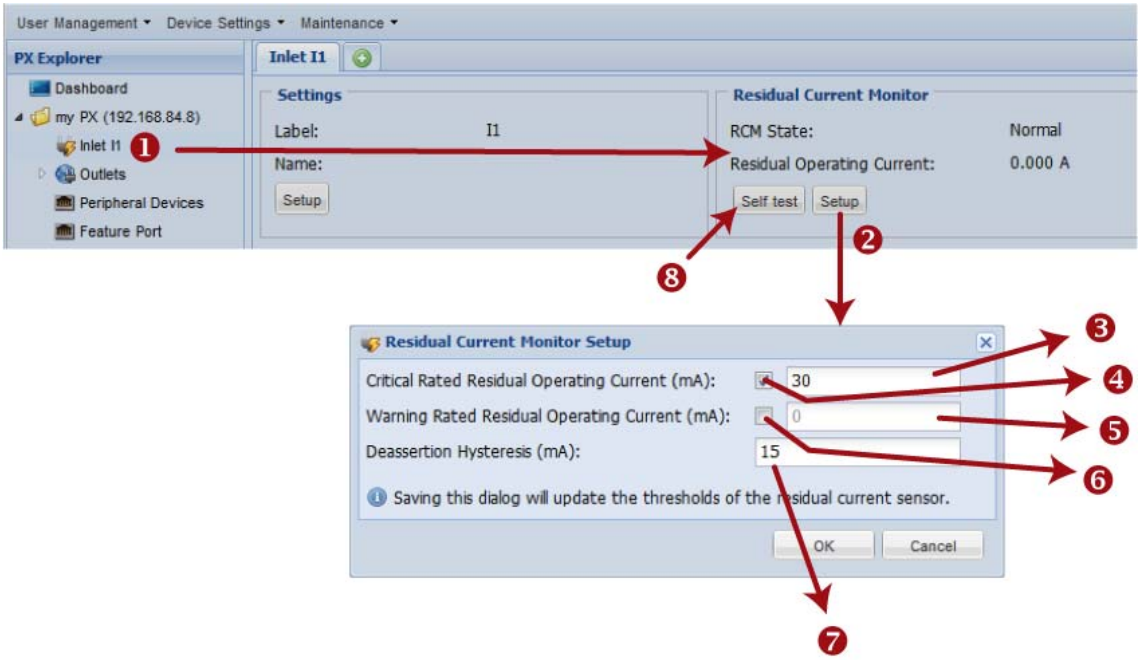


Number	Description
❶	The magnitude of residual current reported by the RCM current sensor.
❷	Critical state reported by the RCM state sensor.

Setting RCM Current Thresholds

The RCM current thresholds define the critical, warning and normal range of residual current.

To configure the RCM current thresholds and run self-test:



1. Click Inlet I1 to open the Inlet page.
2. Click Setup to set up RCM thresholds.
3. Residual current greater than this value triggers Critical RCM state.
4. Enable or disable the RCM critical threshold.
5. Residual current greater than this value triggers Warning RCM state.
6. Enable or disable the RCM warning threshold.
7. Residual current decrease to end Warning or Critical RCM state.
8. Click 'Self test' to run RCM self-test.

Scheduling RCM Self-Test

You can have the PX run RCM self-test automatically at a regular time interval or on a specific date and time. See ***Scheduling an Action*** (on page 262) for the procedure and select "Start residual current monitor self test" to create the scheduled RCM self-test action.

Disabling or Enabling Front Panel RCM Self-Test

You can enable or disable the function of performing the RCM self-test by operating the front panel buttons. By default, this function is enabled.

To disable or enable the front panel RCM self-test:

1. Choose Device Settings > Security > Front Panel Permissions. The Front Panel Permissions dialog appears.
2. Do either of the following:
   - To disable this function, deselect the "Perform RCM self-test" checkbox.
   - To enable this function, select the "Perform RCM self-test" checkbox.
3. Click OK.

Front Panel Operations for RCM

The front panel LCD display shows an alarm message when the RCM enters the critical state. Besides, you can operate the LCD display to check the RCM status.

This section introduces the RCM information shown on the LCD display of a PX3 *phase II* model only.

Note: For the RCM information shown on a PX3 phase I mode's LCD display, see **RCM Information** *(on page 617).*

LCD Message for RCM Critical State

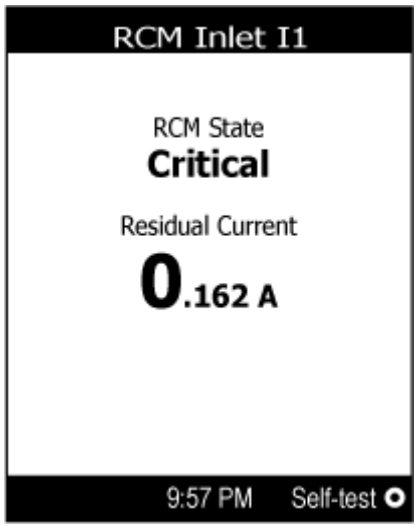
In the RCM critical state, the PDU beeps and the LCD display indicates the RCM critical state.

The RCM alarm information continues to display as long as RCM is in a critical state.

RCM alarm information in the critical state:

1. The LCD display shows two types of information for the inlet with the RCM alarm:
   - RCM State: Critical.

- Residual Current: Residual current value in Amps.



If your PX has more than one inlet, only the inlet which has the RCM alarm enters the critical state.

2. If needed, you can press ⊙ to perform RCM self-test for this inlet. For details, see steps 4 to 5 in the topic titled ***Running RCM Self-Test*** (on page 595).

Checking RCM States on Phase II Models

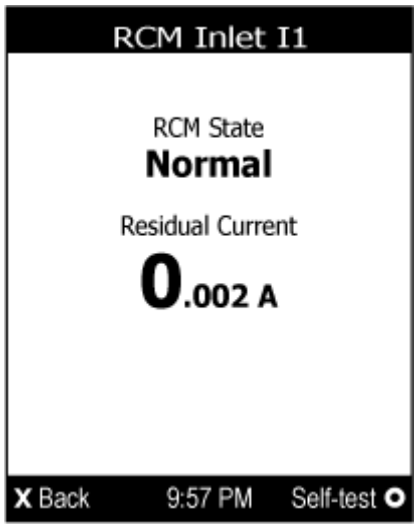
PX3 phase II models allow you to retrieve RCM information from the LCD display even though there is no RCM alarm.

Note: A PX3 phase I model does NOT support this function.

To check RCM information:

1. Press ⊙ or ⊗ to access the ***Main Menu*** (on page 76).
2. Press ▲ or ▼ to select "Residual Current", and press ⊙.
3. The LCD display shows two types of information for Inlet 1.
   - RCM state: Normal or Warning.

- RCM reading: Residual current value in Amps.



If your PX has more than one inlet, a list of inlets is displayed, along with each inlet's RCM state and reading.

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

Displaying the RCM Current

The RCM reading of each inlet is shown along with the RCM status of each inlet. See ***Checking RCM States on Phase II Models*** (on page 594).

Running RCM Self-Test

You can perform the RCM self-test by operating the front panel buttons.

To disable or enable this front panel function, see ***Disabling or Enabling Front Panel RCM Self-Test*** (on page 593). By default, this function is enabled.

To run RCM self-test:

1. Press ◉ or ⊗ to access the ***Main Menu*** (on page 76).
2. Press ▲ or ▼ to select "Residual Current," and press ◉.
3. The LCD display shows the RCM information for the inlet(s).
4. Press ◉ to perform RCM self-test on the selected inlet.
   - If your PDU has multiple inlets, press ▲ or ▼ to select the desired inlet and press ◉.

5. A confirmation message displays. By default, Yes is selected.
   - To execute the RCM self-test, press ⊙.
   - To cancel the RCM self-test, do either of the following:
     - Press ⊗.
     - Press ▲ or ▼ to select No and then press ⊙.

6. After completing the RCM self-test, the LCD display indicates the RCM self-test result: passed or failed.

7. Press ⊙ or ⊗ to return to the RCM information page.
8. Do one of the following:

- To perform RCM self-test for additional inlets, press ▲ or ▼ to select a different inlet and repeat the same steps.
- To return to the Main Menu, press ✕.

RCM SNMP Operations

Make sure you have the correct version of SNMP MIB. The PX supports the RCM feature as of firmware version 2.5.20. See ***Downloading SNMP MIB*** (on page 356) for details.

RCM Trap

An *InletSensorStateChange* trap is sent when the RCM state sensor changes. *InletSensorStateChange* is the generic trap sent for all inlet sensors. The specific trap for RCM has the object *typeOfSensor* set to 27. Included with the trap are *measurementsInletSensorValue* (the residual current value) and *measurementsInletSensorState* (the RCM state that caused the trap).

RCM Residual Current and State Objects

The *inletSensorMeasurementsTable* contains entries for RCM residual current and states.

Use index *sensorType* = 26 to retrieve the row for residual current. Column *measurementsInletSensorValue* contains the residual current.

Use index *sensorType* = 27 to retrieve the row for RCM state. Column *measurementsInletSensorState* contains the RCM state enumeration value.

Setting RCM Thresholds

The inletSensorConfigurationTable contains a row for configuring RCM thresholds. Use index *sensorType* = 26 to reference the row. Columns *inletSensorUpperWarningThreshold*, *inletSensorUpperCriticalThreshold* and *inletSensorHysteresis* set values for RCM warning, critical and deassertion hysteresis respectively.

Note: The PX triggers events when residual current values are above (but not equal to) thresholds. For example, you would set the critical threshold to 29mA to specify the IEC 62020 IΔn of 30mA. See **Compliance with IEC 62020** *(on page 589).*

Running RCM Self-Test

To initiate RCM self-test using SNMP, set column *rcmState* to value 29 in table *rcmSelfTestTable*.

CLI Operations for RCM

For information on using the CLI, see ***Using the Command Line Interface*** (on page 359).

Showing Residual Current Monitor Information

This command syntax shows the residual current monitoring (RCM) information, which is only available on the models with RCM. The information displayed include the RCM current, state and thresholds.

```
#       show residualCurrentMonitor <n>
```

Variables:

- <n> is one of the options: *all*, or a number.

Option	Description
all	Displays the RCM information of 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 RCM information of the specified inlet only. An inlet number needs to be specified only when there are more than 1 inlet on your PDU.

Setting RCM Current Thresholds

Warning Rated Residual Operating Current is the upper warning threshold of the PX RCM sensor, and Critical Rated Residual Operating Current is the upper critical threshold of the RCM sensor. These thresholds are set in the configuration mode. See ***Entering Configuration Mode*** (on page 397).

Note: A residual current sensor's LOWER warning and LOWER critical thresholds do NOT affect the operations of the RCM state sensor so you can ignore them.

To configure the RCM's Critical level:

```
config:#    residualCurrentMonitor <n> criticalRatedResidualOperatingCurrent <value>
```

Note: The PX triggers events when residual current values are above (but not equal to) thresholds. For example, you would set the critical threshold to 29mA to specify the IEC 62020 IΔn of 30mA. See **Compliance with IEC 62020** *(on page 589).*

To configure the RCM's Warning level:

```
config:#    residualCurrentMonitor <n> warningRatedResidualOperatingCurrent <value>
```

To configure the RCM's deassertion hysteresis:

```
config:#    residualCurrentMonitor <n> deassertionHysteresis <hy_value>
```

Variables:

- <n> is the number of the inlet where the desired RCM current sensor is mounted. For a single-inlet PDU, this number is always 1.
- <value> is one of the options: *enable*, *disable* or a numeric value measured in amperes.

Option	Description
enable	Enables the specified RCM current threshold for the specified inlet.
disable	Disables the specified RCM current threshold for the specified inlet.
A numeric value	Sets a value for the specified RCM current threshold of the specified inlet and enables this threshold simultaneously. Note that this value is measured in A, not mA. Therefore, to set the value to 6mA, type *0.006*.

- <hy_value> is a numeric value measured in amperes (A), not milliamperes (mA). For example, to set the value to 15mA, type *0.015*.

Setting Front Panel RCM Self-Test

You can enable or disable the front panel RCM self-test function via CLI in addition to the web interface.

To enable the front panel RCM self-test:

```
#       security frontPanelPermissions add rcmSelfTest
```

To disable the front panel RCM self-test:

```
#       security frontPanelPermissions remove rcmSelfTest
```

Running RCM Self-Test

You can perform RCM self-test for a specific inlet via CLI. After the self-test finishes, the test result is shown: pass or fail.

To perform RCM self-test:

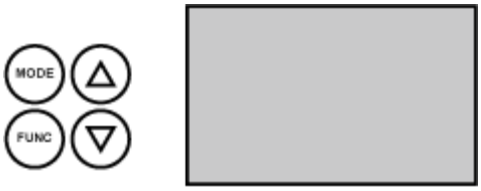
```
#       rcm selfTest inlet <n>
```

Variables:

- <n> is the inlet's number. For a single-inlet PDU, <n> is always 1.

Appendix H PX3 Phase I LCD Display

The following diagram shows the character LCD display panel on a Zero U PX3 **Phase I** model.



The LCD display can show the reading or status of different components on the PX, or the PX's MAC address and IP address.

It consists of:

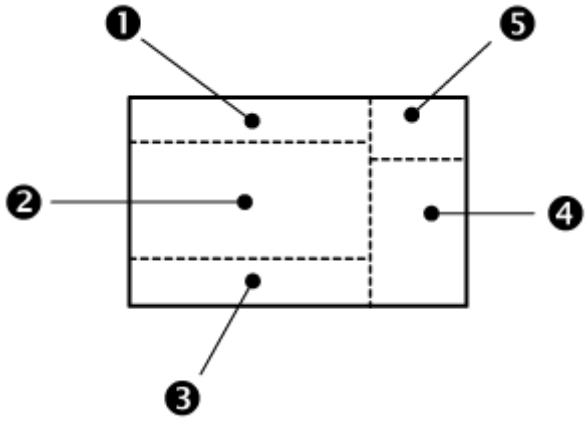
- A character LCD display
- Control buttons

In This Chapter

Overview of the Character LCD Display 601
Control Buttons 602
Operating the Character LCD Display 603

Overview of the Character LCD Display

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



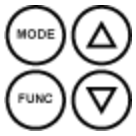
Section	Information shown
1	The selected mode and target, such as INLET 1, OUTLET 1, SENSOR 1, SENSOR 2, and so on.

Section	Information shown
❷	The following information is displayed: • Readings, data or state of the selected target. • During the firmware upgrade, "FUP" is displayed.
❸	Two types of information may be displayed: • The "ALARM" status of the selected target. • The selected inlet line number if your PX is a 3-phase model.
❹	The measurement unit of the displayed data, such as % or °C.
❺	This section indicates: • The Asset Sensor mode if an asset sensor has been connected to the PX. • The device's USB-cascading state - *MASTER* or *SLAVE*. If it is a standalone device, neither MASTER nor SLAVE is displayed.

Note: During the firmware upgrade, some PX models may show bx in the section 1 to indicate the relay or meter board numbered x is being updated.

Control Buttons

There are four control buttons.



- Up and Down buttons for selecting a specific target, which can be an inlet, outlet, overcurrent protector, environmental sensor or a device setting
- MODE button for switching between various modes, including:

  - Inlet mode

  - Outlet mode

  - Overcurrent Protector mode

  - Device mode

  - Sensor mode

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

See ***Overview of the Character LCD Display*** (on page 601) for details.

- FUNC (Function) button for switching between different data of the selected target, such as the current, voltage or power readings of a particular outlet

Operating the Character LCD Display

After powering on or resetting this product, the LCD display panel shows the current reading of OUTLET 1 by default before you select a different target.

Outlet Information

The Outlet mode is displayed as "OUTLET" on the LCD display. By default the PX displays the current reading of OUTLET 1.

Below illustrates the outlet information shown on the LCD display.

Section	Example information
❶	The selected target is OUTLET 3.
❷	This outlet's current reading is 2 amps.
❸	The word "MASTER" indicates the PX is the master device in a USB-cascading configuration. See ***Cascading the PX via USB*** (on page 29). Note: For a standalone PX, this word is NOT displayed. For a slave device, it shows "SLAVE" instead.
❹	The measurement unit is A (Amp), indicating that the reading is the RMS current.

▶ **To display a single-phase outlet's information:**

1. By default this product enters the Outlet mode. If not, press the MODE button until the word "OUTLET" is displayed.
2. In the Outlet mode, press the Up or Down button until the desired outlet's number is displayed at the top of the LCD display.
3. Press the FUNC button to switch between voltage, active power and current readings of the selected target.

- A is displayed for the current reading. A means Amp.
- V is displayed for the voltage reading. V means Volt.
- W is displayed for the power reading. W means Watt.

If the word "ALARM" appears below the reading, it means the currently displayed reading already reaches or crosses the upper or lower thresholds.

To display a 3-phase outlet's information

1. In the Outlet mode, press the Up or Down button until the desired 3-phase outlet is selected.
2. While that 3-phase outlet is being selected, press the Up or Down button to switch between each line, indicated as L1, L2 or L3 at the bottom of the display.
3. When the desired line is being displayed, press the FUNC button to switch between voltage, active power and current readings of this particular line.
   - A is displayed for the current reading. A means Amp.
   - V is displayed for the voltage reading. V means Volt. When voltage is selected, L1-L2, L2-L3, or L3-L1 is displayed at the bottom of the display.
   - W is displayed for the power reading. W means Watt.
4. To show the unbalanced load and active power of this 3-phase outlet, do the following:
   a. Switch to the current reading of L1.
   b. Press the Down button until '%' or 'W' is displayed to the right of the display. Make sure NONE of the lines (L1, L2, L3, L1-L2, L2-L3 or L3-L1) is displayed at the bottom of the display.
      - Unbalanced load - % is displayed for the unbalanced current value.
      - Active power - W is displayed for the power reading. W means Watt.

Inlet Information

The Inlet mode is displayed as "INLET" on the LCD display. Below illustrates the inlet information shown on the LCD display.

Section	Example information
1	The selected target is INLET 1.
2	This inlet's L1 current reading is 23 amps.
3	The selected inlet line is L1.
4	The word "MASTER" indicates the PX is the master device in a USB-cascading configuration. See ***Cascading the PX via USB*** (on page 29). *Note: For a standalone PX, this word is NOT displayed. For a slave device, it shows "SLAVE" instead.*
5	The measurement unit is A (ampere).

To display an inlet's information:

1. Press the MODE button until the term "INLET" is displayed.
2. On a multi-inlet model, press the Up or Down button until the desired inlet's number is displayed at the top.
3. If your PX is a 3-phase model, the selected inlet line is indicated below the reading. Press the Up or Down button until the desired inlet line's number (L1, L2, L3, L1-L2, L2-L3 or L3-L1) is shown.
4. Press the FUNC button to switch between voltage, active power and current readings of the selected target.
   - A is displayed for the current reading. A means Amp.
   - V is displayed for the voltage reading. V means Volt.
   - W is displayed for the power reading. W means Watt.

   If the word "ALARM" appears below the reading, it means the currently displayed reading already reaches or crosses the upper or lower thresholds.

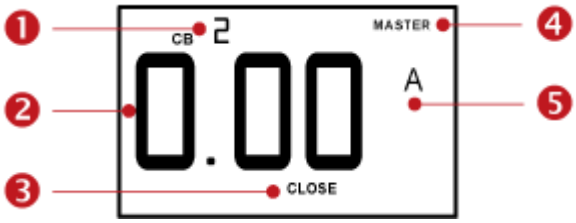
To display the unbalanced load and active power of a 3-phase inlet:

1. Switch to the current reading of any inlet line.
2. Press the Up or Down button until "W" or "%" is displayed to the right of the LCD display. Make sure NONE of the inlet's line number is displayed at the bottom of the display.
   - Unbalanced load - % is displayed for the unbalanced current value.
   - Active power - W is displayed for the power reading. W means Watt.

Overcurrent Protector Information

The Overcurrent Protector mode is displayed as either "CB" or "FUSE" on the LCD display, which varies according to the type of overcurrent protector implemented on your PX. CB refers to the circuit breaker and FUSE refers to the fuse.

Below illustrates an overcurrent protector's information.



Section	Example information
❶	The selected target is the second circuit breaker (CB 2).
❷	This circuit breaker's current reading is 0 amps.
❸	The word "CLOSE" indicates that the state of the selected circuit breaker is closed.
❹	The word "MASTER" indicates the PX is the master device in a USB-cascading configuration. See ***Cascading the PX via USB*** (on page 29). *Note: For a standalone PX, this word is NOT displayed. For a slave device, it shows "SLAVE" instead.*
❺	The measurement unit is A (Amp), indicating that the reading is the current.

To display the overcurrent protector information:

1. Press the MODE button until the word "CB" or "FUSE" is displayed.
2. In the Overcurrent Protector mode, press the Up or Down button until the desired overcurrent protector's number is displayed at the top of the LCD display.
3. Check the reading and the text shown below the reading: CLOSE or OPEN.
   - CLOSE: The selected circuit breaker is closed, or the selected fuse is normal.
   - OPEN: The selected circuit breaker is open, or the selected fuse has burned out. When this occurs, the term CbE is displayed in place of the reading and a blinking word "ALARM" appears next to the word OPEN.

IPv4 Address

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

Below illustrates the IP address information.

Section	Example information
❶	"d" means the LCD display has entered the Device mode.
❷	The LCD display is showing 192, which is one of the four IP address octets. It will cycle through four octets.
❸	"i4" indicates that the IP address shown on the LCD display is an IPv4 address.

Section	Example information
❹	The word "MASTER" indicates the PX is the master device in a USB-cascading configuration. See ***Cascading the PX via USB*** (on page 29). *Note: For a standalone PX, this word is NOT displayed. For a slave device, it shows "SLAVE" instead.*

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

To display the IPv4 address:

1. Press the MODE button to enter the Device mode, indicated by an alphabet "d" at the top left of the display.
2. The LCD display cycles between the four octets of the IPv4 address, indicated by "i4" at the upper right corner of the display.

   For example, 192.168.84.4 cycles in this sequence:

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

MAC Address

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

Below illustrates the MAC address information.

Section	Example information
❶	"d" means the LCD display has entered the Device mode.
❷	"M" indicates that the displayed information is the MAC address.
❸	The word "MASTER" indicates the PX is the master device in a USB-cascading configuration. See ***Cascading the PX via USB*** (on page 29). *Note: For a standalone PX, this word is NOT displayed. For a slave device, it shows "SLAVE" instead.*
❹	The LCD display is showing "03," which is part of the MAC address.

To display the MAC address:

1. Press the MODE button to enter the Device mode, indicated by a 'd' in at the top left of the display.
2. Press the FUNC button until the MAC address is displayed. The character "M" appears in the left side of the LCD display.
3. The MAC address is displayed as "M:XX", where XX are two digits of the MAC address. The LCD will cycle through the MAC address from the first two digits to the final two.

   For example, if the MAC address is 00:0d:5d:03:5E:1A, the LCD display shows the following information one after another:

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

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

Outlet Switching

This section applies to outlet-switching capable models only.

You can turn on or off any outlet using the LCD display in the outlet switching mode. To do this, you must first enable the front panel outlet control function. See ***Enabling Front Panel Outlet Switching*** (on page 224).

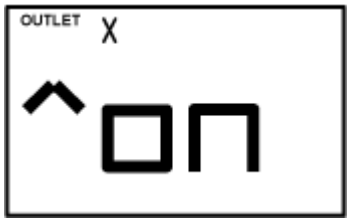
To turn on or off an outlet:

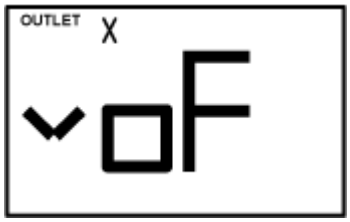
1. Press the MODE button until the LCD display enters the outlet switching mode, which is indicated by the power state of OUTLET 1.

- When outlet 1 has been powered on, the word 'on' is displayed as shown below.

- When outlet 1 has been powered off, the word "oFF" is displayed instead.

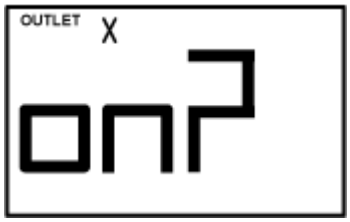
2. Press the Up or Down button to select the desired outlet. The selected outlet's number is displayed at the top of the LCD display.
3. Press the FUNC button to to perform the outlet switching operation. The LCD display cycles between two messages as shown in the two diagrams below. In the following diagrams, X represents the selected outlet's number.



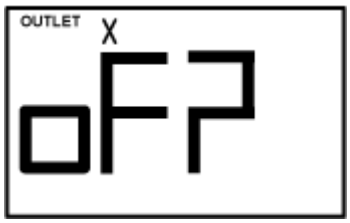


To cancel the outlet switching operation, press the FUNC button again.

4. To turn on the outlet, press the Up button. The "on?" confirmation message displays.



To turn off the outlet, press the Down button. The "oF?" confirmation message displays.



5. Press the same button as step 4 again to confirm the operation.

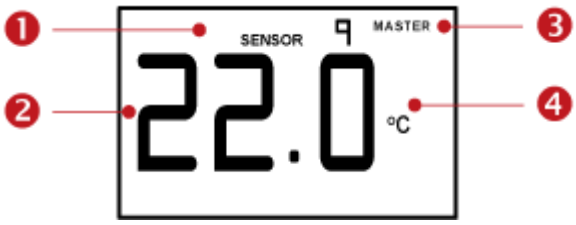
   Note: If you press a different button in this step, for example, pressed the Down button in step 4 but the Up button in step 5, the outlet switching operation is not confirmed and the LCD display will return to the messages in step 3.

6. The outlet switching operation is confirmed now and the LCD display indicates the latest power state of the selected outlet.
   - on: The outlet has been turned on.
   - oFF: The outlet has been turned off.
7. You can verify the power state of the selected outlet by checking its LED color. Green indicates the power off state and red indicates the power on state.

Environmental Sensor Information

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

Below illustrates the environmental sensor information.



Number	Example information
❶	The selected target is the environmental sensor whose ID number is 9 (SENSOR 9).
❷	The selected environmental sensor's reading is 22 °C.
❸	The word "MASTER" indicates the PX is the master device in a USB-cascading configuration. See ***Cascading the PX via USB*** (on page 29). *Note: For a standalone PX, this word is NOT displayed. For a slave device, it shows "SLAVE" instead.*

Number	Example information
❹	The measurement unit is °C (degrees in Celsius).

To display the environmental sensor information:

1. Press the MODE button until this product enters the Sensor mode, as indicated by "SENSOR" at the top of the LCD display.
2. Press the Up or Down button until the desired environmental sensor's ID number is displayed.
3. For example, "SENSOR 1" refers to the sensor #1 listed on the PX web interface.
4. The LCD display shows the reading or state of the selected sensor in the middle of the LCD display.
   - When showing a numeric sensor's reading, the appropriate measurement unit is displayed to the right of the reading.

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

   - Available states for a discrete sensor:

States	Description
nor	The sensor is in the normal state.
ALA	The sensor enters the alarmed state. This state is accompanied with the word "ALARM" below it.

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

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

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

5. Press the FUNC button to show the sensor's port position. There are two types of information.
   - *P:n* (where n is the SENSOR port's number): This information indicates the SENSOR port number.
   - *C:x* (where x is the sensor's position in a sensor chain): This information indicates the sensor's position in a chain, which is available for DPX2, DPX3 and DX sensors only. The LCD display will cycle between the port information (*P:n*) and chain position information (*C:x*).

     Note that if the DPX3-ENVHUB4 sensor hub is used to connect the DPX2, DPX3 or DX sensors, the chain position information (C:x) is displayed twice - the first one indicates the sensor hub's chain position, which is always *C:1*, and the second one indicates the sensor's chain position.
6. Press the FUNC button to display the X, Y and Z coordinates of the sensor respectively.
   - X coordinate is shown as "x:NN," where NN are the first two numeric digits entered for the X coordinate in the web interface.
   - Y coordinate is shown as "y:NN," where NN are the first two numeric digits entered for the Y coordinate in the web interface.
   - Z coordinate is shown as "z:NN," where NN are the first two numeric digits entered for the Z coordinate in the web interface.

   If one or both of the first two digits for a specific coordinate are alphabetical characters, these alphabetical characters are replaced with dashes (-).
7. Press the FUNC button to display the serial number of the sensor, which is shown as "s:XX," where XX are two digits of the serial number. The LCD will cycle through the serial number from the first two digits to the final two.

   For example, if the serial number is AE17A00022, the LCD display shows the following information one after another:

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

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

Asset Sensor Information

If there is any asset sensor connected to the PX, you can enter the Asset Sensor mode to show the asset tag state of each rack unit on the asset sensor. For the Raritan asset sensor, a rack unit refers to a tag port.

When there are no asset sensors connected, this mode is not available.

Below illustrates the asset sensor information.

Section	Example information
1	"1" refers to the asset sensor connected to the first FEATURE port.
2	This symbol ◇ indicates that you can switch between diverse rack units now by pressing the Up or Down button.
3	"30" indicates that the selected target is the 30th rack unit.
4	The word "MASTER" indicates the PX is the master device in a USB-cascading configuration. See ***Cascading the PX via USB*** (on page 29). *Note: For a standalone PX, this word is NOT displayed. For a slave device, it shows "SLAVE" instead.*
5	"ASSET" means that the LCD display enters the Asset Sensor mode.

To display the asset management information:

1. Press the MODE button until the PX enters the Asset Sensor mode, as indicated by "ASSET" to the right of the LCD.
2. By default the PX selects the asset sensor connected to the first FEATURE port so it shows "1" at the top. Because the PX has only one FEATURE port, "1" is the only option.

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

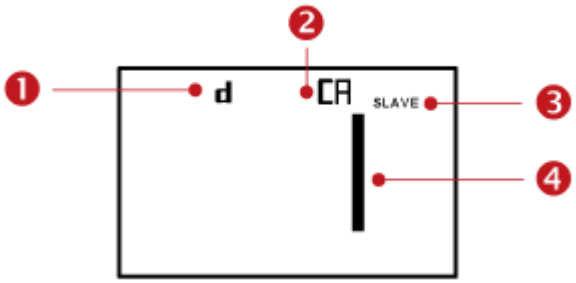
Note: Press and hold the Up or Down button for at least two (2) seconds to quickly move through several items at once.

- If the word "ALARM" appears below the rack unit number, it means no asset tag is physically connected to that rack unit.
- If the word "ALARM" does NOT appear, it means a connected asset tag is detected on the rack unit.

USB-Cascaded Device's Position

A cascaded device's position is available by operating the LCD display. For information on the USB-cascading configuration, see ***Cascading the PX via USB*** (on page 29).

Below illustrates a slave device's position.



Section	Example information
1	"d" means the LCD display has entered the Device mode.
2	"CA" indicates that the USB-cascading information is being displayed.
3	"SLAVE" indicates that this PX is a slave device. *Note: For a master device, it shows the word "MASTER" instead.*
4	The number 1 means the device position is Slave 1.

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

1. Press the MODE button to enter the Device mode, indicated by a 'd' in at the top left of the display.
2. Press the FUNC button until "CA" is displayed at the top right of the display.

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

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

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

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

RCM Information

If your PX3 phase I model supports residual current monitoring (RCM), this information is available in the front panel LCD display. For more information on RCM, see ***PX Models with Residual Current Monitoring*** (on page 587).

The front panel LCD display shows an alarm message when the RCM enters the critical state. Besides, you can operate the LCD display to check the RCM status.

This section introduces the RCM information shown on the LCD display of a PX3 *phase I* model only.

Note: For the RCM information shown on a PX3 phase II mode's LCD display, see **Front Panel Operations for RCM** *(on page 593).*

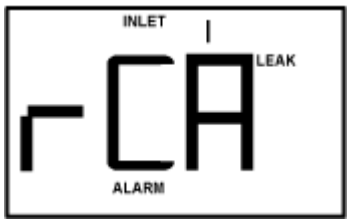
RCM alarm information in the critical state:

In the RCM critical state, the PDU beeps and the LCD display indicates the RCM critical state.

The RCM alarm information continues to display as long as RCM is in a critical state. The following RCM alarm messages are displayed one by one in the critical state.

```
rCA --> rCA --> Residual current value (mA)
```

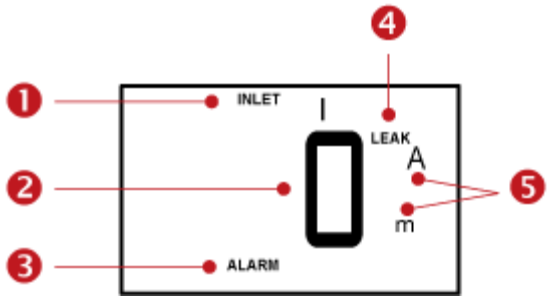
The diagram below illustrates the RCM alarm on the LCD display.



To display the RCM current:

1. Press the MODE button until the term "INLET" is displayed.
2. Verify the LCD is showing the inlet's current, which is indicated by the presence of the letter "A." If not, switch to current by pressing the FUNC button.
3. Depending on the type of your PX, the procedure to display the residual current slightly differs.
   - Single-phase PDU: Press the Up or Down button until the word "LEAK" displays.
   - 3-phase PDU: Press the Up button until the word "LEAK" displays.

Below illustrates the residual current information shown on the LCD display.



Section	Example information
❶	The inlet containing RCM sensor is INLET 1.
❷	This residual current is 0 mA.
❸	*ALARM* always displays for residual current sensor.
❹	*LEAK* always displays for residual current sensor.
❺	Measurement units are mA.

To run RCM self-test:

1. Press the MODE button until the LCD alternates between "SLF" and "tSt," which means **SELF TEST**.
2. Press the FUNC button to start RCM self-test.
3. The LCD shows dash symbols during RCM self-test.
4. Upon completion, RCM self-test results are displayed for 30 seconds, or until you press any button.
   - PAS: Self-test passed.
   - FAL: Self-test failed (the PX also beeps).

Below illustrates the RCM self-test mode.

Section	Example information
❶	The inlet containing RCM sensor is INLET 1.

Section	Example information
❷	The LCD alternates between "SLF" and "tSt" to indicate that this is self-test mode.
❸	*ALARM* always displays for residual current sensor.
❹	*LEAK* always displays for residual current sensor.

Note: To disable or enable this front panel function, see **Disabling or Enabling Front Panel RCM Self-Test** *(on page 593). By default, this function is enabled.*

Appendix I 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 PX

b. Create user groups for the PX on the AD server

c. Configure LDAP authentication on the PX device

d. Configure roles on the PX device

Important: Raritan disables SSL 3.0 and uses TLS for releases 3.0.4, 3.0.20 and later releases due to published security vulnerabilities in SSL 3.0. Make sure your network infrastructure, such as LDAP and mail services, uses TLS rather than SSL 3.0.

In This Chapter

Step A. Determine User Accounts and Roles 620
Step B. Configure User Groups on the AD Server.....621
Step C. Configure LDAP Authentication on the PX Device.....622
Step D. Configure Roles on the PX Device.....624

Step A. Determine User Accounts and Roles

Determine the user accounts and roles (groups) that are authenticated for accessing the PX. 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 PX on the AD server, and then make appropriate users members of these groups.

In this illustration, we assume:

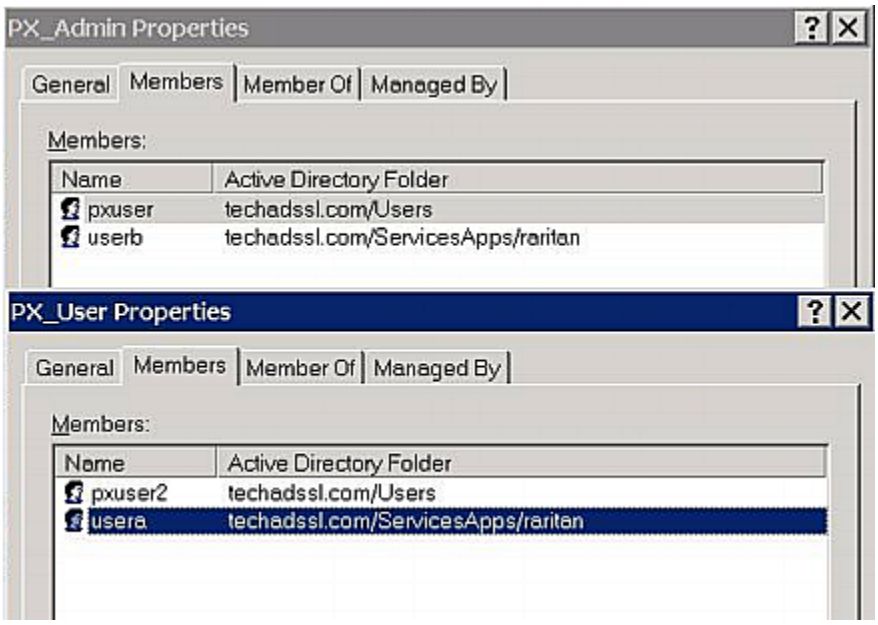
- The groups (roles) for the PX are named *PX_Admin* and *PX_User*.
- User accounts *pxuser*, *pxuser2*, *usera* and *userb* already exist on the AD server.

To configure user groups on the AD server:

1. On the AD server, create new groups -- *PX_Admin* and *PX_User*.

   Note: See 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.



Step C. Configure LDAP Authentication on the PX Device

You must enable and set up LDAP authentication properly on the PX device to use external authentication.

In the illustration, we assume:

- The DNS server settings have been configured properly. See ***Modifying Network Settings*** (on page 134) and ***Role of a DNS Server*** (on page 140).
- The AD server's domain name is *techadssl.com*, and its IP address is *192.168.56.3*.
- The AD protocol is NOT encrypted over TLS.
- The AD server uses the default TCP port *389*.
- Anonymous bind is used.

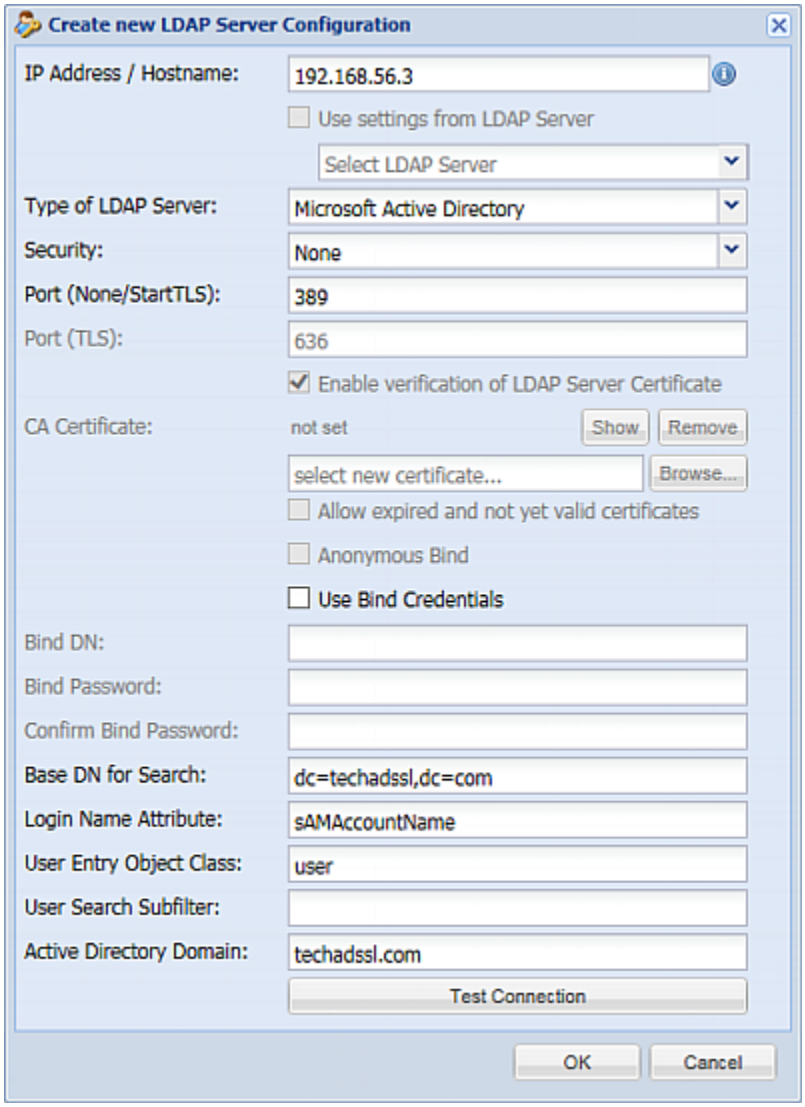
To configure LDAP authentication:

1. Choose Device Settings > Security > Authentication. The Authentication Settings dialog appears.
2. Select the LDAP radio button to activate the LDAP/LDAPS authentication.
3. Click New to add an LDAP/LDAPS AA server. The "Create new LDAP Server Configuration" dialog appears.
4. Provide the PX with the information about the AD server.
   - IP Address / Hostname - Type the domain name `techadssl.com` or IP address `192.168.56.3`.

   Important: Without the TLS encryption enabled, you can type either the domain name or IP address in this field, but you must type the fully qualified domain name if the TLS encryption is enabled.

   - Use settings from LDAP server - Leave the checkbox deselected.
   - Type of LDAP Server - Select "Microsoft Active Directory" from the drop-down list.
   - Security - Select "None" since the TLS encryption is not applied in this example.
   - Port (None/StartTLS) - Ensure the field is set to 389.
   - Port (TLS) and CA Certificate - Skip the two fields since the TLS encryption is not enabled.
   - Use Bind Credentials - Do NOT select this checkbox because anonymous bind is used.
   - Bind DN, Bind Password and Confirm Bind Password -- Skip the three fields because anonymous bind is used.

- Base DN for Search - Type `dc=techadssl,dc=com` as the starting point where your search begins on the AD server.
- Login Name Attribute - Ensure the field is set to `sAMAccountName` because the LDAP server is Microsoft Active Directory.
- User Entry Object Class - Ensure the field is set to `user` because the LDAP server is Microsoft Active Directory.
- User Search Subfilter - The field is optional. The subfilter information is also useful for filtering out additional objects in a large directory structure. In this example, we leave it blank.
- Active Directory Domain - Type `techadssl.com`.



5. Click OK. The LDAP server is saved.

6. Click OK. The LDAP authentication is activated.

Note: If the PX 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 PX and the LDAP server to use the same NTP server(s).

Step D. Configure Roles on the PX Device

A role on the PX device determines the system and outlet permissions. You must create the roles whose names are identical to the user groups created for the PX 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 PX nor access the outlets.
- Users assigned to the *PX_Admin* role have the Administrator permissions so they can both configure PX and access the outlets.

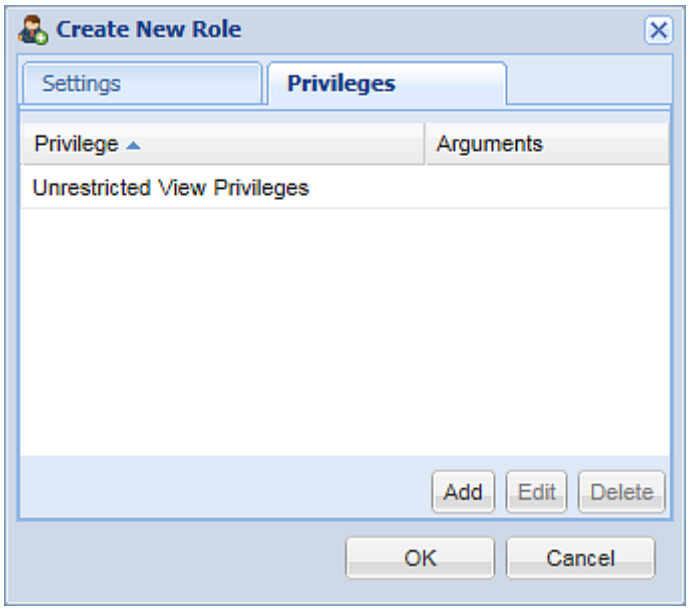
To create the PX_User role with appropriate permissions assigned:

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

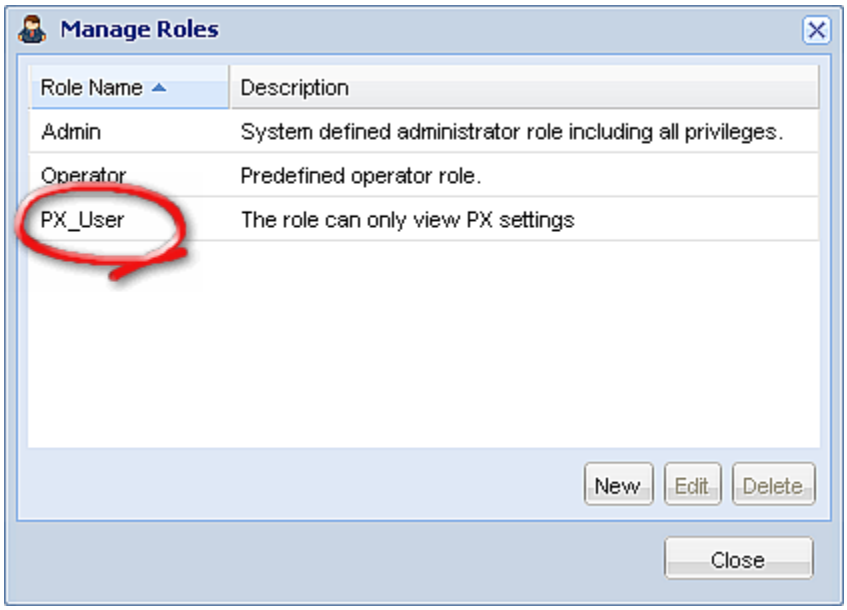
   Tip: You can also access the Manage Roles dialog by clicking the Manage Roles button in the Edit User 'XXX' dialog.

2. Click New. The Create New Role dialog appears.
3. Type `PX_User` in the Role Name field.
4. Type a description for the PX_User role in the Description field. In this example, we type "The role can only view PX settings" to describe the role.
5. Click the Privileges tab to select "Unrestricted View Privileges," which includes all View permissions. The "Unrestricted View Privileges" permission lets users view all settings without the capability to configure or change them.
   a. Click Add. The "Add Privileges to new Role" dialog appears.
   b. Select the permission "Unrestricted View Privileges" from the Privileges list.

c. Click Add.



6. Click OK. The PX_User role is created.

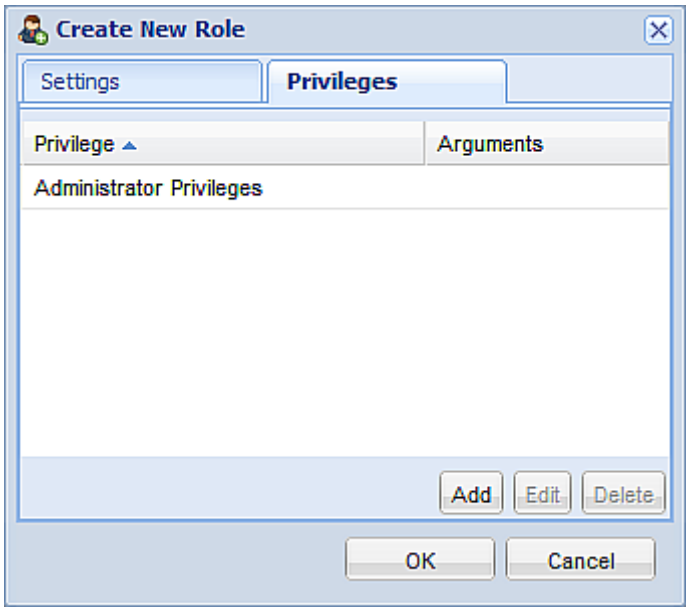


7. Keep the Manage Roles dialog opened to create the PX_Admin role.

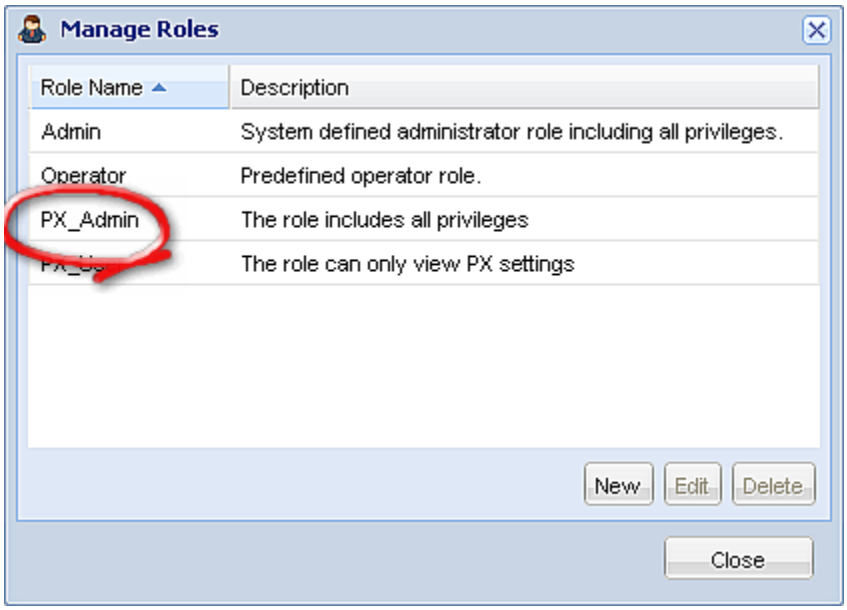
To create the PX_Admin role with full permissions assigned:

1. Click New. The Create New Role dialog appears.
2. Type `PX_Admin` in the Role Name field.

3. Type a description for the PX_Admin role in the Description field. In this example, we type "The role includes all privileges" to describe the role.
4. Click the Privileges tab to select the Administrator permission. The Administrator permission allows users to configure or change all PX settings.
   a. Click Add. The "Add Privileges to new Role" dialog appears.
   b. Select the permission named Administrator Privileges from the Privileges list.
   c. Click Add.



5. Click OK. The PX_Admin role is created.



6. Click Close to quit the dialog.

Appendix J Updating the LDAP Schema

In This Chapter

Returning User Group Information 628
Setting the Registry to Permit Write Operations to the Schema 629
Creating a New Attribute 629
Adding Attributes to the Class 630
Updating the Schema Cache.....632
Editing rciusergroup Attributes for User Members 632

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 PX determines the permissions for a given user based on the permissions of the user's role. Your remote LDAP server can provide these user role names by returning an attribute named as follows:

rciusergroup attribute type: string

This may require a schema extension on your LDAP/LDAPS server. Consult your authentication server administrator to enable this attribute.

In addition, for Microsoft® Active Directory®, the standard LDAP memberOf is used.

From Microsoft Active Directory

Note: This should be attempted only by an experienced Active Directory® administrator.

Returning user role information from Microsoft's® Active Directory for Windows 2000® operating system server requires updating the LDAP/LDAPS schema. See your Microsoft documentation for details.

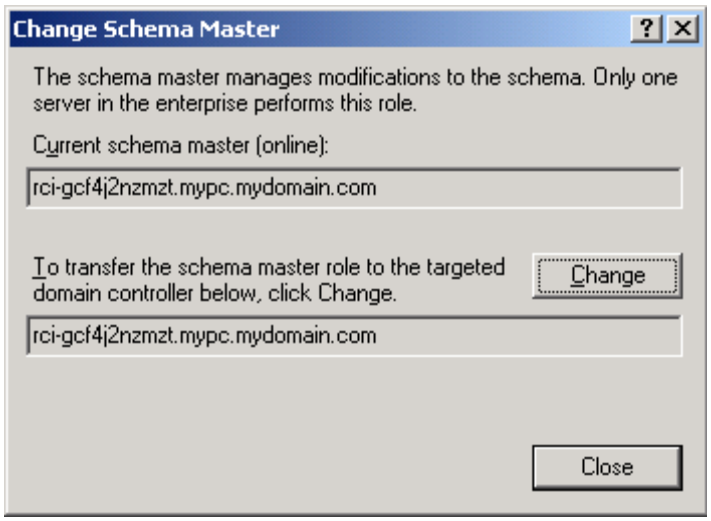
1. Install the schema plug-in for Active Directory. See Microsoft Active Directory documentation for instructions.
2. Run Active Directory Console and select Active Directory Schema.

Setting the Registry to Permit Write Operations to the Schema

To allow a domain controller to write to the schema, you must set a registry entry that permits schema updates.

To permit write operations to the schema:

1. Right-click the Active Directory® Schema root node in the left pane of the window and then click Operations Master. The Change Schema Master dialog appears.



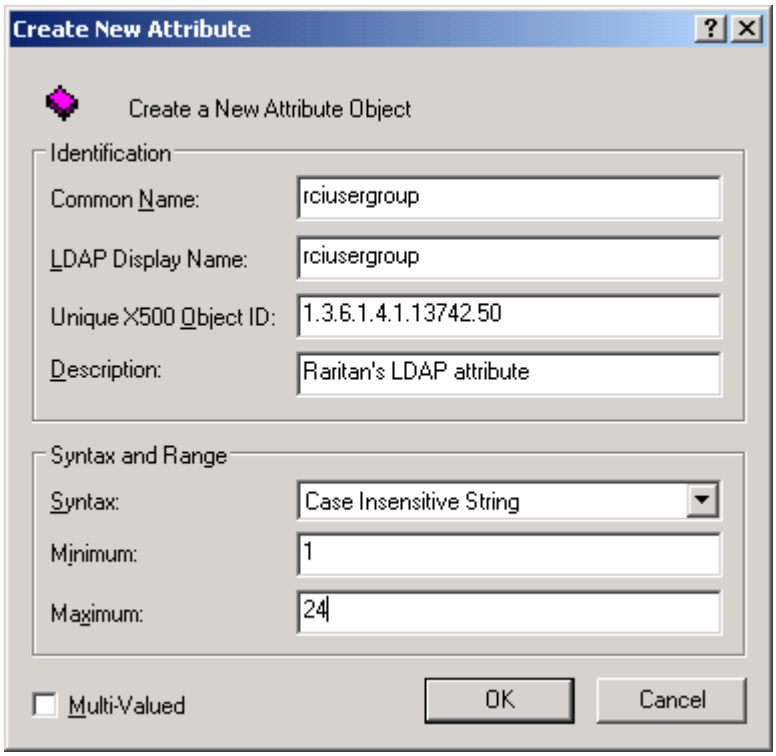
2. Select the "Schema can be modified on this Domain Controller" checkbox. **Optional**
3. Click OK.

Creating a New Attribute

To create new attributes for the rciusergroup class:

1. Click the + symbol before Active Directory® Schema in the left pane of the window.
2. Right-click Attributes in the left pane.

3. Click New and then choose Attribute. When the warning message appears, click Continue and the Create New Attribute dialog appears.



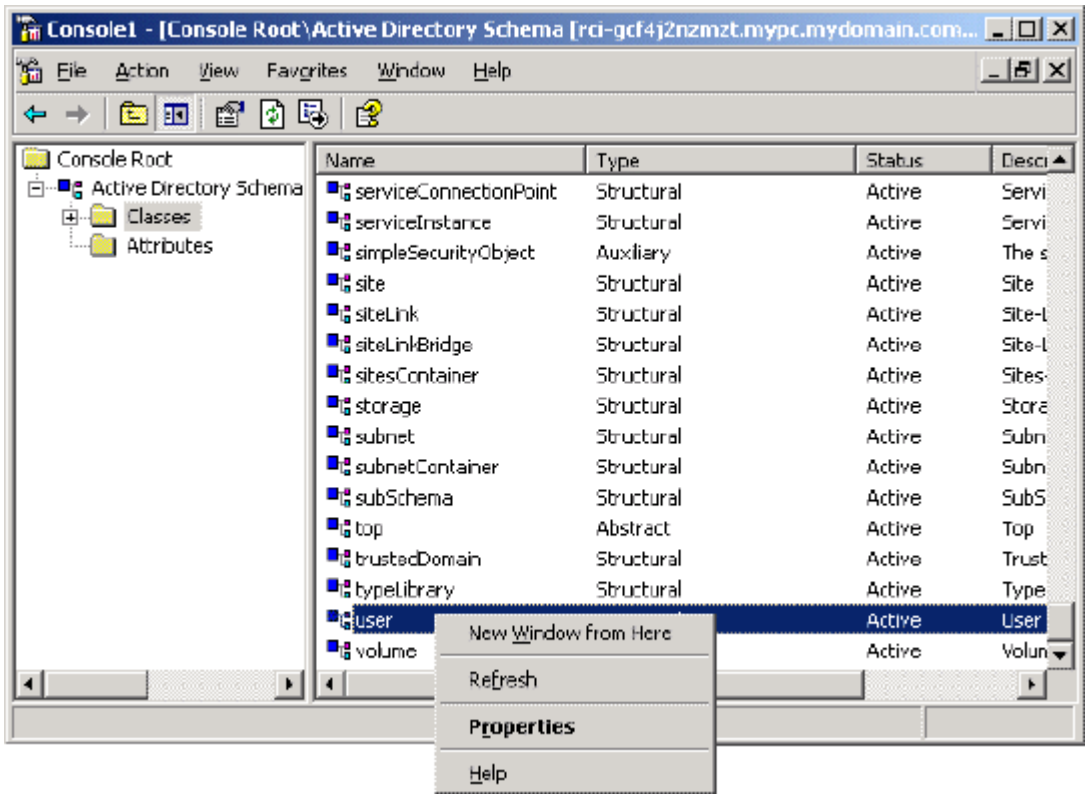
4. Type *rciusergroup* in the Common Name field.
5. Type *rciusergroup* in the LDAP Display Name field.
6. Type *1.3.6.1.4.1.13742.50* in the Unique x5000 Object ID field.
7. Type a meaningful description in the Description field.
8. Click the Syntax drop-down arrow and choose Case Insensitive String from the list.
9. Type *1* in the Minimum field.
10. Type *24* in the Maximum field.
11. Click OK to create the new attribute.

Adding Attributes to the Class

To add attributes to the class:

1. Click Classes in the left pane of the window.

2. Scroll to the user class in the right pane and right-click it.



3. Choose Properties from the menu. The user Properties dialog appears.
4. Click the Attributes tab to open it.
5. Click Add.

6. Choose rciusergroup from the Select Schema Object list.

7. Click OK in the Select Schema Object dialog.
8. Click OK in the User Properties dialog.

Updating the Schema Cache

To update the schema cache:

1. Right-click Active Directory® Schema in the left pane of the window and select Reload the Schema.
2. Minimize the Active Directory Schema MMC (Microsoft® Management Console) console.

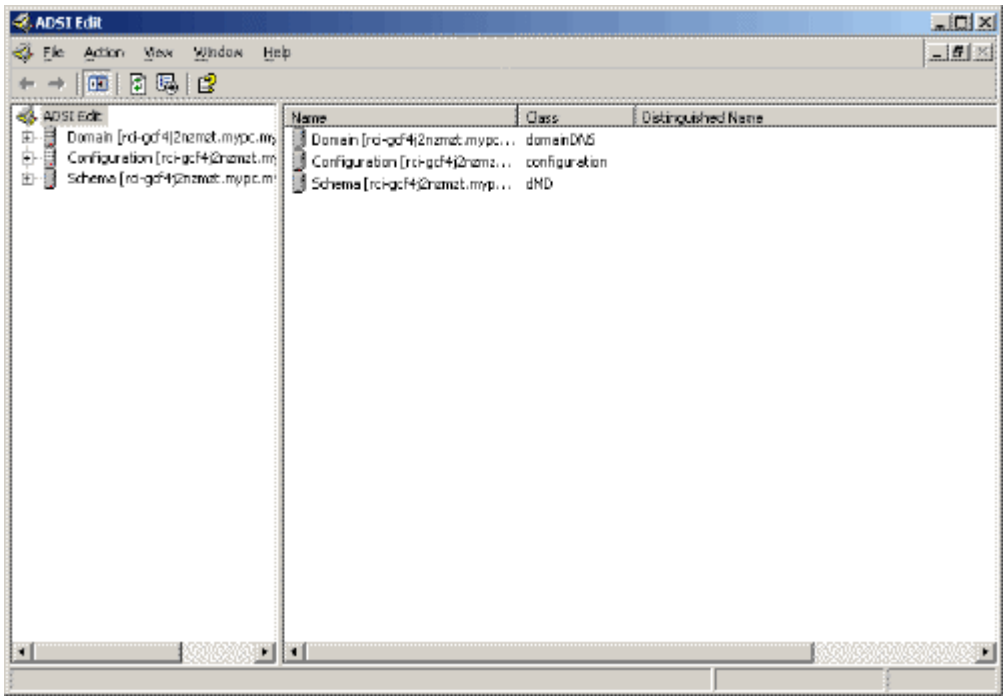
Editing rciusergroup Attributes for User Members

To run the Active Directory® script on a Windows 2003® server, use the script provided by Microsoft® (available on the Windows 2003 server installation CD). These scripts are loaded onto your system with a Microsoft® Windows 2003 installation. ADSI (Active Directory Service Interface) acts as a low-level editor for Active Directory, allowing you to perform common administrative tasks such as adding, deleting, and moving objects with a directory service.

To edit the individual user attributes within the group rciusergroup:

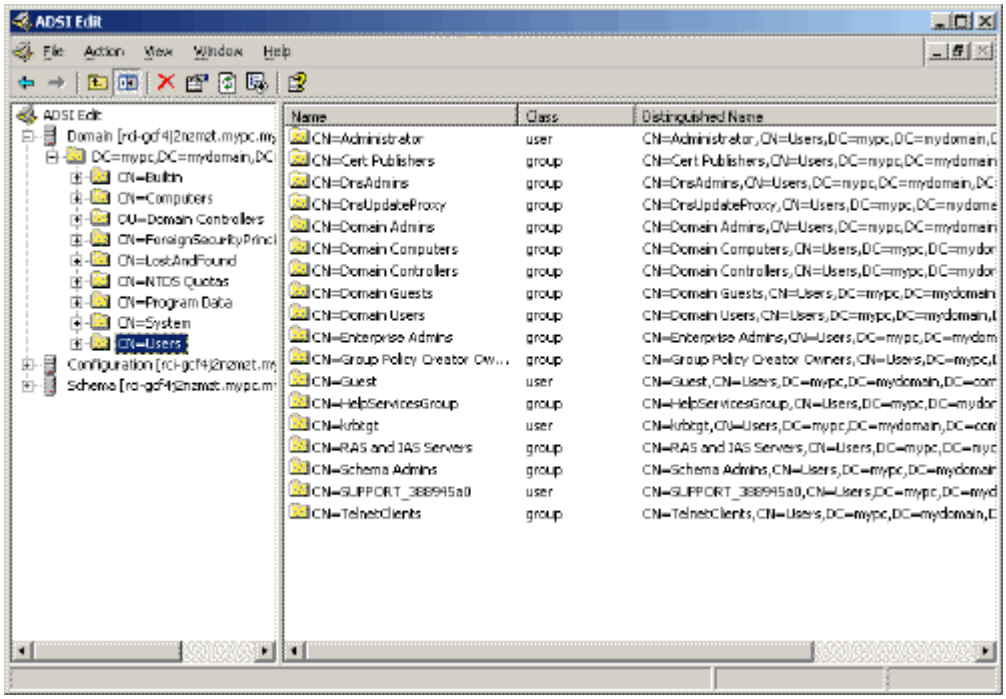
1. From the installation CD, choose Support > Tools.
2. Double-click SUPTOOLS.MSI to install the support tools.

3. Go to the directory where the support tools were installed. Run adsiedit.msc. The ADSI Edit window opens.

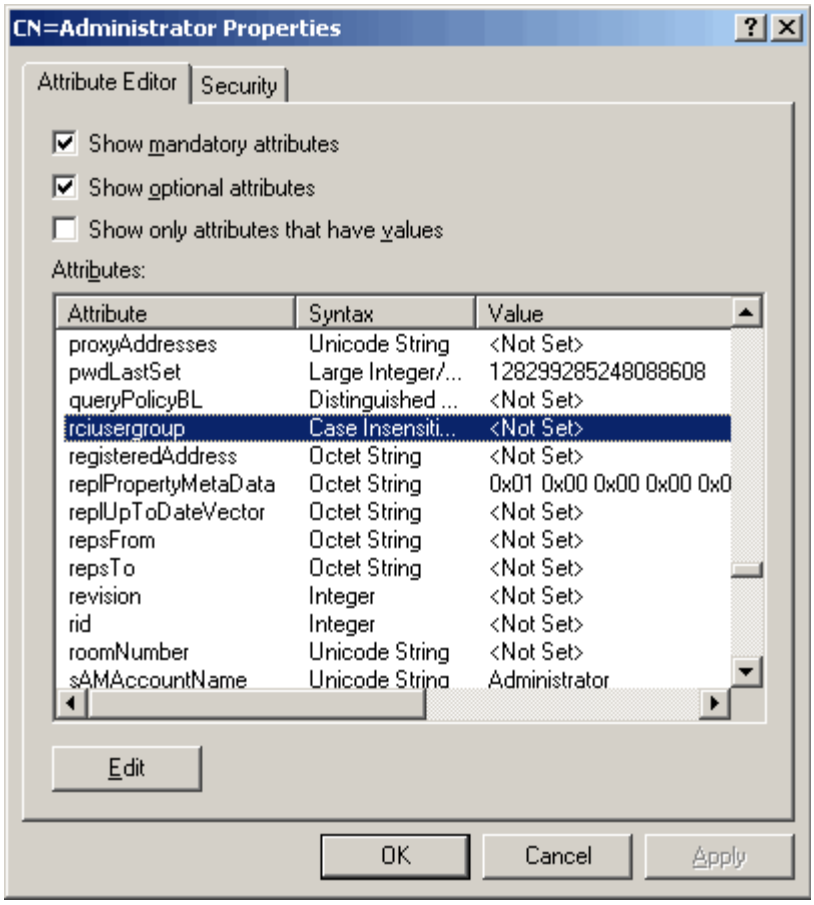


4. Open the Domain.

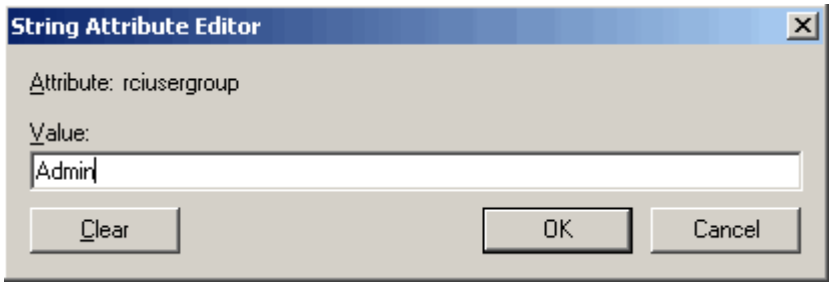
5. In the left pane of the window, select the CN=Users folder.



6. Locate the user name whose properties you want to adjust in the right pane. Right-click the user name and select Properties.
7. Click the Attribute Editor tab if it is not already open. Choose rciusergroup from the Attributes list.



8. Click Edit. The String Attribute Editor dialog appears.
9. Type the user role (created in the PX) in the Edit Attribute field. Click OK.



Appendix K RADIUS Configuration Illustration

This section provides illustrations for configuring RADIUS authentication. One illustration is based on the Microsoft® Network Policy Server (NPS), and the other is based on a non-Windows RADIUS server, such as FreeRADIUS.

The following steps are required for any RADIUS authentication:

1. Configure RADIUS authentication on the PX device. See ***Adding RADIUS Server Settings*** (on page 203).
2. Configure roles on the PX device. See ***Creating a Role*** (on page 174).
3. Configure your RADIUS server. See ***Microsoft Network Policy Server*** (on page 635) or ***Non-Windows RADIUS Server*** (on page 659).

In This Chapter

Microsoft Network Policy Server 635
Non-Windows RADIUS Server 659

Microsoft Network Policy Server

In this Microsoft NPS illustration, we assume that the NPS is running on the Windows 2008 system.

Three major steps are required for configuring Windows 2008 NPS:

a. Add your PX device to NPS as a RADIUS client

b. Configure connection request policies on NPS

c. Configure a vendor-specific attribute on NPS

Some configuration associated with Microsoft Active Directory (AD) is also required for RADIUS authentication. See ***AD-Related Configuration*** (on page 656).

Step A: Add Your PX as a RADIUS Client

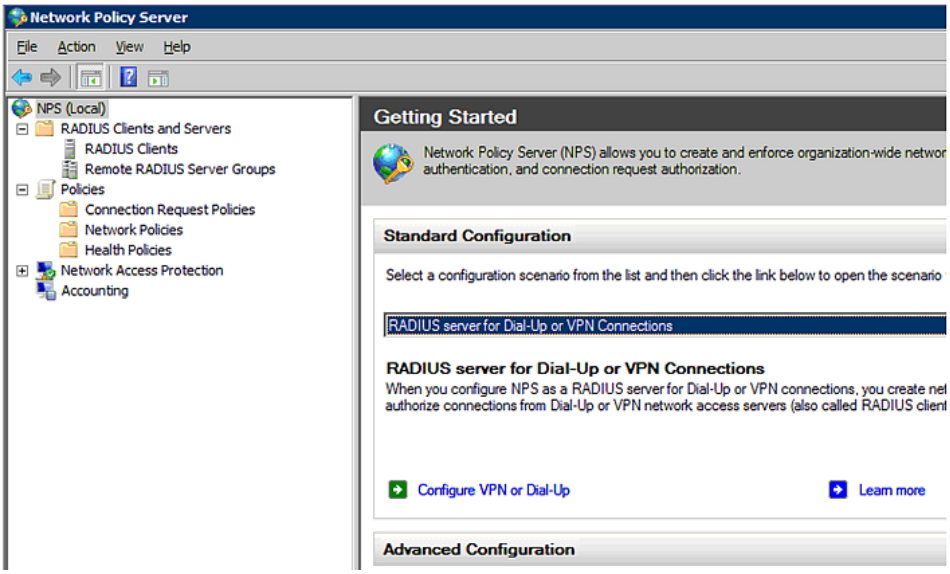
The RADIUS implementation on a PX follows the standard RADIUS Internet Engineering Task Force (IETF) specification so you must select "RADIUS Standard" as its vendor name when configuring the NPS server.

In this illustratrion, we assume:

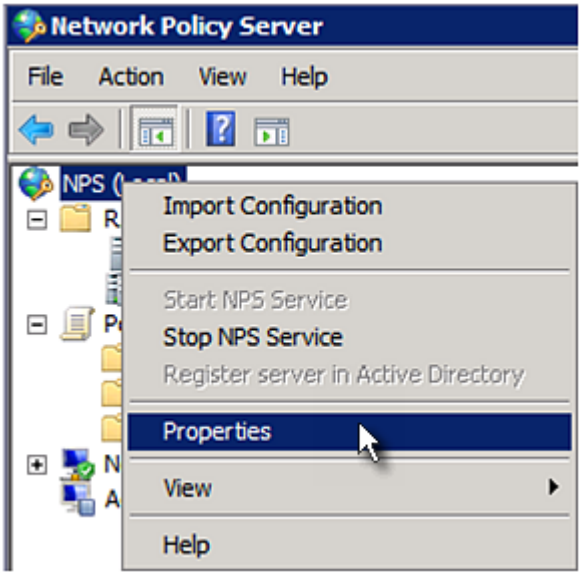
- IP address of your PX: *192.168.56.29*
- RADIUS authentication port specified for PX: *1812*
- RADIUS accounting port specified for PX: *1813*

To add your PX to the RADIUS NPS:

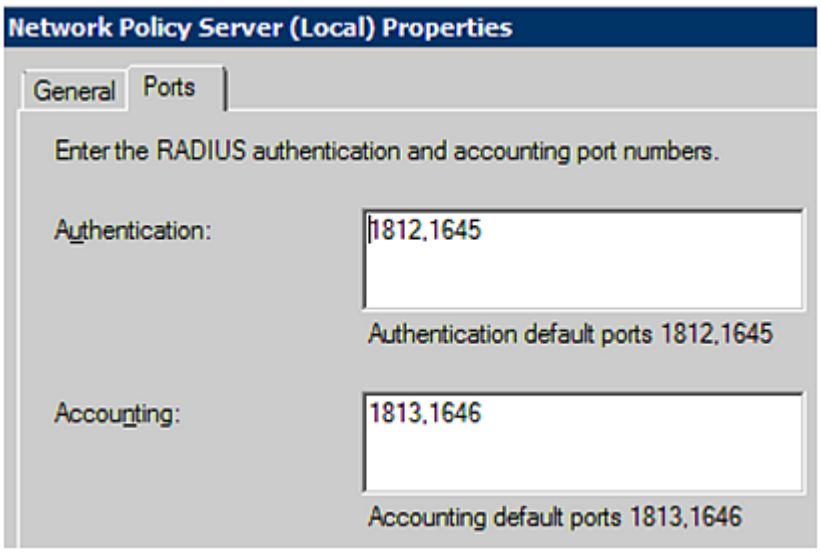
1. Choose Start > Administrative Tools > Network Policy Server. The Network Policy Server console window opens.



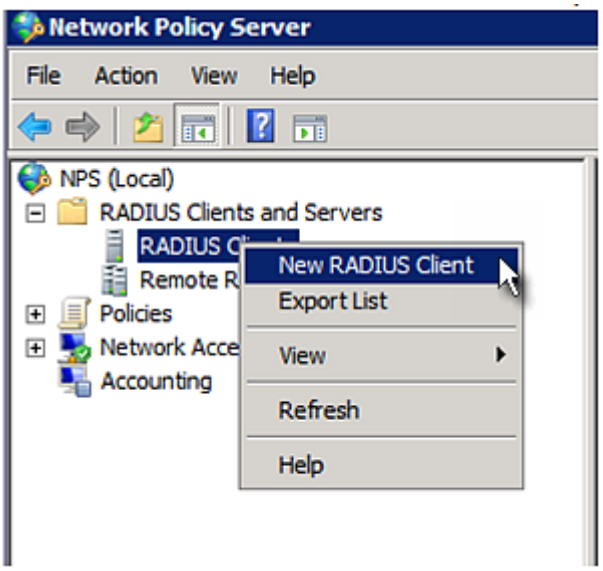
2. Right-click NPS (Local), and select Properties.



Verify the authentication and accounting port numbers shown in the properties dialog are the same as those specified on your PX. In this example, they are 1812 and 1813. Then close this dialog.

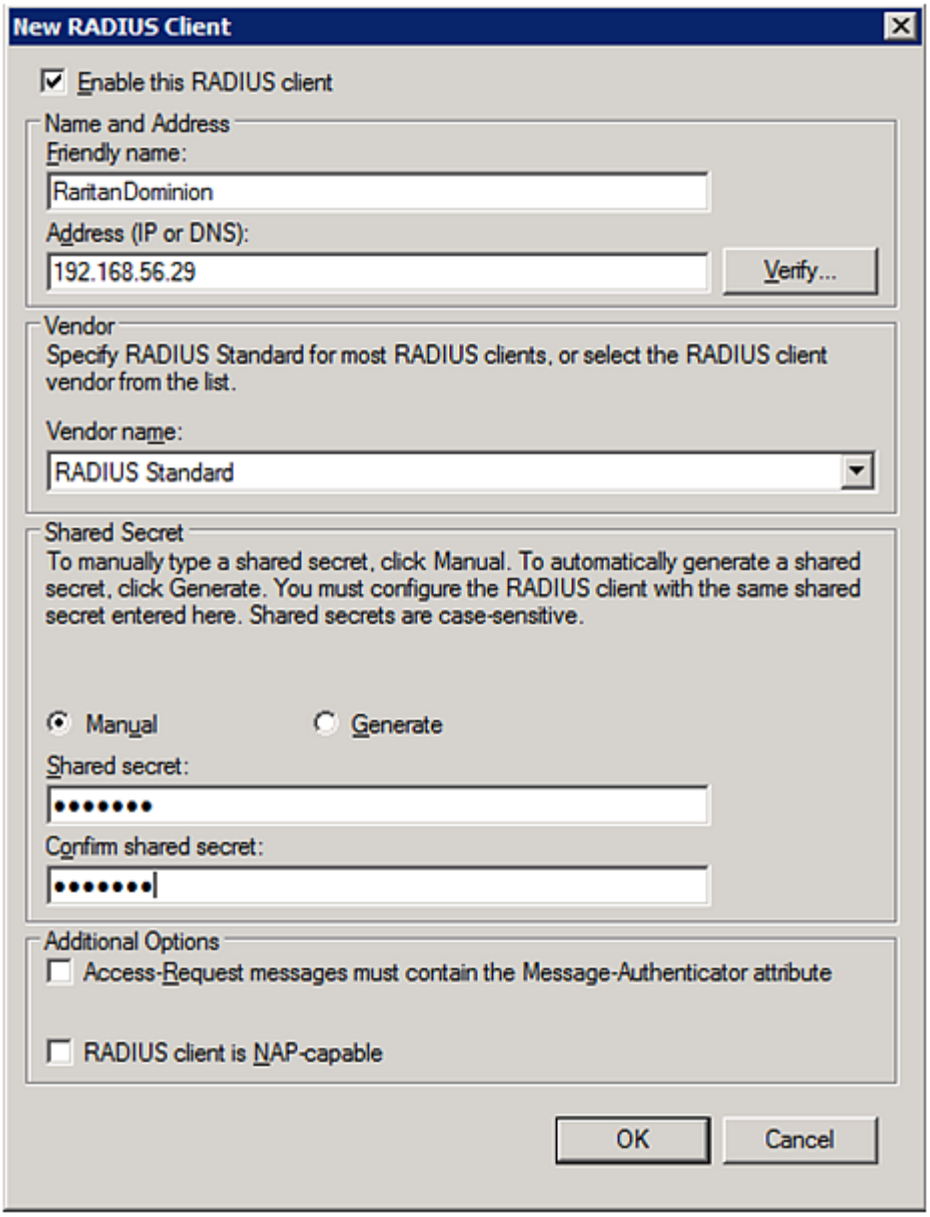


3. Under "RADIUS Clients and Servers," right-click RADIUS Client and select New RADIUS Client. The New RADIUS Client dialog appears.



4. Do the following to add your PX to NPS:
   a. Verify the "Enable this RADIUS client" checkbox is selected.
   b. Type a name for identifying your PX 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 PX.



5. Click OK.

Step B: Configure Connection Request Policies

You need to configure the following for connection request policies:

a. IP address or host name of the PX

b. Connection request forwarding method

c. Authentication method(s)

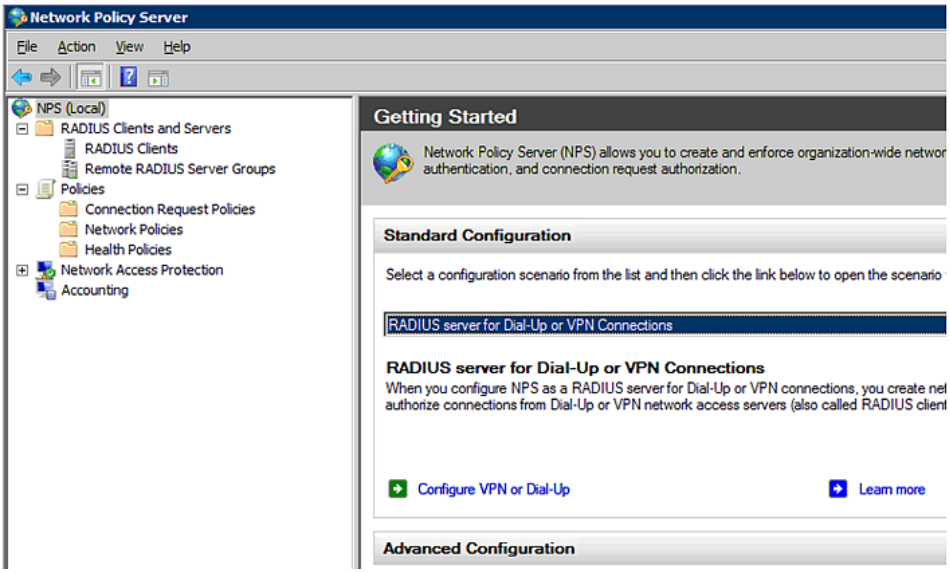
d. Standard RADIUS attributes

In the following illustration, we assume:

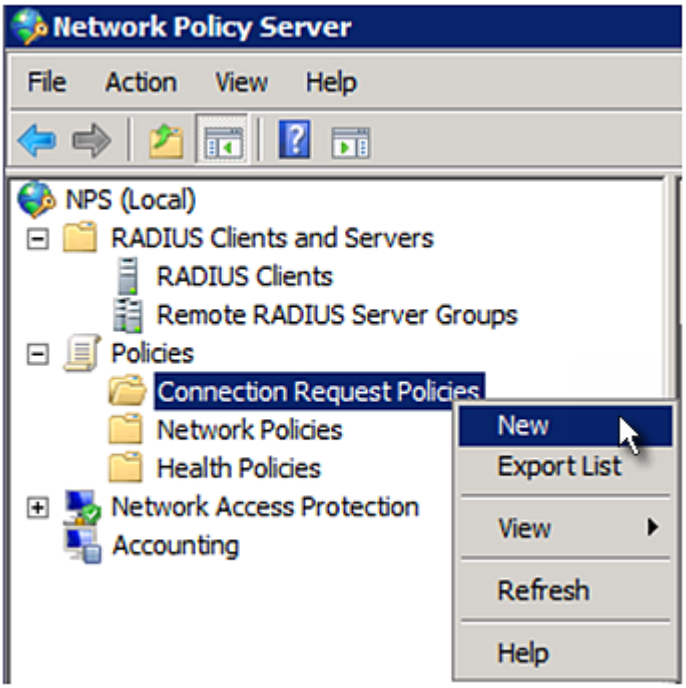
- *Local* NPS server is used
- IP address of your PX: *192.168.56.29*
- RADIUS protocol selected on your PX: *CHAP*
- Existing role of your PX: *Admin*

To configure connection request policies:

1. Open the NPS console, and expand the Policies folder.

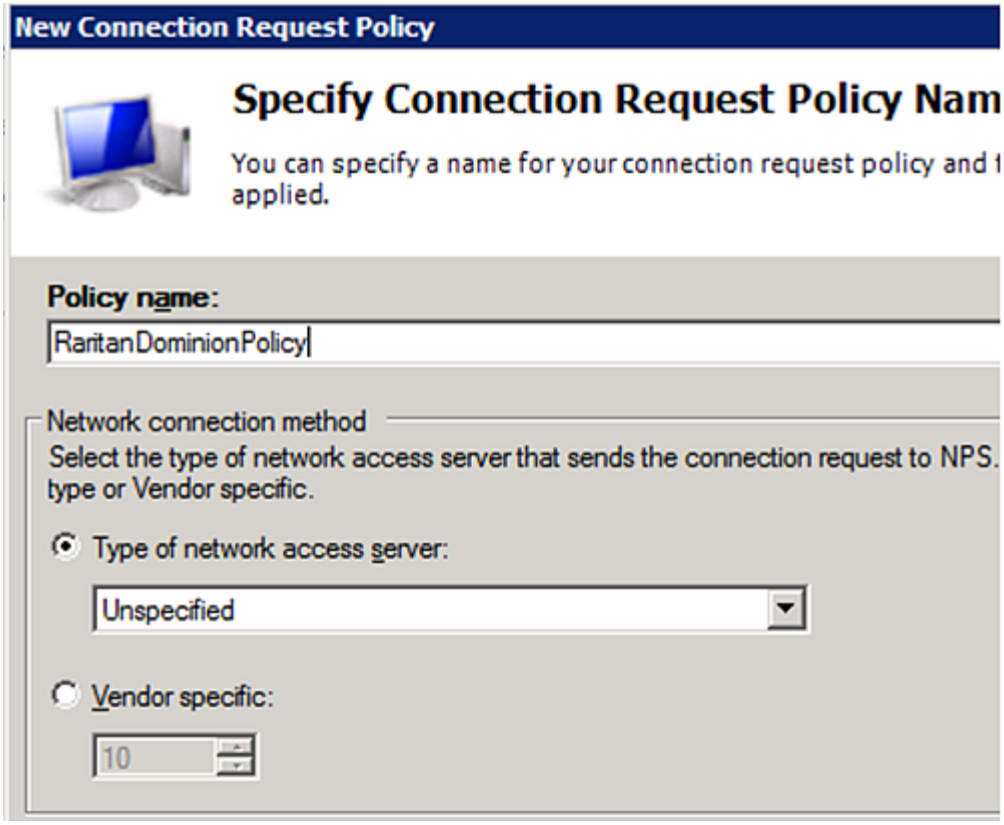


2. Right-click Connection Request Policies and select New. The New Connection Request Policy dialog appears.

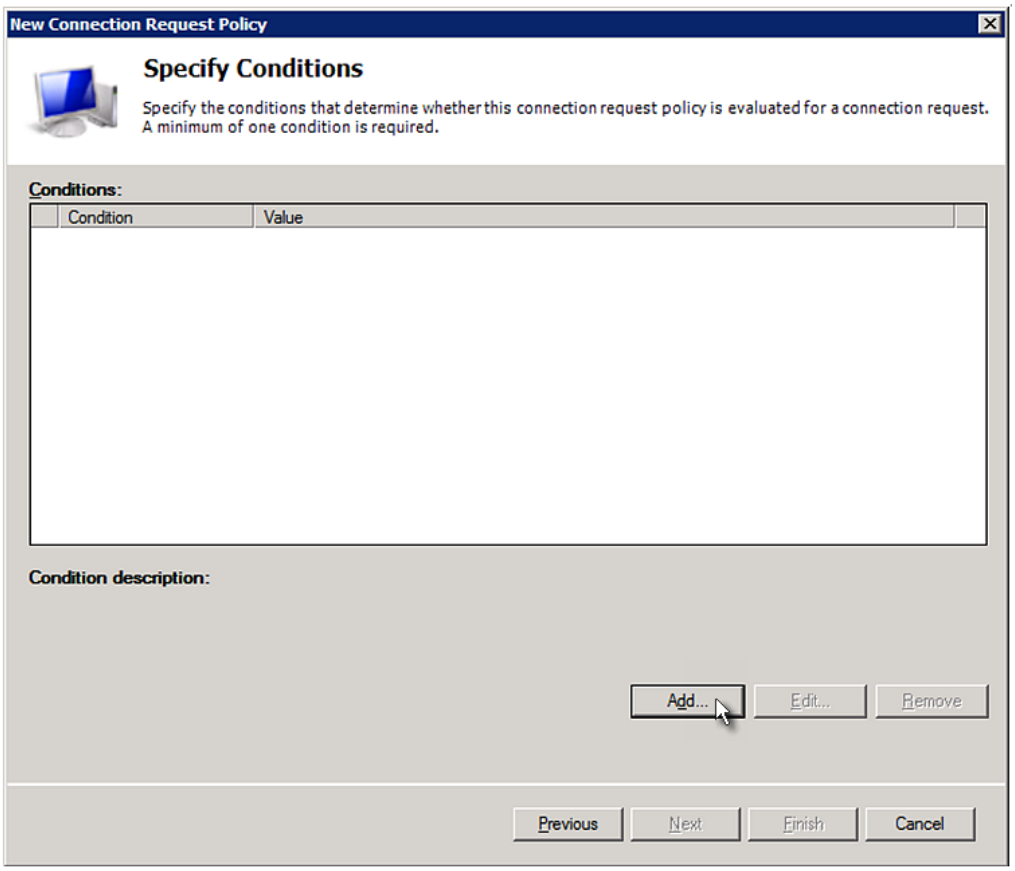


3. Type a descriptive name for identifying this policy in the "Policy name" field.

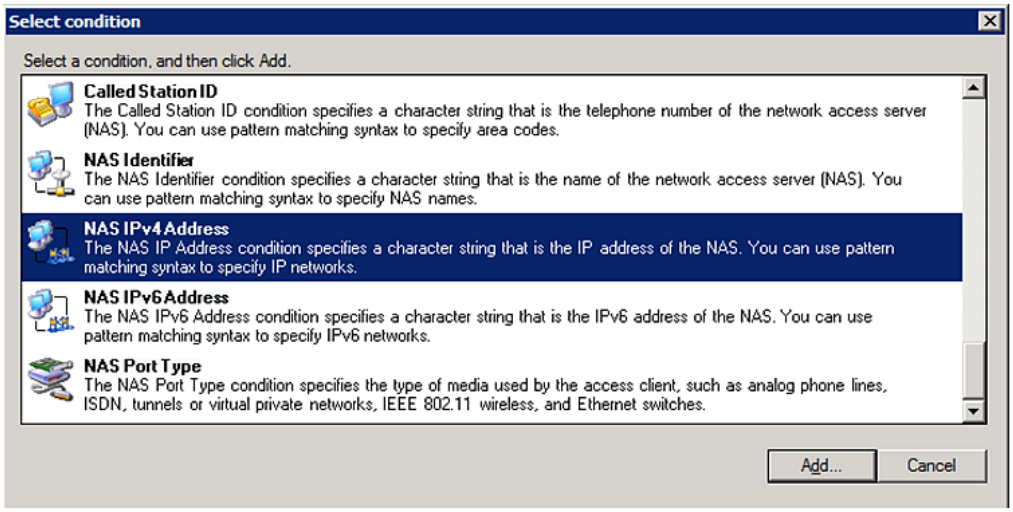
- You can leave the "Type of network access server" field to the default -- Unspecified.



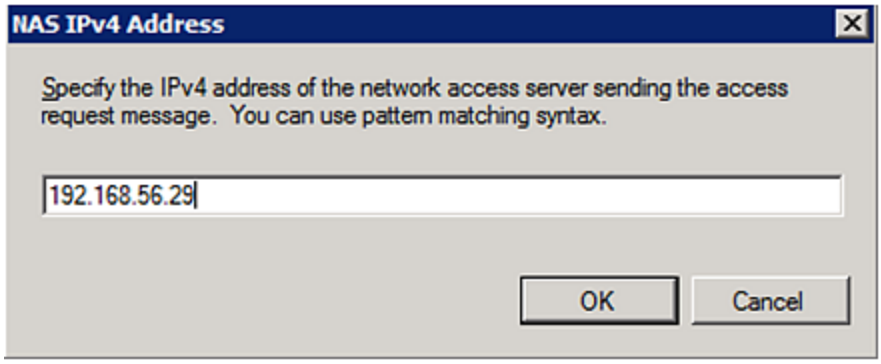
4. Click Next to show the "Specify Conditions" screen. Click Add.



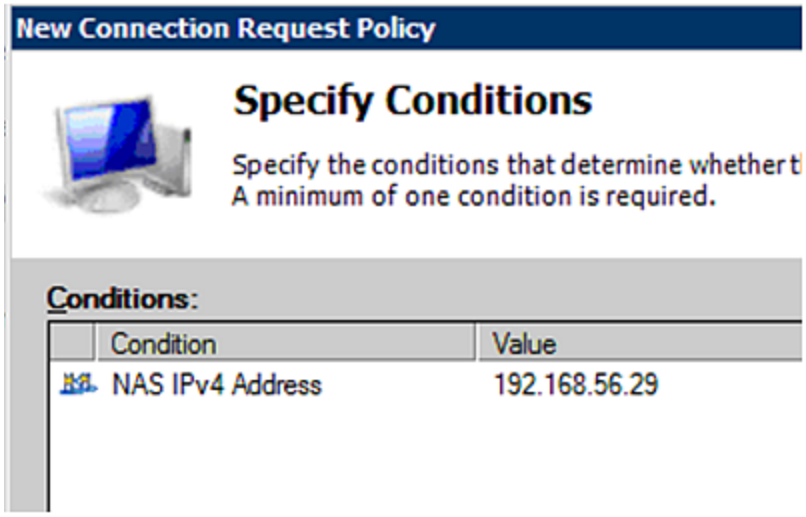
5. The "Select condition" dialog appears. Click Add.



6. The NAS IPv4 Address dialog appears. Type the PX IP address -- *192.168.56.29*, and click OK.

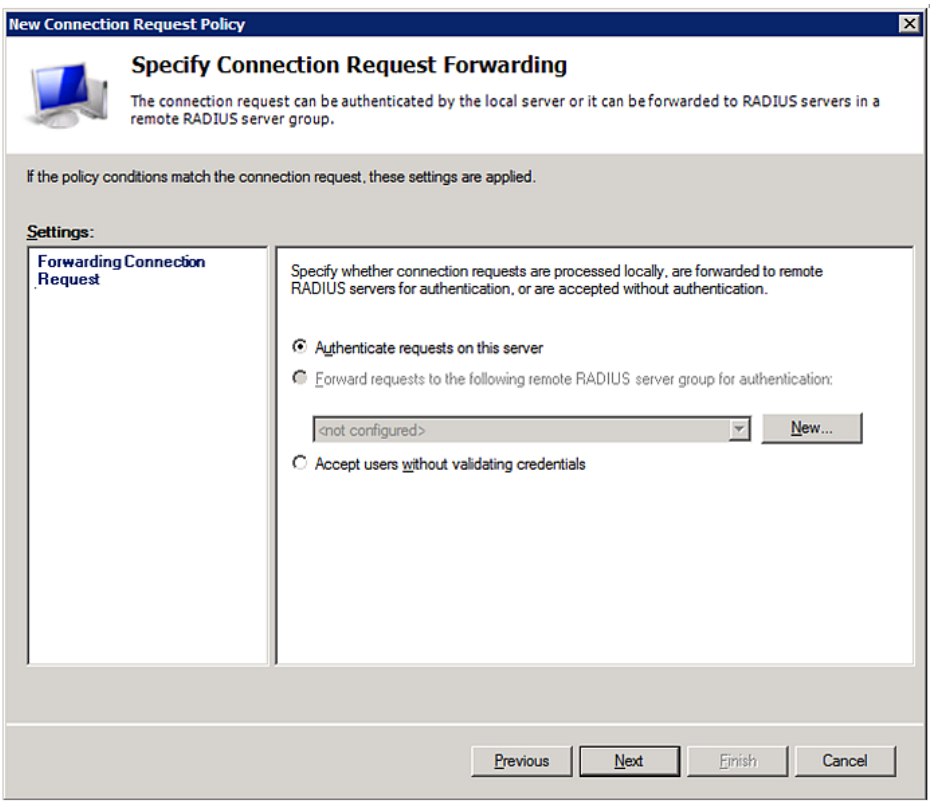


7. Click Next in the New Connection Request Policy dialog.



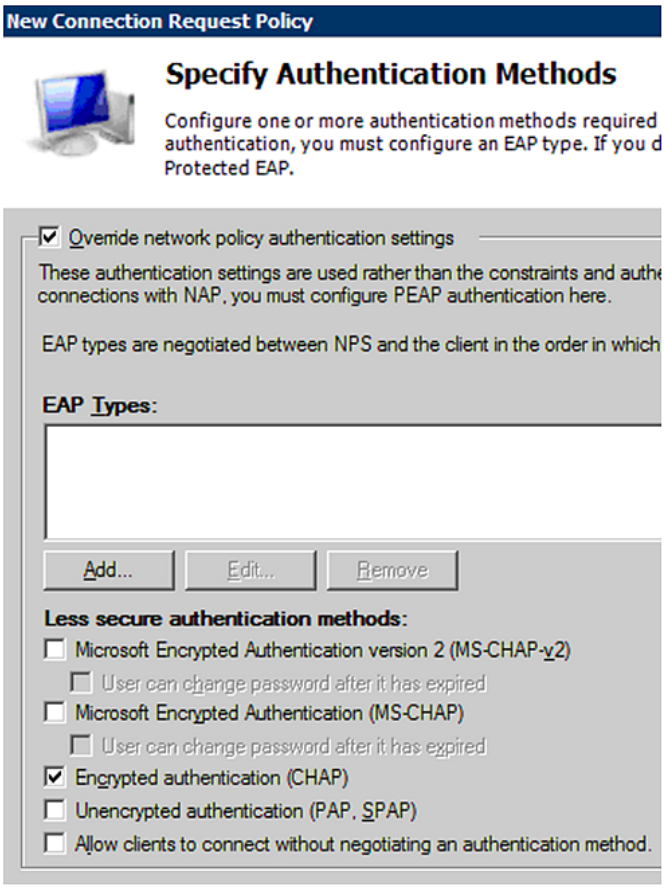
8. Select "Authenticate requests on this server" because a local NPS server is used in this example. Then click Next.

Note: Connection Request Forwarding options must match your environment.

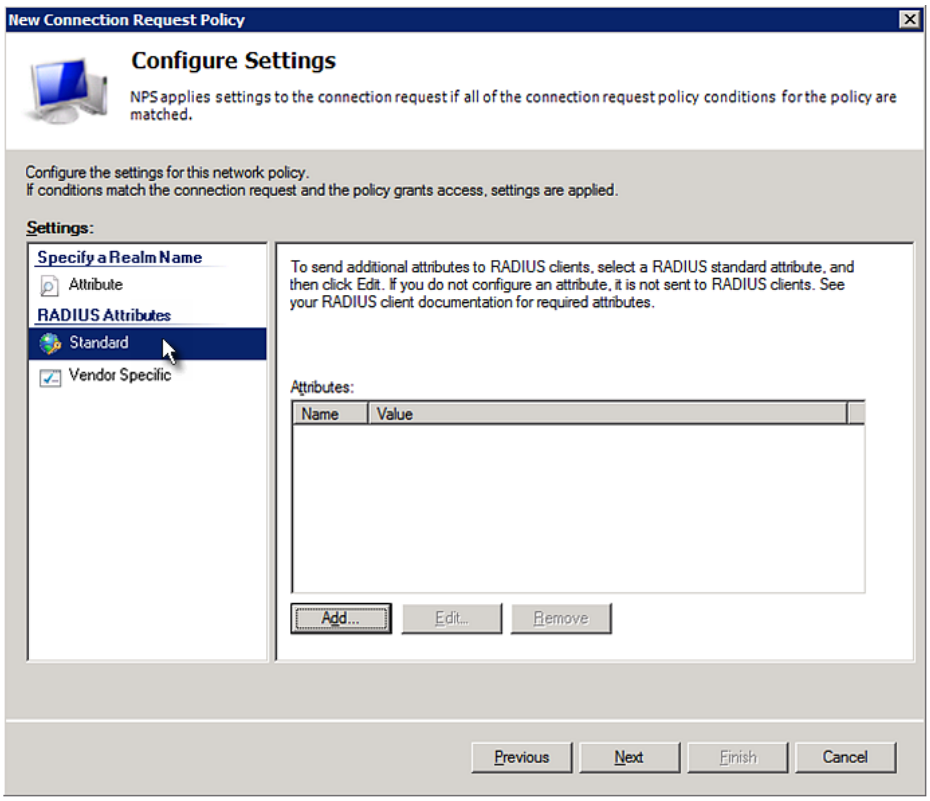


9. When the system prompts you to select the authentication method, select the following two options:
   - Override network policy authentication settings
   - CHAP -- the PX uses "CHAP" in this example

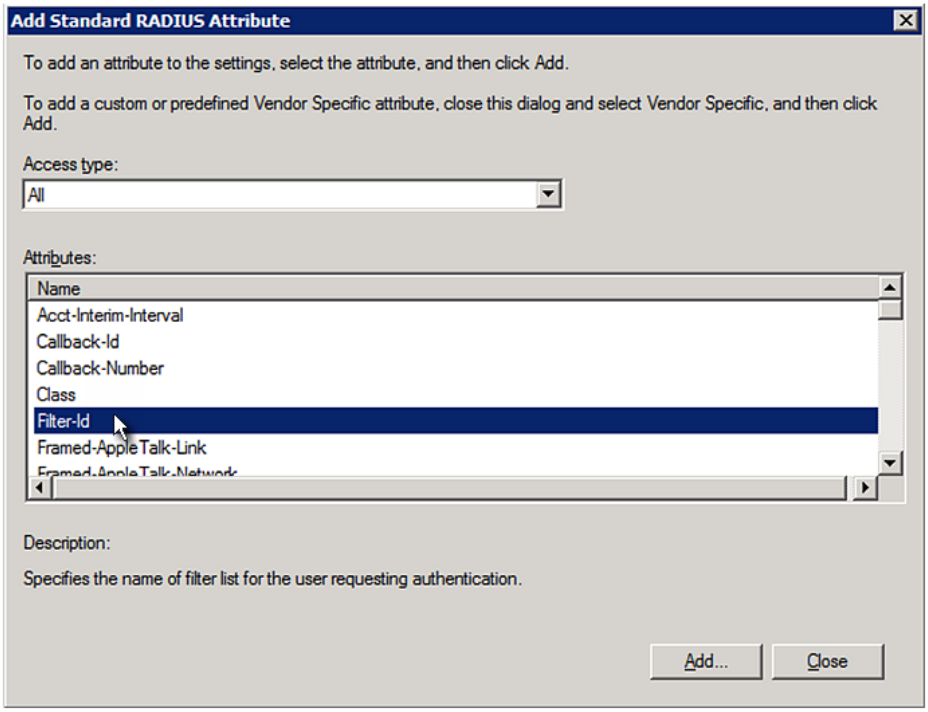
Note: If your PX uses PAP, then select "PAP."



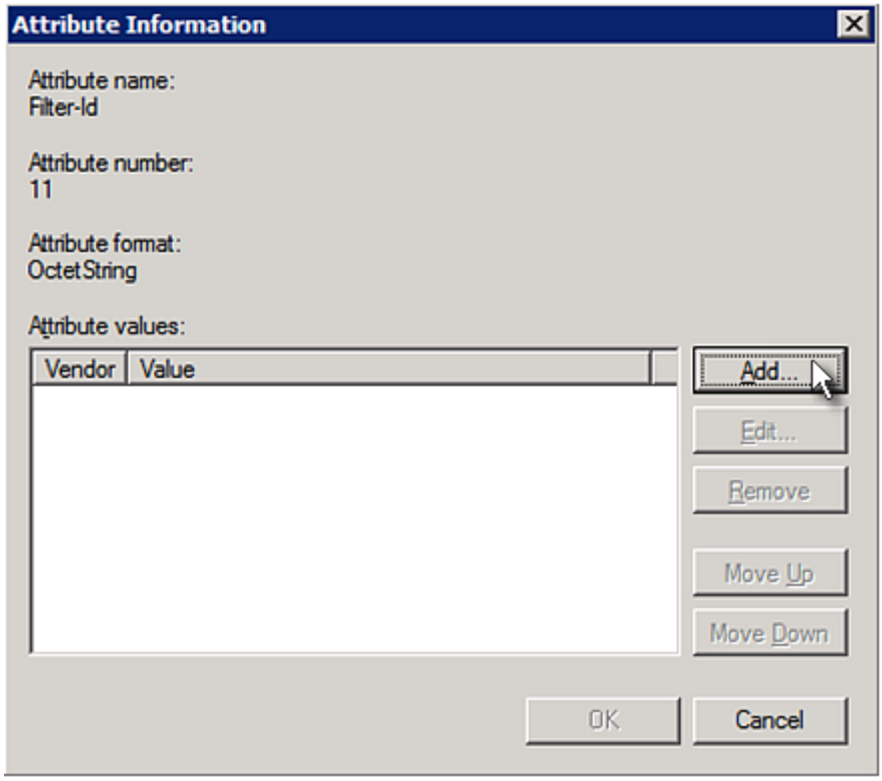
10. Select Standard to the left of the dialog and then click Add.



11. Select Filter-Id from the list of attributes and click Add.

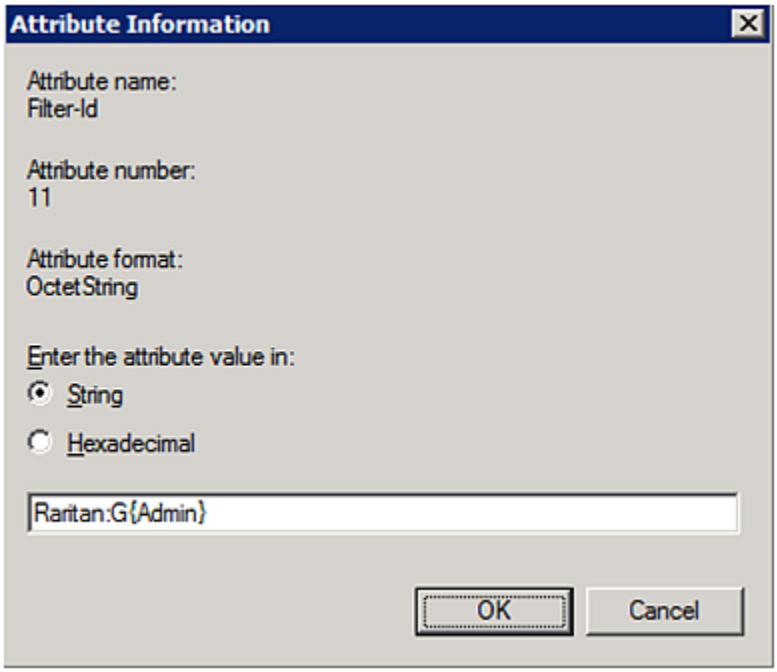


12. In the Attribute Information dialog, click Add.

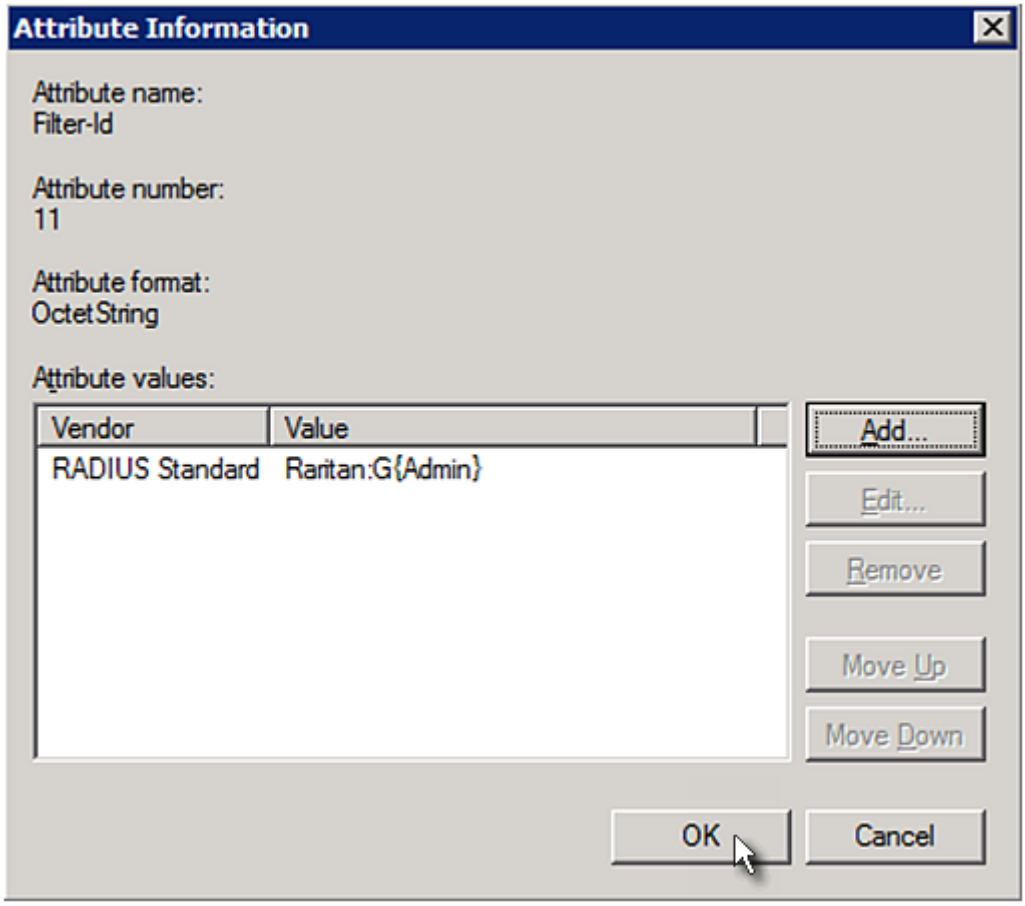


13. Select String, type *Raritan:G{Admin}* in the text box, and then click OK.

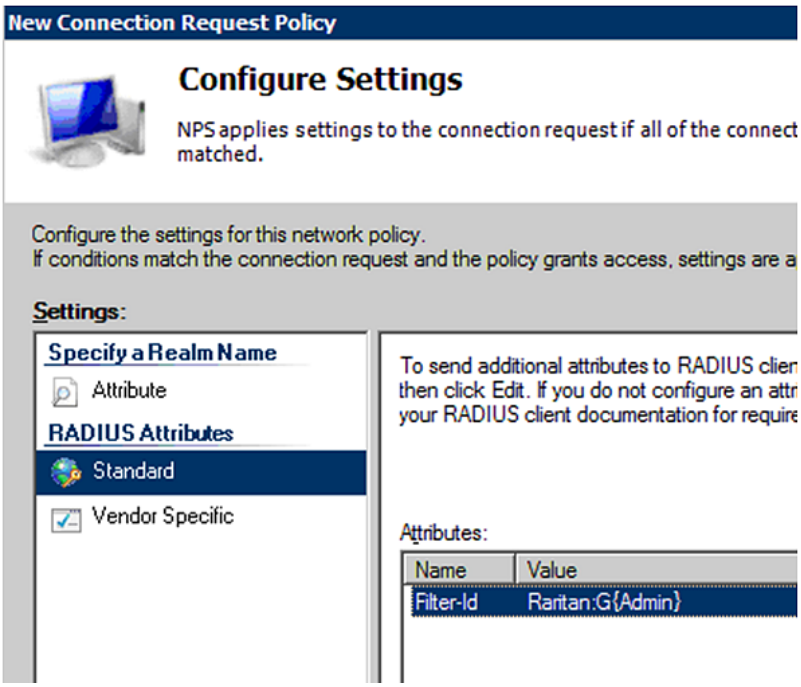
Admin inside the curved brackets {} is the existing role on the PX. It is recommended to use the Admin role to test this configuration. The role name is case sensitive.



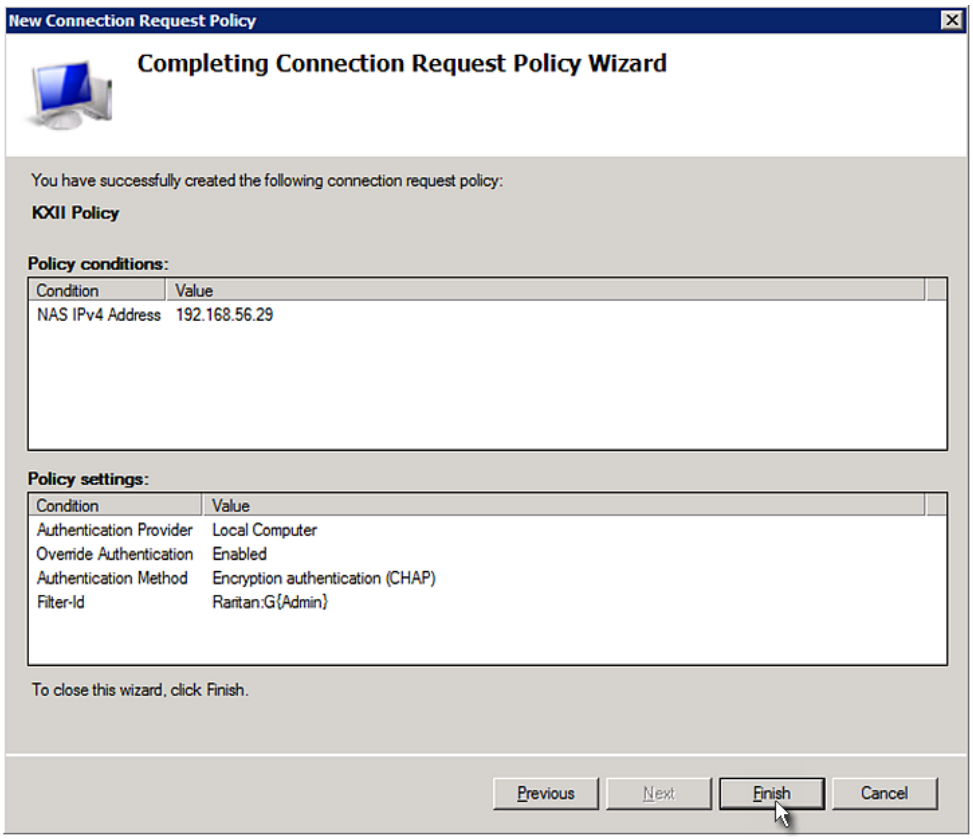
14. The new attribute is added. Click OK.



15. Click Next to continue.



16. A summary showing connection request policy settings is displayed. Click Finish to close the dialog.



Step C: Configure a Vendor-Specific Attribute

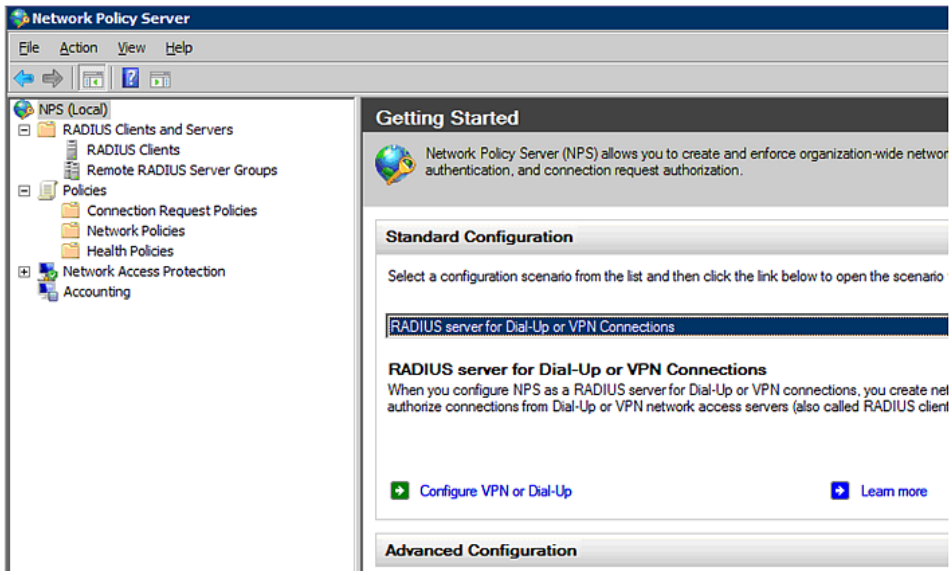
You must specify a vendor-specific attribute (VSA) for Raritan on Windows 2008 NPS. Raritan's vendor code is **13742**.

In the following illustration, we assume:

- There are three roles available on your PX: *Admin*, *User*, and *SystemTester*.

To configure VSA:

1. Open the NPS console, and expand the Policies folder.



2. Select Connection Request Policies and double-click the policy where you want to add a custom VSA. The policy's properties dialog appears.
3. Click the Settings tab.
4. Select Vendor Specific, and click Add. The Add Vendor Specific Attribute dialog appears.
5. Select Custom in the Vendor field, and click Add. The Attribute Information dialog appears.
6. Click Add, and the Vendor-Specific Attribute Information dialog appears.
7. Click "Enter Vendor Code" and type *13742*.
8. Select "Yes, it conforms" to indicate that the custom attribute conforms to the RADIUS Request For Comment (RFC).
9. Click Configure Attribute, and then:

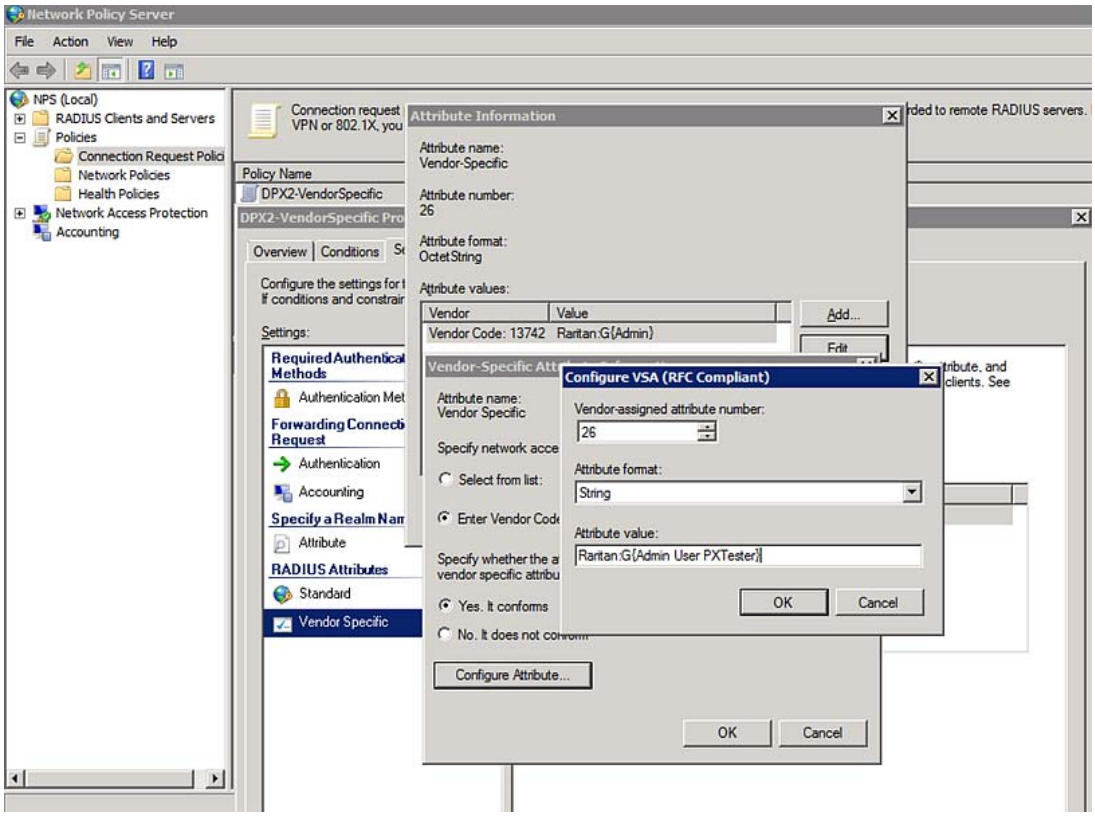
a. Type *26* in the "Vendor-assigned attribute number" field.

b. Select String in the "Attribute format" field.

c. Type *Raritan:G{Admin User SystemTester}* in the "Attribute value" field. In this example, three roles are specified inside the curved brackets {} -- Admin, User and SystemTester.

Note that different roles must be separated with a space.

10. Click OK.



AD-Related Configuration

When RADIUS authentication is intended, make sure you also configure the following settings related to Microsoft Active Directory (AD):

- Register the NPS server in AD
- Configure remote access permission for users in AD

The NPS server is registered in AD only when NPS is configured for the FIRST time and user accounts are created in AD.

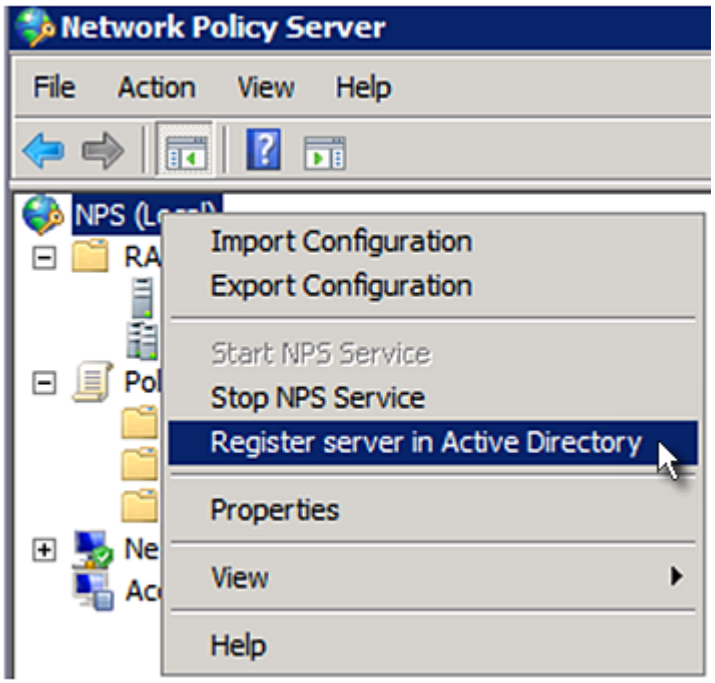
If CHAP authentication is used, you must enable the following feature for user accounts created in AD:

- Store password using reversible encryption

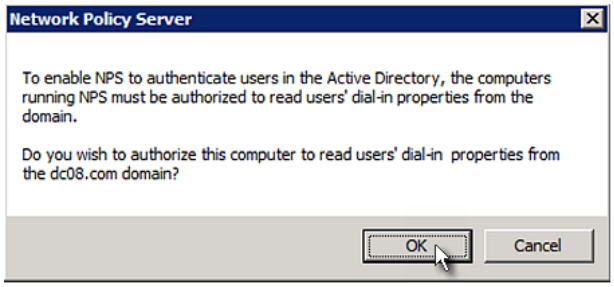
Important: Reset the user password if the password is set before you enable the "Store password using reversible encryption" feature.

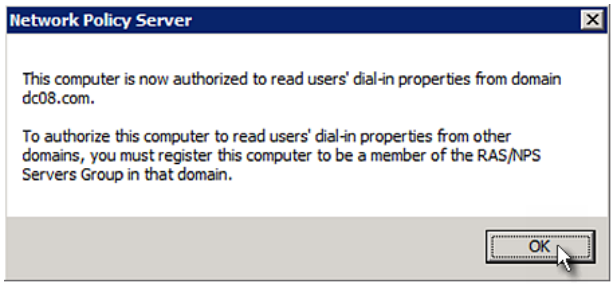
To register NPS:

1. Open the NPS console.
2. Right-click NPS (Local) and select "Register server in Active Directory."



3. Click OK, and then OK again.

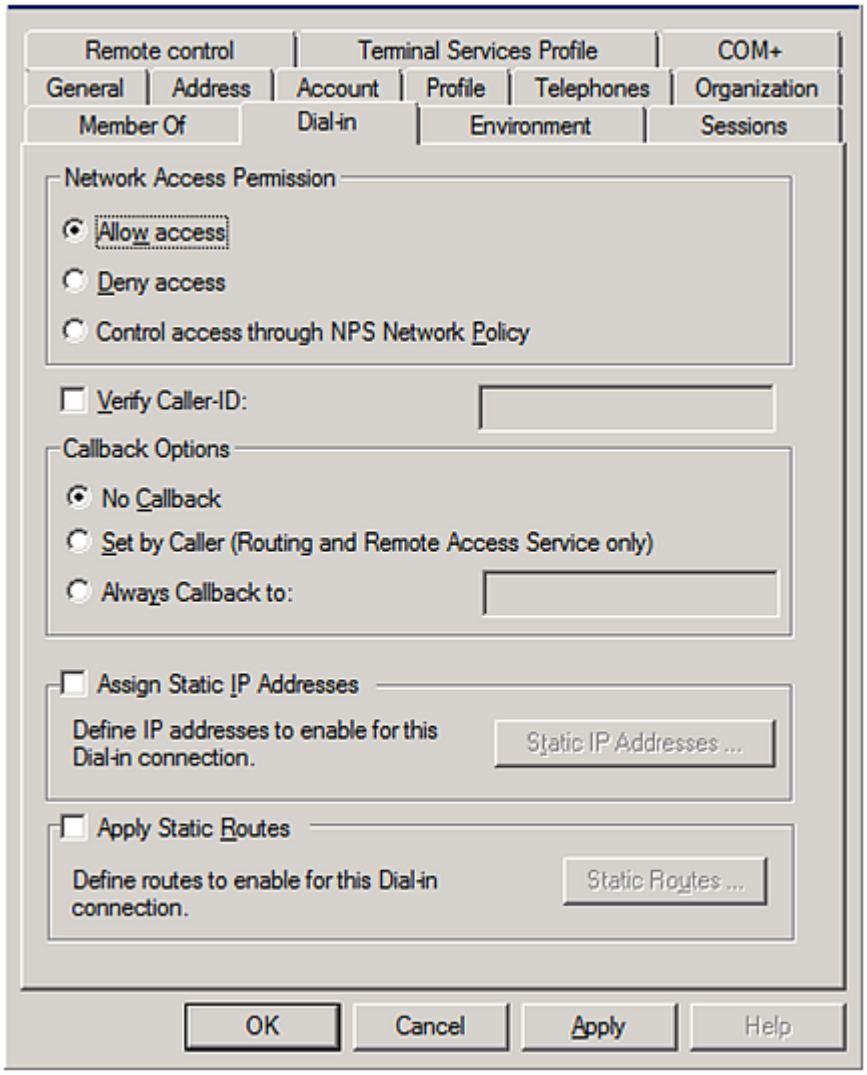




To grant PX users remote access permission:

1. Open Active Directory Users and Computers.
2. Open the properties dialog of the user whom you want to grant the access permission.

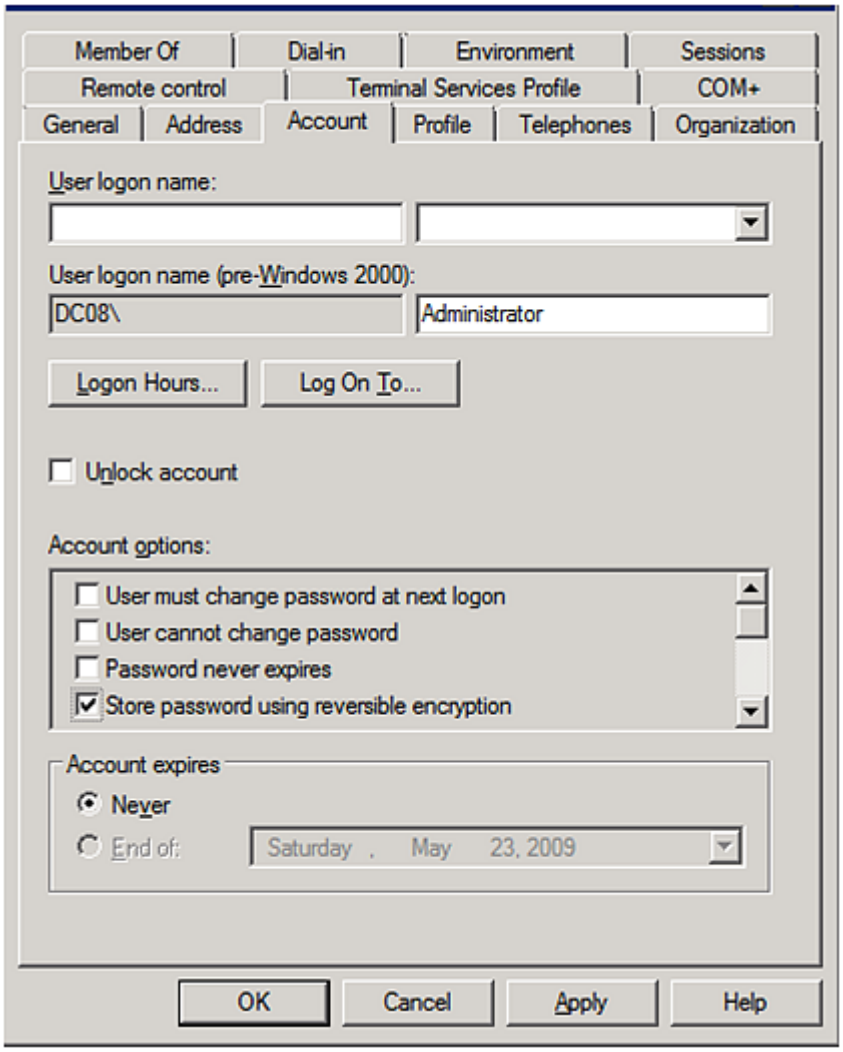
3. Click the Dial-in tab and select the "Allow access" checkbox.



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.



Non-Windows RADIUS Server

For a non-Windows RADIUS server, such as FreeRADIUS, a vendor-specific dictionary file is required.

Dictionary File

Create a vendor-specific dictionary file for Raritan and add the following information to it. Raritan's vendor code is **13742**.

```
# -*- text -*-
#
# dictionary.raritan
#
#
# Version:      $Id$
#
VENDOR          Raritan                         13742
#
#  Standard attribute
#
BEGIN-VENDOR    Raritan

ATTRIBUTE       Raritan-Vendor-Specific         26    string

END-VENDOR      Raritan
```

Note that "string" in the above contents must be replaced by `Raritan:G{roles}`, where "roles" are one or multiple roles to which the user belongs. For more details, see ***Format of the "string"*** (on page 660).

Format of the "string"

The format of `string` in the dictionary file is:

```
Raritan:G{roles}
```

"roles" inside the curved brackets {} are role names, which comprise one or multiple roles to which the user belongs.

Multiple role names are separated with a space.

Example:

If the user has three roles -- *Admin*, *User* and *SystemTester*, then type:

```
Raritan:G{Admin User SystemTester}
```

Therefore, in Raritan's dictionary file, the attribute line is like the following:

```
ATTRIBUTE    Raritan-Vendor-Specific 26    Raritan:G{Admin User SystemTester}
```

Appendix L Additional PX Information

In This Chapter

Locking Outlets and Cords 662
Unbalanced Current Calculation 664
Reserving IP Addresses in Windows DHCP Servers.....665
Sensor Threshold Settings 667
PDView App for Viewing the PX.....674
Altitude Correction Factors.....677
Data for BTU Calculation.....677
Ways to Probe Existing User Profiles.....678
Truncated Data in the Web Interface 678
Raritan Training Website 679

Locking Outlets and Cords

In addition to the cable retention clips, Raritan also provides other approaches to secure the connection of the power cords from your IT equipment to the Raritan PDUs, including:

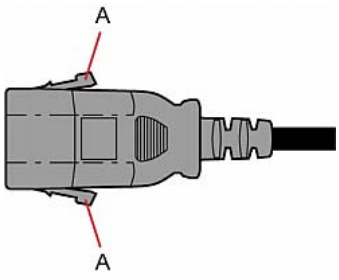
- SecureLock™ outlets and cords
- Button-type locking outlets

Note that NOT all Raritan PDUs are implemented with any of the above locking outlets.

SecureLock™ Outlets and Cords

SecureLock™ is an innovative mechanism designed by Raritan, which securely holds C14 or C20 plugs that are plugged into Raritan PDUs in place. This method requires the following two components:

- Raritan PDU with SecureLock™ outlets, which have a latch slot inside either side of the outlet.
- SecureLock™ cords, which is a power cord with a locking latch on each side of its plug. The following diagram illustrates such a plug.



Item	Description
A	Latches on the SecureLock™ cord's plug

Only specific PDUs are implemented with the SecureLock™ mechanism. If your PDU does not have this design, do NOT use the SecureLock™ cords with it.

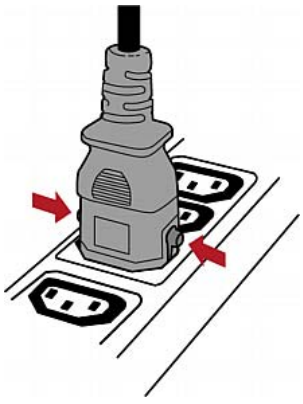
Tip: The SecureLock™ outlets can accept regular power cords for power distribution but the SecureLock™ mechanism does not take effect.

To lock a power cord using the SecureLock™ mechanism:

1. Verify that the SecureLock™ cord you purchased meets your needs.
   - The cords' female socket matches the power socket type (C14 or C20) on your IT equipment.
   - The cord's male plug matches the outlet type (C13 or C19) on your PDU.
2. Connect the SecureLock™ cord between the IT equipment and your PDU.
   - Plug the female socket end of the cord into the power socket of the desired IT equipment.
   - Plug the male plug end of the cord into the appropriate SecureLock™ outlet on the PDU. Push the plug toward the outlet until you hear the click, which indicates the plug's latches are snapped into the latch slots of the outlet.

To remove a SecureLock™ power cord from the PDU:

1. Press and hold down the two latches on the cord's plug as illustrated in the diagram below.



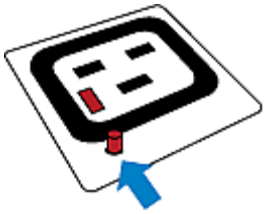
2. Unplug the cord now.

Button-Type Locking Outlets

A button-type 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 on the outlet. Depending on the outlet type, the button location differs.



2. Unplug the power cord now.

Unbalanced Current Calculation

Unbalanced current information is available on 3-phase models only. This section explains how the PX 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%

Reserving IP Addresses in Windows DHCP Servers

The PX uses its serial number as the client identifier in the DHCP request. Therefore, to successfully reserve an IP address for the PX in a Windows® DHCP server, use the PX device's serial number as the unique ID instead of the MAC address.

IP address reservation procedure:

1. Convert the serial number of your PX into hexadecimal ASCII codes.
   - For example, if the serial number is `PEG1A00003`, convert each digit to ASCII codes as shown below:

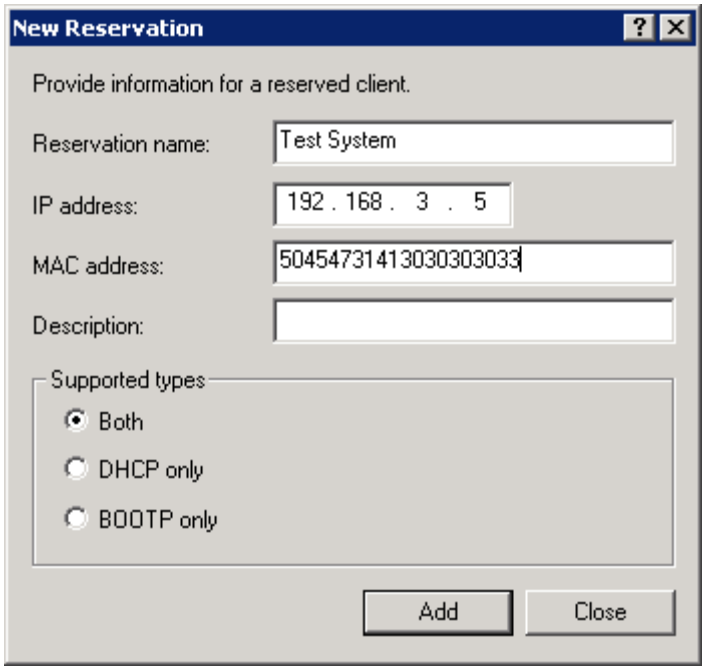
```
P=50
E=45
G=47
1=31
A=41
0=30
3=33
```

Therefore, the complete ASCII codes are as follows:

```
PEG1A00003 = 50454731413030303033
```

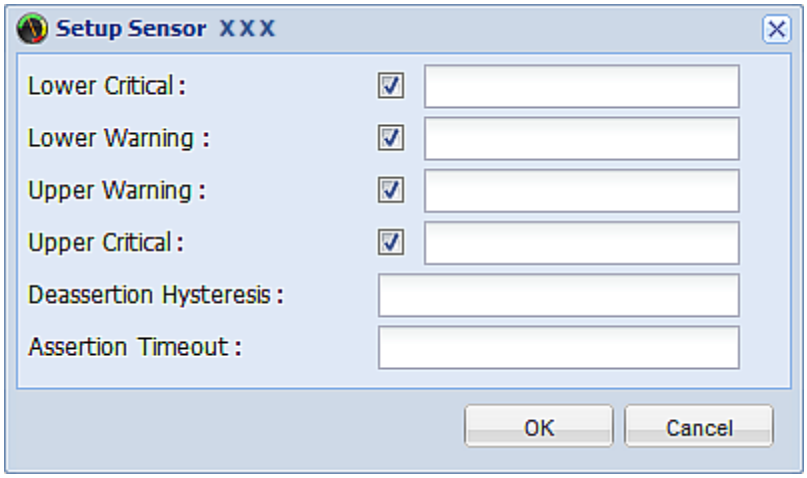
2. In your DHCP server, bring up the New Reservation dialog to reserve the IP address for your PX.

Field	Description
IP address	Enter the IP address you want to reserve.
MAC address	Enter the ASCII codes of the PX serial number. Do NOT contain spaces in the ASCII codes. ▪ In this example, enter `50454731413030303033`
Other fields	Configure them according to your needs.



Sensor Threshold Settings

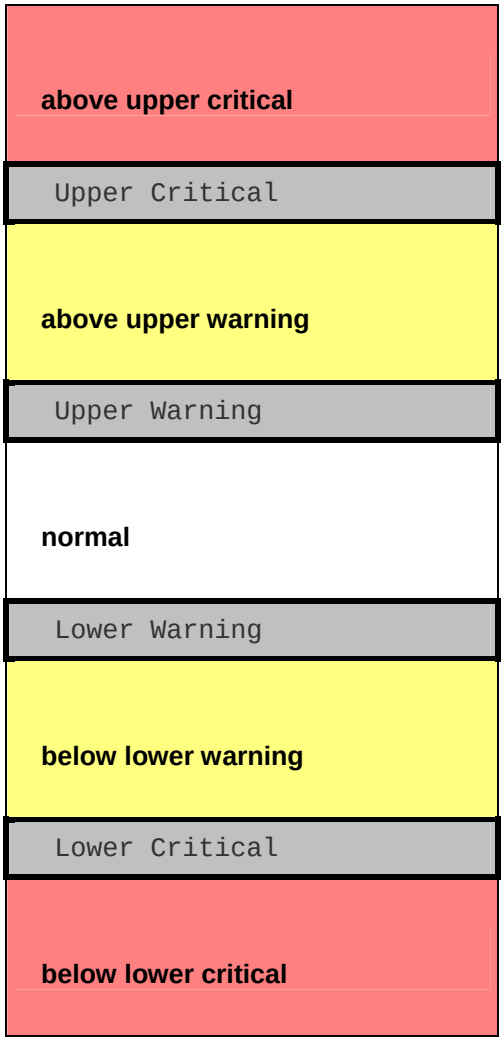
This section explains the thresholds settings in a threshold setup dialog for a numeric internal or external sensor.



Thresholds and Sensor States

A numeric sensor has four threshold settings: Lower Critical, Lower Warning, Upper Warning and Upper Critical.

The threshold settings determine how many sensor states are available for a certain sensor and the range of each sensor state. The diagram below shows how each threshold relates to each state.



Available sensor states:

The more thresholds are enabled for a sensor, the more sensor states are available for it. The "normal' state is always available regardless of whether any threshold is enabled.

For example:

- When a sensor only has the Upper Critical threshold enabled, it has two sensor states: normal and above upper critical.
- When a sensor has both the Upper Critical and Upper Warning thresholds enabled, it has three sensor states: normal, above upper warning, and above upper critical.

States of "above upper warning" and "below lower warning" are warning states to call for your attention.

States of "above upper critical" and "below lower critical" are critical states that require you to immediately handle.

Range of each available sensor state:

The value of each enabled threshold determines the reading range of each available sensor state. For details, see:

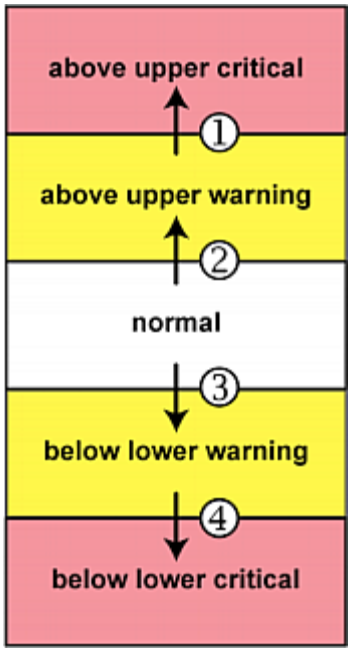
- ***"above upper critical" State*** (on page 311)
- ***"above upper warning" State*** (on page 310)
- ***"below lower critical" State*** (on page 310)
- ***"below lower warning" State*** (on page 310)

"To Assert" and Assertion Timeout

If multiple sensor states are available for a specific sensor, the PX asserts a state for it whenever a bad state change occurs.

To assert a state:

To assert a state is to announce a "worse" new state. Below are bad state changes that cause the PX to assert.

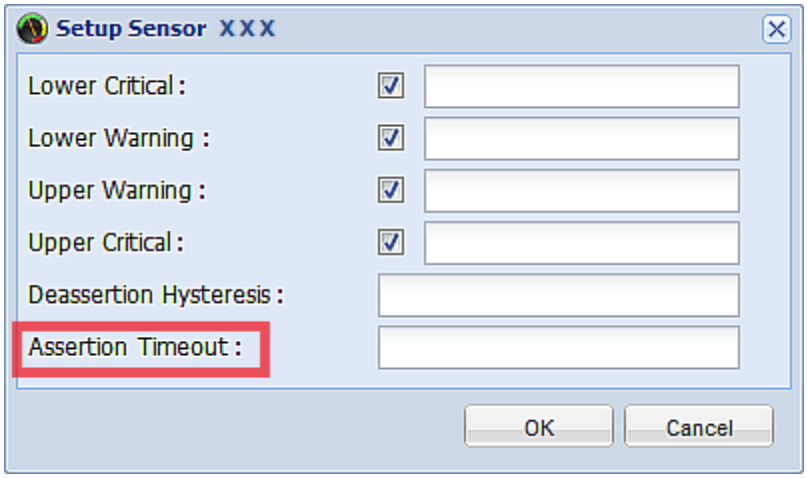


1. above upper warning --> above upper critical
2. normal --> above upper warning
3. normal --> below lower warning
4. below lower warning --> below lower critical

Assertion Timeout:

In the threshold setup dialog, the Assertion Timeout field impacts the "assertion" action. It determines how long a sensor must be in the "worse" new state before the PX turns on the "assertion" action. If that sensor changes its state again within the specified wait time, the PX does NOT assert the worse state.

To disable the assertion timeout, set it to 0 (zero).



Note: For most sensors, the measurement unit in the "Assertion Timeout" field is sample. Because the PX measures each sensor every second, timing of a sample is equal to a second.

How "Assertion Timeout" is helpful:

If you have created an event rule that instructs the PX to send notifications for assertion events, setting the "Assertion Timeout" is helpful for eliminating a number of notifications that you may receive in case the sensor's reading fluctuates around a certain threshold.

Assertion Timeout Example for Temperature Sensors

Assumption:

```
Upper Warning threshold is enabled.
Upper Warning = 25 (degrees Celsius)
Assertion Timeout = 5 samples (that is, 5 seconds)
```

When a temperature sensor's reading exceeds 25 degrees Celsius, moving from the "normal" range to the "above upper warning" range, the PX does NOT immediately announce this warning state. Instead it waits for 5 seconds, and then does either of the following:

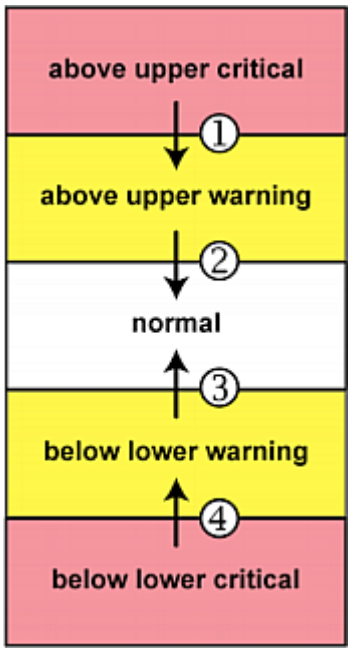
- If the temperature remains above 25 degrees Celsius in the "above upper warning" range for 5 seconds, the PX turns on the "assertion" action to announce the "above upper warning" state.
- If the temperature drops below 25 degrees Celsius within 5 seconds, the PX does NOT turn on the "assertion" action.

"To De-assert" and Deassertion Hysteresis

After the PX asserts a worse state for a sensor, it may de-assert the same state later on.

To de-assert a state:

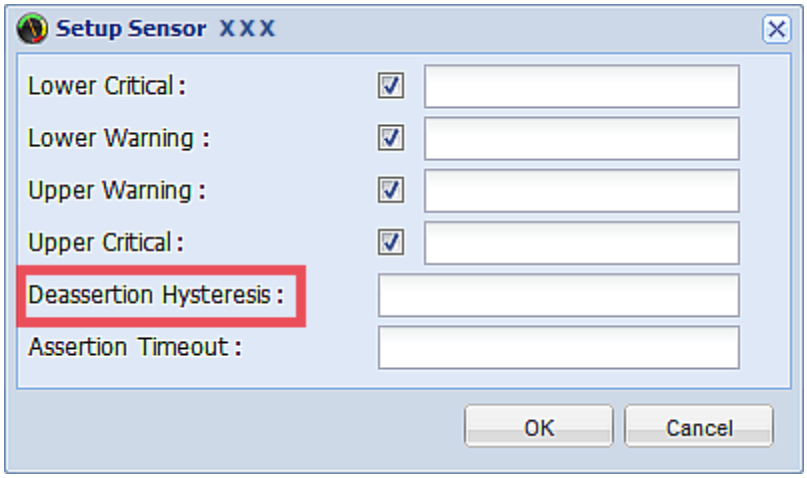
To de-assert a state is to announce the end of the previously asserted worse state. Below are good state changes that cause the PX to de-assert the previous state.



1. above upper critical --> above upper warning
2. above upper warning --> normal
3. below lower warning --> normal
4. below lower critical --> below lower warning

Deassertion Hysteresis:

In the threshold settings dialog, the Deassertion Hysteresis field determines a new level to turn on the "deassertion" action.



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 PX to de-assert the worse state for a sensor only when that sensor's reading hits the pre-determined "deassertion" level.

For upper thresholds, this "deassertion" level is a decrease against each threshold. For lower thresholds, this level is an increase to each threshold. The value of the decrease or increase is exactly the hysteresis value.

For example:

If Deassertion Hysteresis = 2,

- Upper Critical = 33, so its "deassertion" level = 33 - 2 = 31.
- Upper Warning = 25, so its "deassertion" level = 25 - 2 = 23.
- Lower Critical = 10, so its "deassertion" level = 10 + 2 = 12.
- Lower Warning = 18, so its "deassertion" level = 18 + 2 = 20.

To use each threshold as the "deassertion" level instead of determining a new level, set the Deassertion Hysteresis to 0 (zero).

How "Deassertion Hysteresis" is helpful:

If you have created an event rule that instructs the PX to send notifications for deassertion events, setting the "Deassertion Hysteresis" is helpful for eliminating a number of notifications that you may receive in case a sensor's reading fluctuates around a certain threshold.

Deassertion Hysteresis Example for Temperature Sensors

Assumption:

```
Upper Warning threshold is enabled.
Upper Warning = 20 (degrees Celsius)
Deassertion Hysteresis = 3 (degrees Celsius)
"Deassertion"  level = 20-3 = 17 (degrees Celsius)
```

When the PX 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 PX does NOT turn on the "deassertion" action.
- If the temperature drops to 17 degrees Celsius or lower, the PX turns on the "deassertion" action to announce the end of the "above upper warning" state.

PDView App for Viewing the PX

Raritan has developed an app that can turn your iOS or Android mobile device into a local display for the PX.

This app is called PDView and it can be downloaded for free.

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

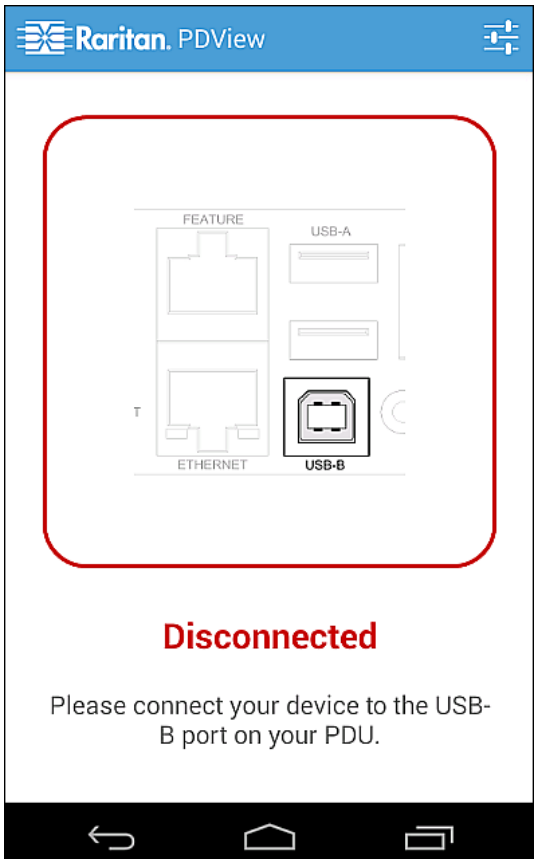
Requirements for using PDView:

- The PX is running firmware version 3.0.0 or later.
- If you are using an Android device, it must support USB "On-The-Go" (OTG).
- An appropriate USB cable is required.
  - For Android, you need a USB OTG adapter cable.
  - For iOS, use the USB cable shipped with your iOS mobile device.

To install PDView:

1. Use your mobile device to download the PDView app from the Google Play or Apple's App Store.

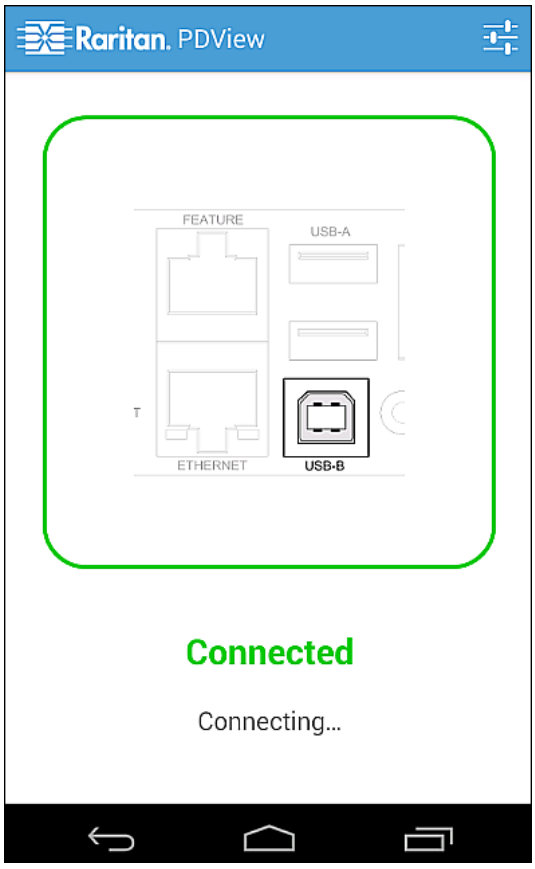
2. After installing the PDView, launch it. Below illustrates the PDView for Android devices.



3. Connect your mobile device to the USB port of the PX.

   Your mobile device type determines which USB port on the PX shall be used to connect the mobile device. The PDView will automatically detect and indicate the appropriate USB port for connecting your mobile device.

The PDView shows a "Connected" message when it detects the physical connection to the PX.



4. Log in to the PDView app at the login prompt. Now you can view limited PX information or even change some settings.

Tip: To skip the final login step, you can click the upper right icon of PDView to save one or multiple user credentials. Next time the app automatically logs in when it detects the PX.

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

Data for BTU Calculation

The heat generated by the PX device differs according to the model you purchased. To calculate the heat (BTU/hr), use the following power data according to your model type in the BTU calculation formula.

Model name	Maximum power (Watt)
PX2-1000 PX3-1000	5
PX2-2000 PX3-2000	20
PX2-3000 PX3-3000	24
PX2-4000 PX3-4000	24
PX2-5000 PX3-5000	24

Ways to Probe Existing User Profiles

This section indicates available ways to query existing user accounts on the PX.

- With SNMP v3 activated, you get the "user unknown" error when the user name used to authenticate does not exist.
- Any user with the permission to view event rules can query all local existing users via JSON RPC.
- Any user with the permission to view the event log may get information about existing users from the log entries.
- Any authenticated users can query currently-existing connection sessions, including Webcam-Live-Preview sessions, which show a list of associated user names.

Truncated Data in the Web Interface

Some fields of the PX web interface can accommodate data entry up to 256 characters. When the data entered is too long, it may be truncated due to some or all of the following factors:

- Screen resolution
- Font size
- Font type
- Size of different characters

Current web browser technology cannot break or wrap these fields with long inputs.

The solution for this issue includes:

- Increase of the screen resolution
- Application of smaller font size
- Use of other interfaces, such as the CLI or SNMP, to view the data in these fields

Raritan Training Website

Raritan offers free training materials for various Raritan products on the ***Raritan training website http://www.raritantraining.com***. The Raritan products introduced on this website include the intelligent PDU, dcTrack®, Power IQ, KVM, EMX, BCM and CommandCenter Secure Gateway (CC-SG). Raritan would update the training materials irregularly according to the latest development of Raritan products.

To get access to these training materials or courses, you need to apply for a username and password through the Raritan training website. After you are verified, you can access the Raritan training website anytime.

Having access to the training website could be helpful for learning or getting some ideas regarding Raritan products and making correct decisions on purchasing them. For example, you can take the dcTrack video training before implementing or using it.

Appendix M Integration

The PX device can work with certain Raritan products to provide diverse power solutions.

In This Chapter

Dominion KX II / III Configuration 680
Dominion KSX II, SX or SX II Configuration 685
Power IQ Configuration 690
dcTrack 691

Dominion KX II / III Configuration

Raritan PX2, PX3 or PX3TS series can be connected to the Raritan's Dominion KX II or KX III device (a digital KVM switch) to provide one more alternative of power management.

Note that this integration requires the following firmware versions:

- Dominion KX II -- 2.4 or later
- Dominion KX III -- ALL versions
- PX2 series -- 2.2 or later
- PX3 series -- 2.5.10 or later
- PX3TS series -- 2.6.1 or later

Dominion KX II or KX III integration requires D2CIM-PWR and straight CAT5 cable.

For more information on KX II / III, refer to:

- KX II or KX III User Guide on the ***Support page*** (***http://www.raritan.com/support/***)
- KX II or KX III Online Help on the ***Product Online Help page*** (***http://www.raritan.com/support/online-help/***)

Note: For documentation conveniences, both Dominion KX II and KX III products are referred to as "KX III" in the following sections.

Configuring Rack PDU Targets

KX III allows you to connect rack PDUs (power strips) to KX III ports.

KX III rack PDU configuration is done from the KX III Port Configuration page.

Note: Raritan recommends no more than eight (8) rack PDUs (power strips) be connected to a KX III at once since performance may be affected.

Connecting a PX PDU

Raritan PX series rack PDUs (power strips) are connected to the Dominion device using the D2CIM-PWR CIM.

To connect the rack PDU:

1. Connect the male RJ-45 of the D2CIM-PWR to the following female RJ-45 connector of the rack PDU.
   - PX1 series: RJ-45 "SERIAL" port
   - PX2 or PX3 series: RJ-45 "FEATURE" port
2. Connect the female RJ-45 connector of the D2CIM-PWR to any of the available female system port connectors on the KX III using a straight through Cat5 cable.
3. Attach an AC power cord to the target server and an available rack PDU outlet.
4. Connect the rack PDU to an AC power source.
5. Power on the device.

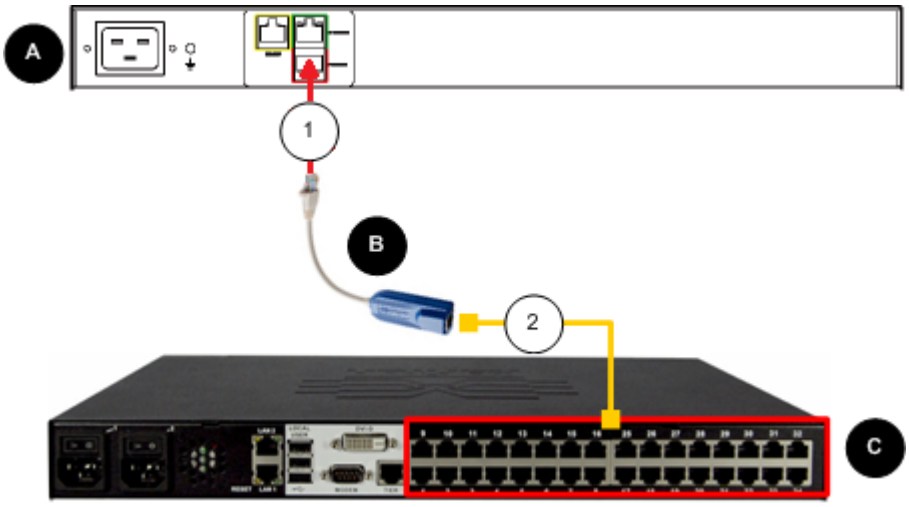


Diagram key	
A	PX rack PDU
B	D2CIM-PWR
C	KX III
1	D2CIM-PWR to rack PDU connection
2	D2CIM-PWR to KX III target device port via Cat5 cable

Naming the Rack PDU (Port Page for Power Strips)

Note: PX rack PDUs (power strips) can be named in the PX as well as in the KX III.

Once a Raritan remote rack PDU is connected to the KX III, it will appear on the Port Configuration page. Click on the power port name on that page to access it. The Type and the Name fields are prepopulated.

Note: The (CIM) Type cannot be changed.

The following information is displayed for each outlet on the rack PDU: [Outlet] Number, Name, and Port Association.

Use this page to name the rack PDU and its outlets. Names can be up to 32 alphanumeric characters and can include special characters.

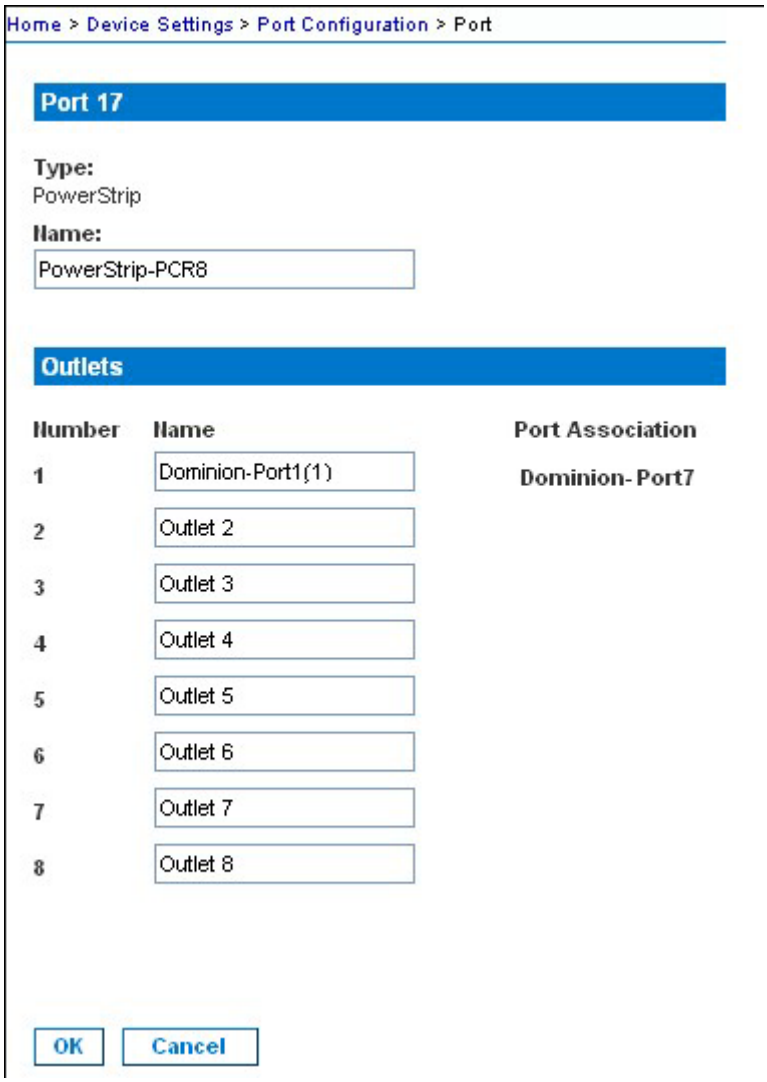
Note: When a rack PDU is associated with a target server (port), the outlet name is replaced by the target server name, even if you assigned another name to the outlet.

To name the rack PDU and outlets:

Note: CommandCenter Secure Gateway does not recognize rack PDU names containing spaces.

1. Enter the Name of the rack PDU (if needed).
2. Change the [Outlet] Name if desired. (Outlet names default to the outlet #.)

3. Click OK.


Home > Device Settings > Port Configuration > Port
Port 17
Type:
PowerStrip
Name:
PowerStrip-PCR8
Outlets
Number
Name
Port Association
1
Dominion-Port1(1)
Dominion- Port7
2
Outlet 2
3
Outlet 3
4
Outlet 4
5
Outlet 5
6
Outlet 6
7
Outlet 7
8
Outlet 8
OK
Cancel

Associating Outlets with Target Devices

The Port page opens when you click on a port on the Port Configuration page.

If an outlet is connected to the same server that the port is connected to, a power association can be made with the target device.

A server can have up to four power plugs and you can associate a different rack PDU (power strip) with each. From this page, you can define those associations so that you can power on, power off, and power cycle the server from the Port Access page.

To use this feature, you will need:

- Raritan remote rack PDU(s)
- Power CIMs (D2CIM-PWR)

Make a Power Association

To make power associations (associate rack PDU outlets to KVM target servers):

Note: When a rack PDU is associated to a target server (port), the outlet name is replaced by the target server name (even if you assigned another name to the outlet).

1. On the Port Configuration page, select the target server you are associating the PDU with.
2. Choose the rack PDU from the Power Strip Name drop-down list.
3. For that rack PDU, choose the outlet from the Outlet Name drop-down list.
4. Repeat steps 1 and 2 for all desired power associations.
5. Click OK. A confirmation message is displayed.

Turning Outlets On/Off and Cycling Power

To turn an outlet on:

1. Click the Power menu to access the Powerstrip page.
2. From the Powerstrip drop-down, select the PX rack PDU (power strip) you want to turn on.
3. Click Refresh to view the power controls.
4. Click On next to the outlet you want to power on.
5. Click OK to close the Power On confirmation dialog. The outlet will be turned on and its state will be displayed as 'on'.

To turn an outlet off:

1. Click Off next to the outlet you want to power off.
2. Click OK on the Power Off dialog.
3. Click OK on the Power Off confirmation dialog. The outlet will be turned off and its state will be displayed as 'off'.

To cycle the power of an outlet:

1. Click Cycle next to the outlet you want to cycle. The Power Cycle Port dialog opens.
2. Click OK. The outlet will then cycle (note that this may take a few seconds).
3. Once the cycling is complete the dialog will open. Click OK to close the dialog.

Dominion KSX II, SX or SX II Configuration

Raritan PX support the integration with Raritan's serial access products - Dominion KSX II, Dominion SX and Dominion SX II.

Cables used for connecting the PX to different Dominion access products are different.

- KSX II - a standard network patch cable (CAT5 or higher)
- SX - a CSCSPCS cable
- SX II - a standard network patch cable (CAT5 or higher) and D2CIM-PWR

Note: To only access the CLI of the PX via SX / SX II, treat the PX as a serial device by connecting SX /SX II to the PDU's serial port instead of the FEATURE port.

For more information on these Dominion serial access product, refer to:

- KSX II, SX or SX II User Guide on the ***Support page*** (***http://www.raritan.com/support/***)
- KSX II, SX or SX II Online Help on the ***Product Online Help page*** (***http://www.raritan.com/support/online-help/***)

Dominion KSX II

After connecting a Dominion KSX II to the Raritan PDU, you can monitor the PDU and even control its outlets if the PDU is an outlet-switching capable model.

Connecting a Rack PDU

To connect the Raritan PX to the KSX II:

1. Connect one end of a Cat5 cable to the following ports of different Raritan PX.
   - PX1 series: RJ-45 "SERIAL" port
   - PX2 or PX3 series: RJ-45 "FEATURE" port
2. Connect the other end of the Cat5 cable to either the Power Ctrl. 1 or Power Ctrl. 2 ports on the back of the KSX II.
3. Attach an AC power cord to the target server and an available rack PDU outlet.
4. Connect the rack PDU to an AC power source.
5. Power on the KSX II device.

Important: When using CC-SG, the power ports should be inactive before attaching rack PDUs that were swapped between the power ports. If this is not done, there is a possibility that the number of power outlets will not be correctly detected, especially after swapping 8 and 20 outlet rack PDU models.

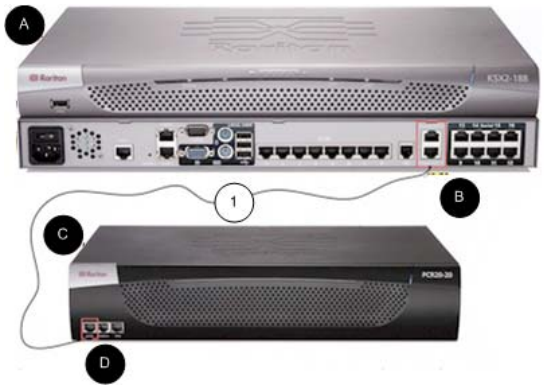


Diagram key			
A	KSX II	D	PX SERIAL or FEATURE port
B	KSX II Power Ctrl. 1 Port or Power Ctrl. 2 Port	1	Cat5 cable
C	PX		

Power Control

The KSX II operation to turn on/off or power cycle a PX is the same as the KX III operation. See ***Turning Outlets On/Off and Cycling Power*** (on page 684).

Dominion SX and SX II

By connecting to a Dominion SX or SX II device, you can associate one or more outlets on a PX device to specific SX or SX II ports.

Dominion SX II

The way to use Dominion SX II to connect, configure and control a Raritan PX is the same as the way to use Dominion KX III. For detailed information, refer to:

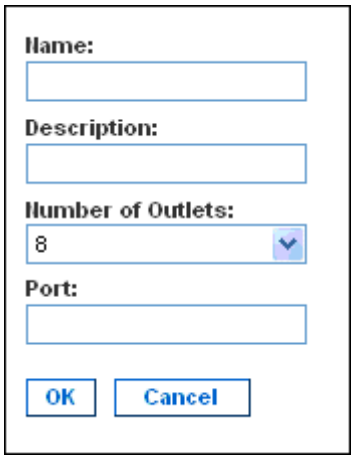
- ***Connecting a PX PDU*** (on page 681)
- ***Naming the Rack PDU (Port Page for Power Strips)*** (on page 682)
- ***Associating Outlets with Target Devices*** (on page 684)
- ***Turning Outlets On/Off and Cycling Power*** (on page 684)

Dominion SX

Configuring a PX on Dominion SX

1. Choose Setup > Power Strip Configuration.

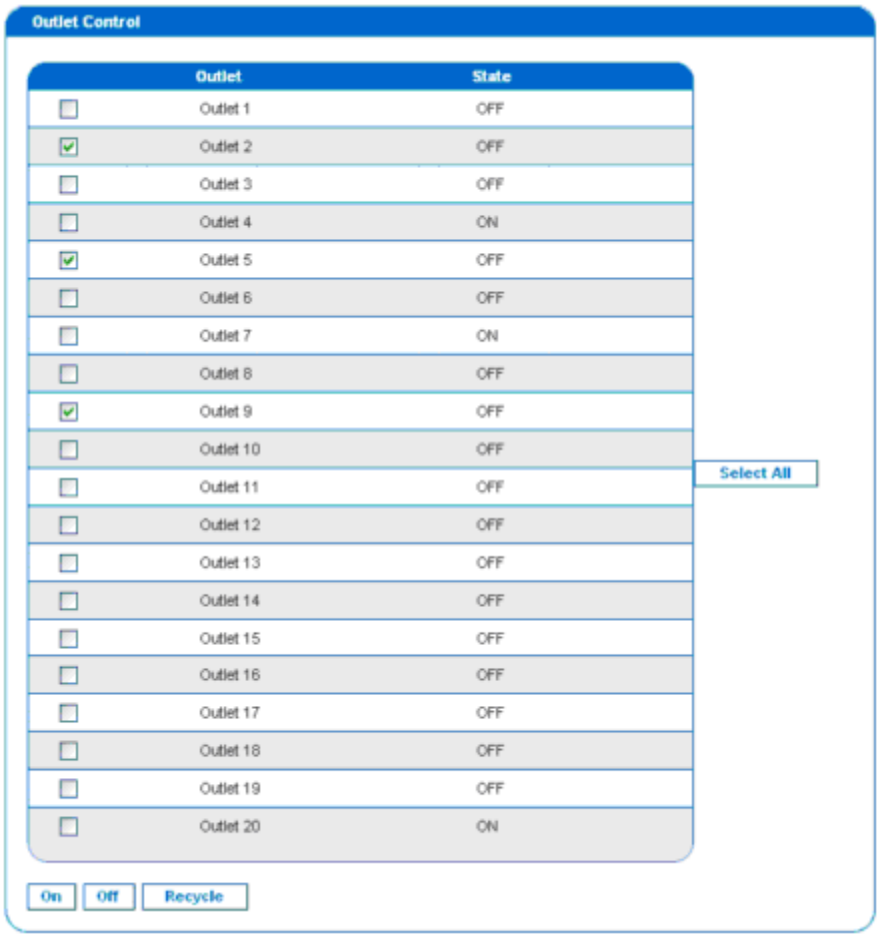
2. Click Add. The Power Strip Configuration screen appears.



3. Type a name and description in the Name and Description fields.
4. Select the number of outlets from the Number of Outlets drop-down menu.
5. Type the port number in the Port field.
6. Click OK.

Power Control

1. Choose Power Control > Power Strip Power Control. The Outlet Control screen appears.



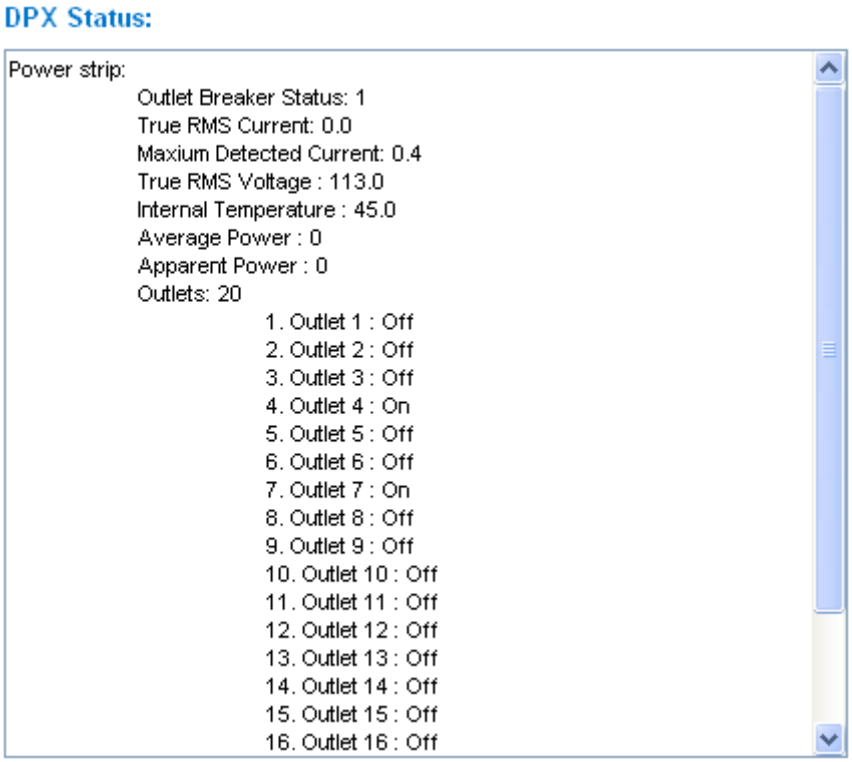
2. Check the box of outlet number you wish to control, and click On/Off buttons to power on/off the selected outlet(s).
3. A confirmation message appears, indicating successful operation.

Outlet 19: The power operation has been sent.

The system shall reflect successful operations shortly.

Checking Power Strip Status

1. Choose Power Control > Power Strip Status.



2. A status box appears, displaying details of the controlled PX, including power state of each outlet on the device.

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 PX is categorized as a power item in dcTrack. dcTrack offers an import wizard for conveniently adding the PX 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.

Asset Management Sensors and dcTrack

If any asset sensors are connected to the PX, the PX can transmit their information to Sunbird's dcTrack. All you have to do is to add the PX to dcTrack, and also add each IT item where an asset tag is attached to dcTrack.

Note: For instructions on connecting asset sensors, see **Connecting Asset Management Sensors** *(on page 54).*

If SNMP is enabled, event information can be transmitted to dcTrack. Specifically, Sunbird's Power IQ detects when an asset tag is connected or disconnected from an asset sensor. Power IQ then generates a connect or disconnect event. When dcTrack polls Power IQ, the connect/disconnect events are pulled into dcTrack, and displayed in the dcTrack Web Client.

To poll and display asset management events in dcTrack

- The PX that the asset sensor is connected to must exist in dcTrack.

  EMX devices are identified as probes in dcTrack; Raritan PDUs are identified as sensors.

- Each IT item connected to the asset sensor via an asset tag must exist in dcTrack.

  You do not need to manually enter the asset tag IDs for IT items that already exist in dcTrack as long as these items are in the Installed status.

  Simply, plug the item's asset tag into an asset sensor that is connected to the PX that exists in dcTrack. dcTrack automatically assigns the asset tag ID to the existing IT item.

  Note: If needed, the asset tag number can be overwritten.

For more details on dcTrack as well as how asset sensors work with dcTrack, contact Sunbird Professional Services and Support from the http://support.sunbirddcim.com.

Index

1

1U and 2U Port Locations • 72
1U Products • 2

2

2U Products • 2

A

A Note about Enabling Thresholds • 362
A Note about Firmware Upgrade Time • 346
A Note about Infinite Loop • 285
A Note about Untriggered Rules • 289
About the Interface • 363
Access Security Control • 178
Accessing the Help • 347
Action Group • 238, 240
Activating or Deactivating the Load Shedding Mode • 222
Actuator Configuration Commands • 482, 483, 499
Actuator Control Operations • 522
Actuator Information • 380
Add Page Icon • 115, 118
Adding a Firewall Rule • 440
Adding a Monitored Device • 500
Adding a Role-Based Access Control Rule • 453
Adding Attributes to the Class • 634
Adding Authentication Servers • 200
Adding IT Devices for Ping Monitoring • 293
Adding LDAP Server Settings • xx, 200
Adding RADIUS Server Settings • 203, 639
Additional PX Information • 666
Adjusting Image Properties • 326, 328
AD-Related Configuration • 639, 660
Alarm • 238, 241
Alarms List • 124, 238, 241
Alert States and LHX Event Log • 341
Alerted Sensors • 79, 123
Alerts • xx, 78
Alerts Notice in a Yellow or Red Screen • xx, 74, 98
All Privileges • xxi, 471, 477, 478, 481
Altitude Correction Factors • 165, 408, 681
APIPA and Link-Local Addressing • xx, 3, 109, 146, 155
Applicable Models • xviii
Assertion Timeout Example for Temperature Sensors • 675
Asset Management • 316
Asset Management Commands • 506
Asset Management Sensors and dcTrack • 697
Asset Sensor Information • 618
Asset Sensor Management • 507
Asset Sensor Settings • 391
Assets • 78, 93
Associating Outlets with Target Devices • 688, 691
Automatic and Manual Modes • xx, 74, 78, 151
Automatically Completing a Command • 529
Available SCP Commands • 587

B

Backup and Restore of PX Device Settings • 321, 324, 555
Backup and Restore via SCP • 325, 589
Beeper • 105, 168
Before You Begin • 13
Blade Extension Strip Settings • 393
Browser-Defined Shortcut Menu • 122
Browsing through the Online Help • 348
Bulk Configuration • 33, 321, 324, 588
Bulk Configuration for Outlet Thresholds • 229, 230
Bulk Configuration for Overcurrent Protector Thresholds • 233
Bulk Configuration Methods • xx, 19, 33
Bulk Configuration or Firmware Upgrade via DHCP/TFTP • 33, 321, 345, 550, 561
Bulk Configuration via SCP • 322, 324, 588
Bulk Configuration/Upgrade Procedure • xxi, 561, 563
Button-Type Locking Outlets • 668

C

Canceling the Power-On Process • 522
Cascading the PX via USB • 22, 30, 72, 73, 127, 133, 155, 607, 609, 610, 612, 613, 615, 618, 619

Certificate Signing Request • 193
Change Load Shedding State • 239, 253
Changing a User's Password • 465
Changing an Outlet's Default State • 460
Changing Default Thresholds • 305, 307
Changing HTTP(S) Settings • 141, 178
Changing Measurement Units • 471, 474
Changing Modbus/TCP Settings • 145
Changing SSH Settings • 144, 172
Changing Telnet Settings • 145
Changing the Cycling Power-Off Period • 215
Changing the Default Policy • 178, 179, 188, 189
Changing the Inlet Name • 462
Changing the LAN Duplex Mode • 426
Changing the LAN Interface Speed • 426
Changing the Modbus Configuration • 432
Changing the Modbus Port • 433
Changing the Outlet Name • 459
Changing the Outlet-Specific Cycling Power-Off Period • 215, 216
Changing the Overcurrent Protector Name • 463
Changing the PDU Name • 402
Changing the PDU-Defined Cycling Power-Off Period • 215, 217
Changing the Role(s) • 471
Changing the Sensor Description • 485
Changing the Sensor Name • 483
Changing the SSH Configuration • 429
Changing the SSH Port • 429
Changing the SSH Public Key • 472
Changing the Telnet Configuration • 428
Changing the Telnet Port • 429
Changing the UDP Port • 505
Changing Your Own Password • 473
Changing Your Password • 112
Checking Power Strip Status • 694
Checking RCM State and Current • 594
Checking RCM States on Phase II Models • 598, 599
Checking Server Monitoring States • 296
Checking the Accessibility of NTP Servers • 438
Checking the Branch Circuit Rating • 14
Checking the Internal Beeper State • 80, 105, 168
Circuit Breaker Orientation Limitation • 6, 8, 9, 10
Circuit Breakers • 100
Clearing Event Entries • 290
Clearing Event Log • 400
Clearing Information • 400
Clearing WLAN Log • xxi, 401
CLI Operations for RCM • 602
Closing a Local Connection • 367
Collapsing the Tree • 117
Combining Regular Asset Sensors • 55
Command History • 397
Commands for Environmental Sensors • 496
Commands for Inlet Pole Sensors • 493
Commands for Inlet Sensors • 491
Commands for Outlet Sensors • 489
Commands for Overcurrent Protector Sensors • 494
Compliance with IEC 62020 • 593, 601, 603
Components of an Event Rule • 237
config.txt • 551, 554, 556
Configuration Files • 550, 551, 561
Configuration or Firmware Upgrade with a USB Drive • xxi, 33, 321, 550, 560, 561
Configuring a PX on Dominion SX • 691
Configuring a Specific Rack Unit • 318
Configuring Data Push Settings • 164, 244
Configuring Environmental Sensors' Default Thresholds • 487
Configuring Environmental Sensors or Actuators • 92, 121, 297, 304, 307, 308
Configuring IP Protocol Settings • 410
Configuring IPv4 Parameters • 417
Configuring IPv6 Parameters • 421
Configuring NTP Server Settings • 361
Configuring Rack PDU Targets • 685
Configuring SMTP Settings • 163, 246, 247
Configuring SNMP Notifications • 282, 283, 295, 353
Configuring SNMP Settings • 143, 170
Configuring Temperature and Fan Thresholds • 121, 338
Configuring the Asset Sensor • 58, 93, 316
Configuring the Cascading Mode • 31, 506
Configuring the Feature Port • 152, 337
Configuring the Firewall • 178
Configuring the LHX/SHX • 336, 337
Configuring the PX • xx, 18, 135
Configuring the PX Device and Network • 401
Configuring the Serial Port • xx, 66, 154, 366
Configuring Users for Encrypted SNMP v3 • 351, 352
Configuring Webcam Storage • 258, 325, 331, 332, 333
Configuring Webcams • 325, 326, 328, 332

Connecting a DPX2 Sensor Package to DPX3 • xx, 45, 54
Connecting a DPX2 Sensor Package to DX • 44, 47, 48, 54
Connecting a GSM Modem • 65
Connecting a Locking Line Cord • 16, 69
Connecting a Logitech Webcam • 64, 115, 325
Connecting a PX PDU • 685, 691
Connecting a Rack PDU • 690
Connecting a Schroff LHX/SHX Heat Exchanger • 67, 152, 336
Connecting an Analog Modem • 66, 366
Connecting an External Beeper • xx, 66, 152
Connecting Asset Management Sensors • 55, 152, 164, 316, 697
Connecting Blade Extension Strips • 59
Connecting Composite Asset Sensors (AMS-Mx-Z) • 62
Connecting Environmental Sensor Packages • xx, 36, 297
Connecting External Equipment (Optional) • 36, 72
Connecting Regular Asset Sensors to the PX • xx, 57, 62
Connecting the PDU to a Power Source • 18
Connecting the PX to a Computer • xx, 3, 19, 584, 585
Connecting the PX to Your Network • 18, 22, 132, 133
Connection Port Functions • 72
Connection Ports • 71
Control Buttons • 75, 606
Controlling Actuators • 315
Copying the PX Configuration • 323
Creating a Certificate Signing Request • 193
Creating a New Attribute • 633
Creating a Role • 172, 175, 477, 639
Creating a Self-Signed Certificate • 195
Creating a User Profile • 109, 144, 169, 173, 174, 175, 176, 352, 464
Creating Actions • 65, 124, 238, 264, 287, 325
Creating an Event Rule • 66, 237
Creating Configuration Files via Mass Deployment Utility • 552, 559
Creating Firewall Rules • 178, 180
Creating Role-Based Access Control Rules • 188, 189
Creating Rules • 258
Customizing the Date and Time • xxi, 437

D

Daisy-Chain Limitations of Composite Asset Sensors • xx, 63
Dashboard Page • 541
Data for BTU Calculation • 681
Data Pane • 119
Date and Time Settings • 376
dcTrack • 695
dcTrack Overview • 696
Deassertion Hysteresis Example for Temperature Sensors • 677
Default Log Messages • xx, 187, 247, 268
Default Measurement Units • 376
Deleting a Firewall Rule • 444
Deleting a Monitored Device • 501
Deleting a Role • 177, 482
Deleting a Role-Based Access Control Rule • 456
Deleting a User Profile • 173, 473
Deleting an Event Rule or Action • 288
Deleting Authentication Server Settings • 205
Deleting Firewall Rules • 183
Deleting Ping Monitoring Settings • 296
Deleting Role-Based Access Control Rules • 192
Derating a Raritan Product • 533
Describing the Sensor's or Actuator's Location • 304, 306
Determining the SSH Authentication Method • xxi, 430
Determining the Time Setup Method • 435, 437
Device Info • 4, 18, 19, 78, 94
Device Management • 125
Device States and Icon Variations • 341, 342
devices.csv • 551, 554, 557, 558
DHCP IPv4 Configuration in Linux • 562, 580
DHCP IPv4 Configuration in Windows • 562, 563
DHCP IPv6 Configuration in Linux • 562, 582
DHCP IPv6 Configuration in Windows • 562, 573
Diagnostic Commands • 527
Dictionary File • 663
Different CLI Modes and Prompts • 365, 367, 369, 400, 401, 402, 438, 517, 519, 522, 527
Disabling an Inlet (for Multi-Inlet PDUs) • 228
Disabling External Authentication • 205
Disabling or Enabling Front Panel RCM Self-Test • 597, 599, 623

Disabling the Automatic Management Function • 302, 314, 409
Disconnecting a Locking Line Cord • 17
Displaying PDU Information • 126
Displaying the Asset Sensor Information • 320
Displaying the RCM Current • 599
Dominion KSX II • 689
Dominion KSX II, SX or SX II Configuration • xxi, 152, 689
Dominion KX II / III Configuration • xxi, 152, 684
Dominion SX • 691
Dominion SX and SX II • 691
Dominion SX II • 691
Dot-Matrix LCD Display • 73
Downloading Diagnostic Information • xxi, 335
Downloading Key and Certificate Files • 197
Downloading SNMP MIB • 143, 352, 353, 359, 601
DPX Sensor Packages • xx, 36, 37
DPX2 Sensor Packages • 36, 42
DPX3 Sensor Packages • xx, 36, 44
DX Sensor Packages • 36, 46, 257

E

EAP CA Certificate Example • 414, 416
Editing Authentication Server Settings • 205
Editing Firewall Rules • 182
Editing Ping Monitoring Settings • 296
Editing rciusergroup Attributes for User Members • 636
Editing Role-Based Access Control Rules • 191
Email and SMS Message Placeholders • xx, 246, 247, 253, 254, 278
Enabling and Disabling Schroff LHX/SHX Heat Exchanger Support • 153, 245, 255, 336, 337
Enabling and Editing the Security Banner • 187
Enabling Data Logging • 162
Enabling External and Local Authentication Services • 206
Enabling Front Panel Outlet Switching • 85, 87, 224, 613
Enabling IPv4 or IPv6 • 411
Enabling Login Limitations • 185, 330
Enabling or Disabling a User Profile • 467
Enabling or Disabling an Inlet (for Multi-Inlet PDUs) • 462
Enabling or Disabling Data Logging • 407
Enabling or Disabling EnergyWise • 504
Enabling or Disabling Front Panel Actuator Control • 457
Enabling or Disabling Front Panel Outlet Switching • 457
Enabling or Disabling Load Shedding • 518
Enabling or Disabling Modbus • 432
Enabling or Disabling Peripheral Device Auto Management • xxi, 409
Enabling or Disabling SNMP v1/v2c • 430
Enabling or Disabling SNMP v3 • 431
Enabling or Disabling SSH • 429
Enabling or Disabling Strong Passwords • 449
Enabling or Disabling Telnet • 428
Enabling or Disabling the Read-Only Mode • 433
Enabling or Disabling the Restricted Service Agreement • 445
Enabling or Disabling the Service Advertisement • 433
Enabling Password Aging • 186
Enabling Service Advertisement • 146, 433
Enabling SNMP • 143, 162, 351
Enabling Strong Passwords • 186
Enabling the Feature • 188
Enabling the Firewall • 178
Enabling the Front Panel Actuator Control • 89, 315
Enabling User Blocking • 184
EnergyWise Configuration Commands • 504
EnergyWise Settings • 391
Entering Configuration Mode • 367, 401, 416, 465, 473, 602
Entering Diagnostic Mode • 367, 526
Environmental Sensor Configuration Commands • 482
Environmental Sensor Default Thresholds • 387
Environmental Sensor Information • 377, 615
Environmental Sensor Package Information • 379
Environmental Sensor Threshold Information • 386
Environmental Sensors and Actuators • 297
Equipment Setup Worksheet • 14, 546
Event Log • 394
Event Rules and Actions • 143, 163, 168, 229, 237, 293, 353
Example • 436, 446, 465, 473, 515, 518

Ping Monitoring and SNMP Notifications • 294
Example - Actuator Naming • 500
Example - Creating a Role • 482
Example - Default Upper Thresholds for Temperature • 489
Example - Inlet Naming • 463
Example - OCP Naming • 463
Example - Outlet Naming • 461
Example - Ping Command • 529
Example - Power Cycling Specific Outlets • 522
Example - Server Settings Changed • 503
Example - Setting Up EnergyWise • 506
Example - Turning On a Specific Actuator • 524
Example 1 • 285
Example 1 - Asset Sensor LED Colors for Disconnected Tags • 513
Example 1 - Basic Security Information • 398
Example 1 - Combination of IP, Subnet Mask and Gateway Parameters • 515
Example 1 - Creating a User Profile • 476
Example 1 - Environmental Sensor Naming • 487
Example 1 - IPv4 Firewall Control Configuration • 458
Example 1 - Networking Mode • 434
Example 1 - PDU Naming • 409
Example 1 - Time Setup Method • 438
Example 1 - Upper Critical Threshold for a Temperature Sensor • 498
Example 2 • 285
Example 2 - Adding an IPv4 Firewall Rule • 458
Example 2 - Combination of Upper Critical and Upper Warning Settings • 516
Example 2 - Enabling Both IP Protocols • 434
Example 2 - In-Depth Security Information • 399
Example 2 - Modifying a User's Roles • 476
Example 2 - Outlet Sequence • 409
Example 2 - Primary NTP Server • 438
Example 2 - Rack Unit Naming • 513
Example 2 - Sensor Threshold Selection • 487
Example 2 - Warning Thresholds for Inlet Sensors • 498
Example 3 • 286
Example 3 - Basic PDU Information • 399
Example 3 - Combination of SSID and PSK Parameters • 516
Example 3 - Default Measurement Units • 476
Example 3 - Outlet Sequence Delay • 409
Example 3 - Upper Thresholds for Overcurrent Protector Sensors • 498
Example 3 - User Blocking • 458
Example 3 - Wireless Authentication Method • 434
Example 4 - Adding an IPv4 Role-based Access Control Rule • 459
Example 4 - Combination of Upper Critical, Upper Warning and Lower Warning Settings • 517
Example 4 - In-Depth PDU Information • 400
Example 4 - Non-Critical Outlets • 410
Example 4 - Static IPv4 Configuration • 434
Examples • 398, 409, 434, 438, 457, 475, 486, 497, 513
Existing Roles • 390
Existing User Profiles • 376, 389
Expanding a Blade Extension Strip • 319
Expanding the Tree • 115, 208, 209, 211, 212, 214, 216, 221, 222, 223, 225, 227, 229, 230, 232
External Beeper • 238, 242

F

Feature RJ-45 Port Pinouts • 544
Filling Out the Equipment Setup Worksheet • 14
Firewall Control • 439
Firmware Update via SCP • 345, 587
Firmware Update via Web Interface • 344, 587
Firmware Upgrade • 323, 343
Firmware Upgrade via USB • 345, 550, 560
Flexible Cord Installation Instructions • 532
Flexible Cord Selection • 532
Forcing a Password Change • 467
Forcing HTTPS Encryption • 178, 193
Forcing the Device Detection Mode • xxi, 514
Format of the • 664
From LDAP/LDAPS • 632
From Microsoft Active Directory • 632
Front Panel Operations for RCM • 78, 597, 621
Full Disaster Recovery • 347
Fuse • 102
Fuse Replacement on 1U Models • 103
Fuse Replacement on Zero U Models • 102
fwupdate.cfg • 551, 553, 556, 558, 560

G

Gathering the External Authentication Information • 198
Gathering the LDAP Information • 199
Gathering the RADIUS Information • 199

H

Help Command • 368
History Buffer Length • 397
How to Use the Calendar • 148

I

Identifying Cascaded Devices • 32, 126, 127
Identifying Environmental Sensors and Actuators • 297, 298, 302
Identifying Sensor or Actuator Channels • 301
Idle Timeout • 448
Initial Network Configuration via CLI • 19, 20, 24, 117, 584, 585
Inlet • 69, 78, 82
Inlet and Overcurrent Protector Management • 224
Inlet Configuration Commands • 461
Inlet Information • 374, 609
Inlet Pole Sensor Threshold Information • 384
Inlet Sensor Threshold Information • 383
In-Line Monitor Unused Channels • 534
In-Line Monitors • 531
In-Line Monitor's Web Interface • 540
Installation and Configuration • 13
Installing a CA-Signed Certificate • 195
Installing Cable Retention Clips on Outlets (Optional) • 34
Installing Cable Retention Clips on the Inlet (Optional) • 14
Installing Existing Key and Certificate Files • 197
Installing the USB-to-Serial Driver (Optional) • 20, 21, 359
Integration • 684
Internal Beeper • 239, 255
Introduction • 1
Introduction to the Web Interface • 113
IP Configuration • 370
IPv4 Address • 4, 18, 19, 611

L

LAN Interface Settings • 370
Layout • 360
LCD Message for RCM Critical State • 597
LDAP Configuration Illustration • 204, 624
Listing TCP Connections • 335
Load Shedding Configuration Commands • 517
Load Shedding Settings • 390
Locking Outlets and Cords • 34, 666
Log an Event Message • 239, 243
Logging in to CLI • 364, 585
Logging in to the Web Interface • 109
Logging out of CLI • 530
Login • xx, 19, 20, 109, 170
Login Limitation • 446
Logout • 112
Lowercase Character Requirement • 450

M

MAC Address • 612
Main Menu • 74, 77, 598, 599
Make a Power Association • 688
Managing Environmental Sensors or Actuators • 46, 297, 302
Managing Event Logging • 289
Managing Firewall Rules • 440
Managing Role-Based Access Control Rules • 453
Managing the Schroff LHX/SHX Heat Exchanger • 67, 152, 336
Managing the Snapshots Saved to PX • 332
Marking All Outlets • 221
Marking an Outlet • 221
Matching the Position • xxi, 298, 299
Matching the Serial Number • 298
Maximum Ambient Operating Temperature • 14, 543
Maximum Password History • 451
Maximum Password Length • 449
Menus • 114
Microsoft Network Policy Server • 639
Minimum Password Length • 449
Mixing Diverse Sensor Types • xx, 49, 50
Modifying a Firewall Rule • 442
Modifying a Monitored Device's Settings • 501
Modifying a Role • 172, 173, 176, 480

Modifying a Role-Based Access Control Rule • 454
Modifying a User Profile • 112, 173, 176, 464
Modifying a User's Personal Data • 466
Modifying an Action • 144, 288
Modifying an Event Rule • 286
Modifying Firewall Control Parameters • 439
Modifying IPv4 Settings • 136
Modifying IPv6 Settings • 137
Modifying Network Interface Settings • 132
Modifying Network Service Settings • 141, 363, 365
Modifying Network Settings • 117, 135, 146, 626
Modifying Role-Based Access Control Parameters • 452
Modifying SNMPv3 Settings • 468
Modifying the Network Configuration • 24, 131
Monitoring All Outlets • 208
Monitoring an Outlet • 209
Monitoring Overcurrent Protectors • 226
Monitoring Server Accessibility • 292
Monitoring the Inlet • 225
Monitoring the LHX/SHX • 336, 339
Monitoring Total Active Energy or Power • 167
More Information • 119
More Information about AD or RADIUS Configuration • 204
Mounting 1U or 2U Models • 11
Mounting Zero U Models Using Button Mount • 8
Mounting Zero U Models Using Claw-Foot Brackets • 9
Mounting Zero U Models Using L-Brackets • 6
Mounting Zero U Models Using Two Rear Buttons • 10
Multi-Command Syntax • 440, 446, 448, 449, 453, 464, 466, 468, 471, 474, 487, 489, 491, 493, 494, 496, 499, 501, 515

N

Naming a Rack Unit • 510
Naming an Asset Sensor • 507
Naming Outlets • 208
Naming Overcurrent Protectors • 225
Naming the Inlet • 225
Naming the PDU • 115, 117, 131, 165, 166, 167, 168, 207, 211, 214, 216, 217, 218, 219, 220, 221, 222, 231, 235, 305, 314
Naming the Rack PDU (Port Page for Power Strips) • 686, 691
Network Configuration • 370
Network Configuration Commands • 410
Network Diagnostics • 334
Network Service Settings • 371
Network Troubleshooting • 334, 526
Networking Mode • 371
Non-Windows RADIUS Server • 639, 663
Numeric Character Requirement • 450

O

OCPs • 78, 84
Operating Hours • 342
Operating the Character LCD Display • 607
Operating the Dot-Matrix LCD Display • xx, 75, 76, 77, 79, 100
Outlet Configuration Commands • 459
Outlet Information • 373, 607
Outlet Management • 206
Outlet Monitoring • 208
Outlet Page • 541
Outlet Pole Sensor Threshold Information • 382
Outlet Relay Behavior in Latching and Non-Latching Mode • 207
Outlet Sensor Threshold Information • 381
Outlet Switching • 210, 613
Outlets • 70, 78, 85
Overcurrent Protector Configuration Commands • 463
Overcurrent Protector Information • 100, 375, 610
Overcurrent Protector Sensor Threshold Information • 385
Overriding DHCP-Assigned NTP Servers • 436, 438
Overriding the IPv4 DHCP-Assigned DNS Server • 419, 420
Overriding the IPv6 DHCP-Assigned DNS Server • 423, 424
Overview • 531
Overview of the Cascading Modes • xx, 155, 157
Overview of the Character LCD Display • 605, 607

P

Package Contents • 1, 13
Panel Components • 68
Password Aging • 447
Password Aging Interval • 447

PDU • xx, 78, 80
PDU Configuration • 168, 372
PDU Configuration Commands • 402
PDView App for Viewing the PX • xxi, 678
Peripherals • 78, 89, 315
Pinging a Host • 334
Plug Selection • 533
Port Forwarding Examples • 111, 156, 159, 160
Port Number Syntax • 156, 158, 160
Power Control • 87, 210, 691, 693
Power Control Operations • 519
Power Cycling the Outlet(s) • 521
Power IQ Configuration • 694
Preparing the Installation Site • 14
Product Models • 1
Push Out Sensor Readings • 164, 239, 244
PX Explorer Pane • 114
PX Models with Residual Current Monitoring • 591, 621
PX3 Latching Relay Behavior • 206, 403, 404
PX3 Phase I LCD Display • 68, 605
PX3-3000 Series • 70
PX3-4000 Series • 70
PX3-5000 Series • 70

Q

Querying Available Parameters for a Command • 368, 369
Querying DNS Servers • 527
Quitting Configuration Mode • 402, 446
Quitting Diagnostic Mode • 527

R

Rack Unit Configuration • 510
Rack Unit Settings of an Asset Sensor • 392
Rackmount Safety Guidelines • 5
Rack-Mounting the PDU • 5
RADIUS Configuration Illustration • 204, 639
Raritan Training Website • 683
RCM Critical State Alarm • 595
RCM Current Sensor • 591
RCM Information • xxi, 597, 621
RCM Residual Current and State Objects • 601
RCM Self-Test • 594
RCM SNMP Operations • 601
RCM State Sensor • 592, 594
RCM Trap • 601
Rebooting the PX Device • 166
Receptacle Selection • 533
Record Snapshots to Webcam Storage • 239, 257
Reliability Data • 397
Reliability Error Log • 397
Remembering User Names and Passwords • 112
Replaceable Controller • xx, 68, 106
Request LHX/SHX Maximum Cooling • 239, 245
Requesting Maximum Cooling for an SHX-30 • 343
Reserving IP Addresses in Windows DHCP Servers • 669
Reset Button • 99
Resetting Active Energy Readings • 525
Resetting All Active Energy Readings • 166, 167, 228, 235
Resetting Inlet Active Energy Readings • 167, 227
Resetting Outlet Active Energy Readings • 167, 223
Resetting the Button-Type Circuit Breaker • 100
Resetting the Handle-Type Circuit Breaker • 101
Resetting the PX • 524
Resetting to Factory Defaults • 99, 526, 584
Restarting the PDU • 525
Restricted Service Agreement • 444
Retrieving Energy Usage • 362
Retrieving Previous Commands • 529
Retrieving Software Packages Information • 347
Returning User Group Information • 632
Role Configuration Commands • 477
Role of a DNS Server • 141, 626
Role-Based Access Control • 451
Running RCM Self-Test • 598, 599, 601, 604

S

Safety Guidelines • ii
Safety Instructions • iii, 14, 531
Sample Environmental-Sensor-Level Event Rule • 284
Sample Event Rules • 281
Sample Inlet-Level Event Rule • 283
Sample Outlet-Level Event Rule • 282
Sample PDU-Level Event Rule • 281

Saving Snapshots • 325, 328, 331, 332
Saving the PX Configuration • 322, 555
Scheduling an Action • 164, 244, 263, 268, 596
Scheduling RCM Self-Test • 596
SecureLock™ Outlets and Cords • 666
Security Configuration Commands • 439
Security Settings • 388
Selecting IPv4 or IPv6 Addresses • 411
Selecting the Internet Protocol • 3, 135, 136, 137
Send a Snapshot via Email • 239, 245
Send an SNMP Notification • 239, 247
Send EMail • 239, 246, 266, 268
Send Sensor Report • 239, 251, 267
Send Sensor Report Example • xx, 265
Send SMS Message • 239, 254
Sending Snapshots or Videos in an Email or Instant Message • 292, 325, 327, 329
Sensor RJ-45 Port Pinouts • 543
Sensor Threshold Configuration Commands • 489
Sensor Threshold Settings • 229, 305, 671
Serial Port Configuration Commands • 513
Serial Port Settings • 391
Serial RS-232 Port Pinouts • 543
Server Reachability Configuration Commands • 500
Server Reachability Information • 395
Server Reachability Information for a Specific Server • 396
Setting an LED Color for a Rack Unit • 511, 512
Setting an LED Mode for a Rack Unit • 511, 512
Setting an Outlet's Cycling Power-Off Period • 461
Setting an Outlet's Thresholds • 229, 230
Setting an Overcurrent Protector's Thresholds • 232, 233
Setting Asset Sensor LED Colors • 93, 317
Setting Data Logging • 162, 407
Setting Data Logging Measurements Per Entry • 407
Setting Default Measurement Units • 151, 165, 174, 471, 474
Setting EAP Parameters • 414
Setting Front Panel RCM Self-Test • 604
Setting Inlet Thresholds • 232
Setting IPv4 Static Routes • 421
Setting IPv6 Static Routes • 425
Setting LAN Interface Parameters • 425
Setting LED Colors for Connected Tags • 509, 511, 512
Setting LED Colors for Disconnected Tags • 510, 511, 512
Setting Network Service Parameters • 426
Setting Non-Critical Outlets and Load Shedding Mode • 220, 253, 406
Setting NTP Parameters • 435, 438
Setting Power Thresholds • 121, 206, 224, 229, 361
Setting RCM Current Thresholds • 592, 595, 596, 602
Setting RCM Thresholds • 601
Setting the Alarmed to Normal Delay for DX-PIR • 486
Setting the Authentication Method • 412
Setting the Automatic Daylight Savings Time • 437
Setting the Baud Rates • xxi, 514
Setting the BSSID • 417
Setting the Cascading Mode • 3, 30, 31, 95, 128, 155, 157, 159
Setting the Date and Time • 147, 361
Setting the Default Outlet State • 213
Setting the EnergyWise Configuration • 168
Setting the History Buffer Length • 515
Setting the HTTP Port • 427
Setting the HTTPS Port • 428
Setting the Initialization Delay • 207, 217, 406
Setting the Inrush Guard Delay • 218
Setting the Inrush Guard Delay Time • 405
Setting the IPv4 Address • 418
Setting the IPv4 Configuration Mode • 418
Setting the IPv4 Gateway • 419
Setting the IPv4 Preferred Host Name • 418
Setting the IPv4 Primary DNS Server • 419
Setting the IPv4 Secondary DNS Server • 420
Setting the IPv4 Subnet Mask • 419
Setting the IPv6 Address • 423
Setting the IPv6 Configuration Mode • 422
Setting the IPv6 Gateway • 423
Setting the IPv6 Preferred Host Name • 422
Setting the IPv6 Primary DNS Server • 423
Setting the IPv6 Secondary DNS Server • 424
Setting the LCD Display's Default View • 74, 151
Setting the LED Operation Mode • 511
Setting the Networking Mode • 410
Setting the Outlet Initialization Delay • 406
Setting the Outlet Power-On Sequence • 219, 403

Setting the Outlet Power-On Sequence Delay • 404
Setting the Outlet Relay Behavior • 207, 403, 405, 406
Setting the Outlet-Specific Default State • 207, 214
Setting the Outlet-Specific Power-On Delay • 220
Setting the PDU-Defined Cycling Power-Off Period • 405, 461
Setting the PDU-Defined Default Outlet State • 404, 460
Setting the PDU-Defined Default State • 207, 214, 215
Setting the Polling Interval • 505
Setting the PSK • 413
Setting the Registry to Permit Write Operations to the Schema • 633
Setting the SNMP Configuration • 430
Setting the SNMP Read Community • 431
Setting the SNMP Write Community • 431
Setting the SSID • 412
Setting the sysContact Value • 431
Setting the sysLocation Value • 432
Setting the sysName Value • 432
Setting the Time Zone • 361, 436
Setting the X Coordinate • 484
Setting the Y Coordinate • 484
Setting the Z Coordinate • 408, 485
Setting the Z Coordinate Format • 304, 305
Setting the Z Coordinate Format for Environmental Sensors • 408, 485, 500
Setting Thresholds for Multiple Sensors • 305, 308
Setting Thresholds for Total Active Energy or Power • 235
Setting Up a TLS Certificate • 178, 192
Setting Up an LHX/SHX • 338
Setting Up External Authentication • 141, 178, 198
Setting Up Role-Based Access Control Rules • 188
Setting Up Roles • 112, 169, 172, 175
Setting Up User Login Controls • 184
Setting Up Your Preferred Measurement Units • 151, 173, 174
Setting Wireless Parameters • 412
Setup Button • 117
Showing an Outlet's Information • 85, 88
Showing Information • 369
Showing Network Connections • 527
Showing Residual Current Monitor Information • 602
Showing the Firmware Upgrade Progress • 99
Single Login Limitation • 447
Snapshot Storage • 331
SNMP Gets and Sets • 358
SNMP Sets and Thresholds • 361
SNMPv2c Notifications • 144, 354
SNMPv3 Notifications • 144, 356
Sorting Firewall Rules • 183
Sorting Role-Based Access Control Rules • 191
Sorting the Access Order • 204
Special Character Requirement • 451
Specifications • 5, 543
Specifying Non-Critical Outlets • 390, 406
Specifying the Agreement Contents • 445
Specifying the Asset Sensor Orientation • 509
Specifying the CC Sensor Type • 483
Specifying the Device Altitude • 165, 408
Specifying the EnergyWise Domain • 504
Specifying the EnergyWise Secret • 505
Specifying the Number of Rack Units • 507
Specifying the Primary NTP Server • 435
Specifying the Rack Unit Numbering Mode • 508
Specifying the Rack Unit Numbering Offset • 508
Specifying the Secondary NTP Server • 435
States of Managed Actuators • 90, 313
States of Managed Sensors • 80, 90, 310
States of Unmanaged Sensors or Actuators • xxi, 313, 314
Static Route Examples • 136, 137, 139
Status Bar • 117
Step A
  Add Your PX as a RADIUS Client • 640
Step A. Determine User Accounts and Roles • 624
Step B
  Configure Connection Request Policies • 643
Step B. Configure User Groups on the AD Server • 625
Step by Step Flexible Cord Installation • 534
Step C
  Configure a Vendor-Specific Attribute • 658
Step C. Configure LDAP Authentication on the PX Device • 626
Step D. Configure Roles on the PX Device • 628

Stopping the Power-On Sequence • 213
Strong Passwords • 449
Supported Maximum DPX Sensor Distances • 37, 41
Supported Web Browsers • xx, 108
Supported Wireless LAN Configuration • 24
Switch LHX/SHX • 239, 255
Switch Outlets • 240, 256
Switch Peripheral Actuator • 240, 257
Switching an Outlet • 212
Switching Multiple or All Outlets • 211, 212, 213
Switching Off an Actuator • 523
Switching On an Actuator • 523
Syslog Message • 239, 250
System and USB Requirements • 550, 551

T

Testing the Network Connectivity • 528
Testing the Server Connection • 204
TFTP Requirements • 562
The PX MIB • 359
The Yellow- or Red-Highlighted Sensors • 76, 79, 89, 98, 120, 123, 124, 209, 210, 226, 227, 229, 309, 340
Thresholds and Sensor States • 672
Time Configuration Commands • 434
Tracing the Network Route • 334
Tracing the Route • 529
Truncated Data in the Web Interface • 682
Turning Off the Outlet(s) • 520
Turning On the Outlet(s) • 519
Turning Outlets On/Off and Cycling Power • 688, 691
Turning the LHX/SHX On or Off • 336, 342

U

Unbalanced Current Calculation • 668
Unblocking a User • 184, 524
Unmanaging Environmental Sensors or Actuators • xxi, 46, 303, 313
Unpacking the Product and Components • 13
Updating the Asset Sensor Firmware • 347
Updating the LDAP Schema • xxi, 632
Updating the PX Firmware • 30, 155, 344
Updating the Schema Cache • 636
Uppercase Character Requirement • 450
USB Wireless LAN Adapters • 23, 24, 30, 128
USB-Cascaded Device's Position • 619
USB-Cascading Configuration Commands • 506
USB-Cascading Configuration Information • 391
User Blocking • 448
User Configuration Commands • 463
User Management • 169
Using an Optional DPX3-ENVHUB4 Sensor Hub • xx, 49
Using an Optional DPX-ENVHUB2 cable • 39
Using an Optional DPX-ENVHUB4 Sensor Hub • 38
Using Default Thresholds • 486
Using SNMP • 345, 350
Using the CLI Command • 526, 585
Using the Command Line Interface • 141, 306, 363, 585, 602
Using the PDU • 68
Using the Reset Button • 584
Using the Web Interface • 108, 540

V

Viewing Connected Users • 291, 327, 329
Viewing Details • 340
Viewing Firmware Update History • 346
Viewing Sensor or Actuator Data • 309
Viewing the Dashboard • 123
Viewing the Local Event Log • 163, 200, 250, 289
Viewing the Summary • 340, 341
Viewing the Wireless LAN Diagnostic Log • 290
Viewing Webcam Snapshots or Videos • 65, 327

W

Warning Icon • 119
Ways to Probe Existing User Profiles • 682
Web Interface Operations for RCM • 594
Webcam Management • 325
What's New in the PX User Guide • xx
Windows NTP Server Synchronization Solution • 148, 150
Wired Network Settings • 132
Wireless Configuration • 371
Wireless LAN Diagnostic Log • 395
Wireless Network Settings • 133
Wiring of 3-Phase In-Line Monitors • 532, 534
With an Analog Modem • 366
With HyperTerminal • 364, 524

With SSH or Telnet • 365

Z

Zero U Connection Ports • 71
Zero U Models' Relocatable Inlet • 69
Zero U Products • 2

U.S./Canada/Latin America

Monday - Friday
8 a.m. - 6 p.m. ET
Phone: 800-724-8090 or 732-764-8886
For CommandCenter NOC: Press 6, then Press 1
For CommandCenter Secure Gateway: Press 6, then Press 2
Fax: 732-764-8887
Email for CommandCenter NOC: tech-ccnoc@raritan.com
Email for all other products: tech@raritan.com

China

Beijing
Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +86-10-88091890

Shanghai
Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +86-21-5425-2499

GuangZhou
Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +86-20-8755-5561

India

Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +91-124-410-7881

Japan

Monday - Friday
9:30 a.m. - 5:30 p.m. local time
Phone: +81-3-5795-3170
Email: support.japan@raritan.com

Europe

Europe
Monday - Friday
8:30 a.m. - 5 p.m. GMT+1 CET
Phone: +31-10-2844040
Email: tech.europe@raritan.com

United Kingdom
Monday - Friday
8:30 a.m. to 5 p.m. GMT
Phone +44(0)20-7090-1390

France
Monday - Friday
8:30 a.m. - 5 p.m. GMT+1 CET
Phone: +33-1-47-56-20-39

Germany
Monday - Friday
8:30 a.m. - 5:30 p.m. GMT+1 CET
Phone: +49-20-17-47-98-0
Email: rg-support@raritan.com

Melbourne, Australia

Monday - Friday
9:00 a.m. - 6 p.m. local time
Phone: +61-3-9866-6887

Taiwan

Monday - Friday
9 a.m. - 6 p.m. GMT -5 Standard -4 Daylight
Phone: +886-2-8919-1333
Email: support.apac@raritan.com