



# Raritan PXE

User Guide  
Release 3.2.10

---

Copyright © 2016 Raritan, Inc.

PXE-0E-v3.2.10-E

March 2016

255-80-0008-00

---

# 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.

#### FCC Information

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

#### VCCI Information (Japan)

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

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

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



### Warning

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

### CAUTION:



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



SecureLock™

# Contents

<b>Safety Guidelines</b>	<b>ii</b>
<hr/>	
<b>Safety Instructions</b>	<b>iii</b>
<hr/>	
<b>What's New in the PXE User Guide</b>	<b>xv</b>
<hr/>	
<b>Chapter 1 Introduction</b>	<b>1</b>
<hr/>	
Product Models .....	1
Package Contents.....	1
Zero U Products.....	1
1U Products .....	1
APIPA and Link-Local Addressing .....	2
 <b>Chapter 2 Rack-Mounting the PDU</b>	 <b>4</b>
<hr/>	
Rackmount Safety Guidelines .....	4
Circuit Breaker Orientation Limitation .....	4
Mounting 1U Models Using L-Brackets and Buttons .....	5
Mounting Zero U Models Using Two Rear Buttons .....	6
Mounting Zero U Models Using L-Brackets and Buttons.....	8
 <b>Chapter 3 Installation and Configuration</b>	 <b>10</b>
<hr/>	
Before You Begin .....	10
Unpacking the Product and Components.....	10
Preparing the Installation Site.....	10
Filling Out the Equipment Setup Worksheet .....	11
Checking the Branch Circuit Rating.....	11
Connecting the PDU to a Power Source .....	11
Configuring the PXE .....	11
Installing the USB-to-Serial Driver (Optional).....	13
Connecting the PXE to a Computer .....	14
Connecting the PXE to Your Network .....	15

Initial Network Configuration via CLI .....	16
Bulk Configuration Methods.....	20
Installing Cable Retention Clips on Outlets (Optional) .....	20

## **Chapter 4 Connecting Environmental Sensor Packages 22**

DPX Sensor Packages .....	23
Using an Optional DPX-ENVHUB4 Sensor Hub .....	24
Using an Optional DPX-ENVHUB2 cable.....	26
Supported Maximum DPX Sensor Distances.....	28
DPX2 Sensor Packages .....	29
DPX3 Sensor Packages .....	31
Connecting a DPX2 Sensor Package to DPX3 .....	32
DX Sensor Packages.....	34
Connecting a DPX2 Sensor Package to DX .....	35
Using an Optional DPX3-ENVHUB4 Sensor Hub .....	36
Mixing Diverse Sensor Types .....	38

## **Chapter 5 Using the PDU 42**

Panel Components .....	42
Power Cord.....	42
Outlets .....	42
Connection Ports .....	43
LED Display .....	44
Reset Button .....	47
Circuit Breakers .....	47
Resetting the Button-Type Circuit Breaker.....	47
Resetting the Handle-Type Circuit Breaker .....	48

## **Chapter 6 Using the Web Interface 50**

Supported Web Browsers .....	50
Logging in to the Web Interface.....	51
Login.....	51
Changing Your Password.....	53
Remembering User Names and Passwords .....	54
Logout .....	54
Introduction to the Web Interface.....	55
Menus .....	56
PX Explorer Pane .....	56
Setup Button .....	58
Status Bar .....	58
Add Page Icon .....	59
Data Pane.....	60
More Information .....	60
Viewing the Dashboard.....	64
Alerted Sensors .....	64

Alarms List .....	65
Device Management .....	66
Displaying PDU Information .....	67
Naming the PDU .....	68
Modifying the Network Configuration .....	68
Modifying Network Service Settings .....	76
Setting the Date and Time .....	82
Setting Default Measurement Units .....	86
Specifying the Device Altitude .....	86
Setting Data Logging .....	87
Configuring SMTP Settings .....	88
Rebooting the PXE Device .....	89
Resetting All Active Energy Readings .....	90
Internal Beeper State .....	90
Setting the EnergyWise Configuration .....	90
User Management .....	91
Creating a User Profile .....	91
Modifying a User Profile .....	94
Deleting a User Profile .....	95
Setting Up Your Preferred Measurement Units .....	96
Setting Up Roles .....	96
Creating a Role .....	97
Modifying a Role .....	97
Deleting a Role .....	99
Forcing HTTPS Encryption .....	99
Access Security Control .....	99
Configuring the Firewall .....	99
Setting Up User Login Controls .....	106
Setting Up Role-Based Access Control Rules .....	110
Setting Up a TLS Certificate .....	114
Certificate Signing Request .....	115
Creating a Self-Signed Certificate .....	117
Installing Existing Key and Certificate Files .....	119
Downloading Key and Certificate Files .....	119
Setting Up External Authentication .....	120
Gathering the External Authentication Information .....	120
Adding Authentication Servers .....	122
Sorting the Access Order .....	126
Testing the Server Connection .....	126
Editing Authentication Server Settings .....	127
Deleting Authentication Server Settings .....	127
Disabling External Authentication .....	127
Enabling External and Local Authentication Services .....	128
Outlet Management .....	128
Naming Outlets .....	128
Checking Outlet-Specific Data .....	129
Inlet and Overcurrent Protector Management .....	129
Naming the Inlet .....	130
Monitoring the Inlet .....	130
Naming Overcurrent Protectors .....	131
Resetting Inlet Active Energy Readings .....	131
Disabling an Inlet (for Multi-Inlet PDUs) .....	132



Setting Power Thresholds.....	133
Setting Inlet Thresholds.....	133
Event Rules and Actions.....	135
Components of an Event Rule.....	135
Creating an Event Rule.....	135
Sample Event Rules.....	166
A Note about Infinite Loop.....	168
Modifying an Event Rule.....	168
Modifying an Action.....	170
Deleting an Event Rule or Action.....	170
A Note about Untriggered Rules.....	171
Managing Event Logging.....	171
Viewing the Local Event Log.....	171
Clearing Event Entries.....	172
Viewing Connected Users.....	172
Monitoring Server Accessibility.....	173
Adding IT Devices for Ping Monitoring.....	174
Editing Ping Monitoring Settings.....	176
Deleting Ping Monitoring Settings.....	177
Checking Server Monitoring States.....	177
Environmental Sensors and Actuators.....	178
Identifying Environmental Sensors and Actuators.....	179
Managing Environmental Sensors or Actuators.....	182
Configuring Environmental Sensors or Actuators.....	184
Viewing Sensor or Actuator Data.....	189
Unmanaging Environmental Sensors or Actuators.....	193
Disabling the Automatic Management Function.....	194
Controlling Actuators.....	195
Bulk Configuration.....	196
Saving the PXE Configuration.....	197
Copying the PXE Configuration.....	198
Backup and Restore of PXE Device Settings.....	199
Network Diagnostics.....	200
Pinging a Host.....	200
Tracing the Network Route.....	201
Listing TCP Connections.....	201
Downloading Diagnostic Information.....	201
Firmware Upgrade.....	202
Updating the PXE Firmware.....	202
Viewing Firmware Update History.....	204
Full Disaster Recovery.....	204
Accessing the Help.....	204
Retrieving Software Packages Information.....	205
Browsing through the Online Help.....	205

## Chapter 7 Using SNMP 207

Enabling SNMP.....	207
Configuring Users for Encrypted SNMP v3 .....	208
Configuring SNMP Notifications .....	209
SNMPv2c Notifications .....	210
SNMPv3 Notifications.....	212
SNMP Gets and Sets.....	214
The PEX MIB.....	215
A Note about Enabling Thresholds.....	217

## Chapter 8 Using the Command Line Interface 218

About the Interface.....	218
Logging in to CLI.....	219
With HyperTerminal.....	219
With SSH or Telnet.....	220
Different CLI Modes and Prompts .....	221
Closing a Local Connection.....	221
Logging out of CLI.....	221
Help Command .....	222
Querying Available Parameters for a Command .....	223
Showing Information .....	223
Network Configuration .....	224
PDU Configuration.....	226
Outlet Information .....	226
Inlet Information.....	227
Overcurrent Protector Information .....	228
Date and Time Settings .....	229
Default Measurement Units .....	229
Environmental Sensor Information .....	230
Actuator Information .....	231
Environmental Sensor Package Information .....	232
Inlet Sensor Threshold Information .....	233
Inlet Pole Sensor Threshold Information .....	234
Environmental Sensor Threshold Information.....	236
Environmental Sensor Default Thresholds.....	237
Security Settings.....	238
Existing User Profiles .....	239
Existing Roles.....	240
EnergyWise Settings .....	240
Event Log.....	241
Server Reachability Information .....	242
Command History.....	243
History Buffer Length.....	243
Reliability Data.....	243
Reliability Error Log .....	244
Examples.....	244

Clearing Information.....	246
Clearing Event Log .....	246
Configuring the PXE Device and Network .....	247
Entering Configuration Mode.....	247
Quitting Configuration Mode.....	247
PDU Configuration Commands .....	248
Network Configuration Commands.....	251
Time Configuration Commands.....	269
Checking the Accessibility of NTP Servers .....	273
Security Configuration Commands.....	274
Outlet Configuration Commands .....	293
Inlet Configuration Commands .....	293
Overcurrent Protector Configuration Commands .....	295
User Configuration Commands .....	295
Role Configuration Commands .....	309
Environmental Sensor Configuration Commands .....	314
Configuring Environmental Sensors' Default Thresholds.....	319
Sensor Threshold Configuration Commands .....	321
Actuator Configuration Commands .....	328
Server Reachability Configuration Commands .....	329
EnergyWise Configuration Commands .....	333
Setting the History Buffer Length.....	335
Multi-Command Syntax .....	335
Actuator Control Operations .....	336
Switching On an Actuator .....	337
Switching Off an Actuator .....	337
Example - Turning On a Specific Actuator .....	338
Unblocking a User.....	338
Resetting the PXE.....	338
Restarting the PDU.....	339
Resetting Active Energy Readings .....	339
Resetting to Factory Defaults .....	340
Network Troubleshooting .....	340
Entering Diagnostic Mode .....	340
Quitting Diagnostic Mode .....	340
Diagnostic Commands .....	341

## Contents

Retrieving Previous Commands .....	343
Automatically Completing a Command.....	343

## **Appendix A Specifications 345**

---

Maximum Ambient Operating Temperature .....	345
Sensor RJ-12 Port Pinouts .....	345
RS-485 Port Pinouts .....	345

## **Appendix B Equipment Setup Worksheet 347**

---

## **Appendix C Bulk Configuration or Firmware Upgrade via DHCP/TFTP 351**

---

Bulk Configuration/Upgrade Procedure .....	351
Configuration Files .....	352
fwupdate.cfg .....	354
config.txt .....	357
devices.csv .....	359
Creating Configuration Files via Mass Deployment Utility .....	360

TFTP Requirements.....	361
DHCP IPv4 Configuration in Windows.....	361
DHCP IPv6 Configuration in Windows.....	371
DHCP IPv4 Configuration in Linux.....	378
DHCP IPv6 Configuration in Linux.....	380

## Appendix D Resetting to Factory Defaults 382

Using the CLI Command .....	382
-----------------------------	-----

## Appendix E Available SCP Commands 384

Firmware Update via SCP .....	384
Bulk Configuration via SCP .....	385
Backup and Restore via SCP .....	386

## Appendix F LDAP Configuration Illustration 388

Step A. Determine User Accounts and Roles.....	388
Step B. Configure User Groups on the AD Server .....	389
Step C. Configure LDAP Authentication on the PXE Device .....	390
Step D. Configure Roles on the PXE Device.....	392

## Appendix G Updating the LDAP Schema 396

Returning User Group Information.....	396
From LDAP/LDAPS .....	396
From Microsoft Active Directory .....	396
Setting the Registry to Permit Write Operations to the Schema .....	397
Creating a New Attribute.....	397
Adding Attributes to the Class .....	398
Updating the Schema Cache.....	400
Editing rcigroup Attributes for User Members.....	400

## Appendix H RADIUS Configuration Illustration 403

Microsoft Network Policy Server.....	403
Step A: Add Your PXE as a RADIUS Client.....	404
Step B: Configure Connection Request Policies.....	407
Step C: Configure a Vendor-Specific Attribute.....	422
AD-Related Configuration.....	424
Non-Windows RADIUS Server.....	427
Dictionary File.....	427
Format of the "string".....	428

## Appendix I Additional PXE Information 430

---

MAC Address .....	430
Locking Outlets and Cords .....	430
SecureLock™ Outlets and Cords .....	431
Button-Type Locking Outlets .....	432
Unbalanced Current Calculation .....	433
PDView App for Viewing the PXE .....	434
Altitude Correction Factors .....	437
Raritan Training Website .....	437
Truncated Data in the Web Interface .....	438
Reserving IP Addresses in Windows DHCP Servers .....	438
Sensor Threshold Settings .....	440
Thresholds and Sensor States .....	441
"To Assert" and Assertion Timeout .....	443
"To De-assert" and Deassertion Hysteresis .....	445
Ways to Probe Existing User Profiles .....	447
Schroff LHX/SHX and USB Cascading Not Supported .....	448

## Appendix J Integration 449

---

Power IQ Configuration .....	449
dcTrack .....	449
dcTrack Overview .....	450

## Index 451

---

# What's New in the PXE User Guide

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

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

***APIPA and Link-Local Addressing*** (on page 2)

***Configuring the PXE*** (on page 11)

***Connecting the PXE to a Computer*** (on page 14)

***Bulk Configuration Methods*** (on page 20)

***Connecting Environmental Sensor Packages*** (on page 22)

***DPX Sensor Packages*** (on page 23)

***DPX3 Sensor Packages*** (on page 31)

***Connecting a DPX2 Sensor Package to DPX3*** (on page 32)

***Using an Optional DPX3-ENVHUB4 Sensor Hub*** (on page 36)

***Mixing Diverse Sensor Types*** (on page 38)

***Supported Web Browsers*** (on page 50)

***Login*** (on page 51)

***Adding LDAP Server Settings*** (on page 122)

***Send Sensor Report Example*** (on page 154)

***Default Log Messages*** (on page 157)

***Email and SMS Message Placeholders*** (on page 164)

***Matching the Position*** (on page 180)

***States of Unmanaged Sensors or Actuators*** (on page 193)

***Unmanaging Environmental Sensors or Actuators*** (on page 193)

***Downloading Diagnostic Information*** (on page 201)

***Enabling or Disabling Peripheral Device Auto Management*** (on page 250)

***Determining the SSH Authentication Method*** (on page 265)

***Customizing the Date and Time*** (on page 272)

***All Privileges*** (on page 310)

***Bulk Configuration or Firmware Upgrade via DHCP/TFTP*** (on page 351)

***Updating the LDAP Schema*** (on page 396)

***PDView App for Viewing the PXE*** (on page 434)

***Ways to Probe Existing User Profiles*** (on page 447)

***Schroff LHX/SHX and USB Cascading Not Supported*** (on page 448)

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



# Chapter 1 Introduction

Raritan PXE is an intelligent power distribution unit (PDU) that allows you to remotely monitor power consumed by IT equipment in the server room or data center.

The intended use of the PXE 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.

## In This Chapter

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

---

## Product Models

The PXE 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 PXE 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 PXE device
- Mounting screws, brackets and/or buttons
- Cable retention clips for outlets (optional)

---

### 1U Products

- The PXE device
- Mounting screws, brackets and/or buttons

---

## APIPA and Link-Local Addressing

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

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

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

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

---

*Note: Configuration by connecting the PXE to a computer using a network cable is an application of this scenario. See **Connecting the PXE to a Computer** (on page 14).*

---

- The PXE 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 PXE. See **Selecting the Internet Protocol** (on page 70).

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

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

- ▶ **Retrieval of the link-local address:**
  - Perform the first three steps in the ***Initial Network Configuration via CLI*** (on page 16).

## Chapter 2 Rack-Mounting the PDU

This chapter describes how to rack mount a PXE device.

### In This Chapter

Rackmount Safety Guidelines .....	4
Circuit Breaker Orientation Limitation.....	4
Mounting 1U Models Using L-Brackets and Buttons.....	5
Mounting Zero U Models Using Two Rear Buttons .....	6
Mounting Zero U Models Using L-Brackets and Buttons .....	8

---

### 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 345) 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.*

---

---

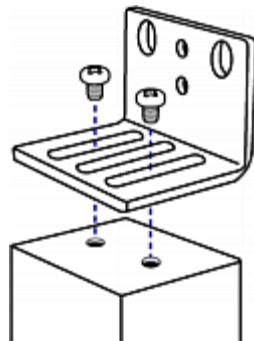
## Mounting 1U Models Using L-Brackets and Buttons

This section describes how to mount a 1U PXE device using L-brackets and two buttons.



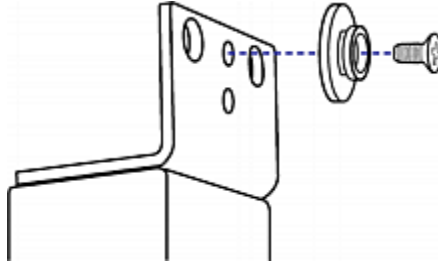
► **To mount 1U models using L-brackets and two buttons:**

1. Align the two edge slots of the L-bracket with the two screw holes on the top of the PXE device.
2. Screw the L-bracket to the device and ensure the bracket is fastened securely.



3. Repeat Steps 1 to 2 to screw another L-bracket to the bottom of the device.
4. After both L-brackets are installed, you can choose either of the following ways to mount the device in the rack.
  - Using rack screws, fasten the device to the rack through two identical holes near the edge of each L-bracket.

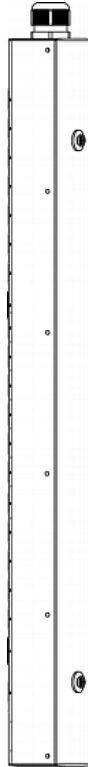
- Mount the device by screwing a mounting button in the back center of each L-bracket and then having both buttons engage the mounting holes in the rack. The recommended torque for the button is 1.96 N·m (20 kgf·cm).



---

### Mounting Zero U Models Using Two Rear Buttons

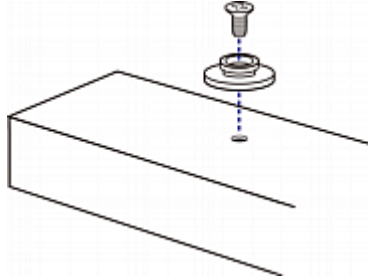
The following describes how to mount a PDU using two buttons only. If your PDU has circuit breakers implemented, read **Circuit Breaker Orientation Limitation** (on page 4) before mounting it.



► **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).

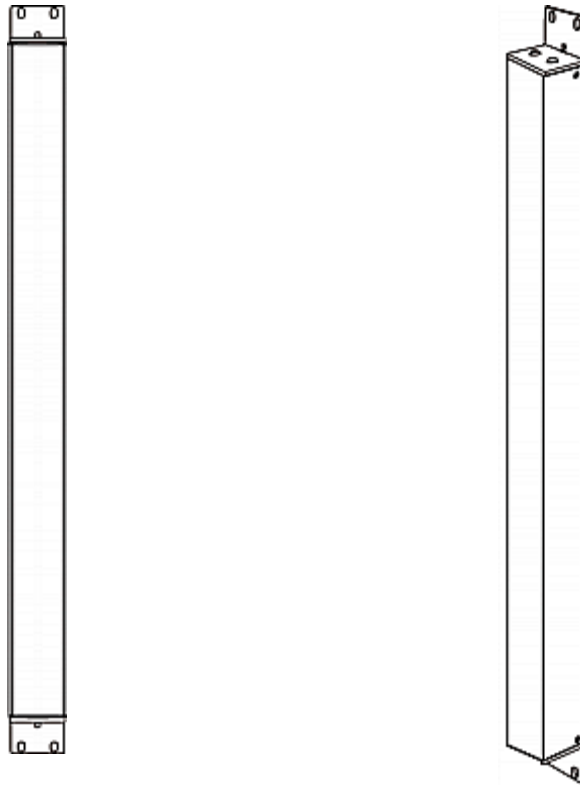


4. Screw a button in the screw hole near the top. The recommended torque for the button is 1.96 N·m (20 kgf·cm).
5. Ensure that the two buttons can engage their mounting holes in the rack or cabinet simultaneously.
6. Press the PXE device forward, pushing the mounting buttons through the mounting holes,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

---

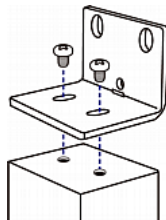
## Mounting Zero U Models Using L-Brackets and Buttons

This section describes how to mount a PDU using L-brackets and two buttons. 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 and two buttons:**

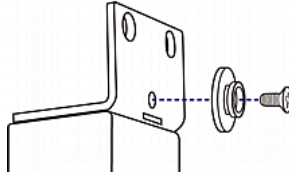
1. Align the two central holes of the L-bracket with the two screw holes on the top of the PXE device.
2. Screw the L-bracket to the device and ensure the bracket is fastened securely.



3. Repeat Steps 1 to 2 to screw another L-bracket to the bottom of the device.



4. After both L-brackets are installed, you can choose either of the following ways to mount the device in the rack.
  - Using rack screws, fasten the device to the rack through two identical holes near the edge of each L-bracket.
  - Mount the device by screwing a mounting button in the back center of each L-bracket and then having both buttons engage the mounting holes in the rack. The recommended torque for the button is 1.96 N·m (20 kgf·cm).



## Chapter 3 Installation and Configuration

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

### In This Chapter

Before You Begin .....	10
Connecting the PDU to a Power Source .....	11
Configuring the PXE .....	11
Bulk Configuration Methods .....	20
Installing Cable Retention Clips on Outlets (Optional) .....	20

---

### 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 PXE 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 PXE 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 PXE 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 345).*

---

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

---

### Filling Out the Equipment Setup Worksheet

An Equipment Setup Worksheet is provided in this User Guide. See **Equipment Setup Worksheet** (on page 347). 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.

---

### 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.

---

## Connecting the PDU to a Power Source

1. Verify that all circuit breakers on the PXE 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 PXE devices have overcurrent protection mechanisms.*

---

2. Connect each PXE to an appropriately rated branch circuit. See the label or nameplate affixed to your PXE for appropriate input ratings or range of ratings.
3. When a PXE device powers up, it proceeds with the power-on self test and software loading for a few moments.
4. When the software has completed loading, the LED display illuminates and shows numeric digits.

---

## Configuring the PXE

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

### ► Configuration using a connected computer:

1. Connect the PXE to a computer. See **Connecting the PXE to a Computer** (on page 14).

2. Use the connected computer to configure the PXE via the command line or web interface.
  - Command line interface: See **Initial Network Configuration via CLI** (on page 16).
  - Web interface: Launch the web browser on the computer, and type the link-local IP address or *pdu.local* to access the PXE. See **Login** (on page 51).

For IP address retrieval, see step 2 below.

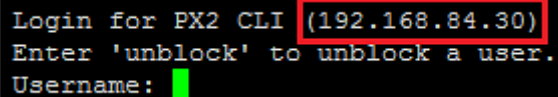
---

*Note: For details on the link-local addressing, see **APIPA and Link-Local Addressing** (on page 2).*

---

► **Configuration over a DHCP-enabled network:**

1. Connect the PXE to a DHCP network. See **Connecting the PXE to Your Network** (on page 15).
2. Retrieve the DHCP-assigned IPv4 address. Do one of the following:
  - Perform the first three steps in the section titled **Initial Network Configuration via CLI** (on page 16). The IPv4 address is displayed in the communications program as illustrated below.



```
Login for PX2 CLI (192.168.84.30)
Enter 'unblock' to unblock a user.
Username: █
```

- Use the MAC address of the PXE to retrieve the IP address. Contact your administrator for help. See **MAC Address** (on page 430).
3. Launch a web browser to configure the PXE. See **Login** (on page 51).

---

*Tip: To configure a number of PXE devices quickly, see **Bulk Configuration Methods** (on page 20).*

---

---

### Installing the USB-to-Serial Driver (Optional)

The PXE 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 PXE 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 PXE to the computer via a USB cable. The driver is automatically installed.

#### ► Manual driver installation in Windows®:

1. Make sure the PXE 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 PXE 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 PXE 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
```

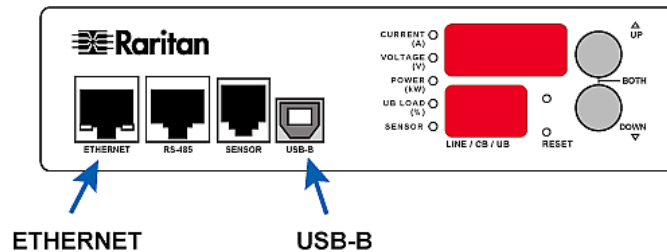
---

**Connecting the PXE to a Computer**

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

- ETHERNET port (female)
- USB-B port (male)

Zero U models:



To use the command line interface (CLI) for configuration, make a USB connection to the computer.

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

► **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 13).

2. Connect a USB cable between the PXE device's USB-B port and a computer's USB-A port.
3. Perform **Initial Network Configuration via CLI** (on page 16).

---

*Note: Not all serial-to-USB converters work properly with the PXE 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 PXE.
2. Connect the other end to a computer's Ethernet port.
3. On the connected computer, launch a web browser to access the PXE, using either link-local addressing: *pdu.local* or *169.254.x.x*. See **Login** (on page 51).

---

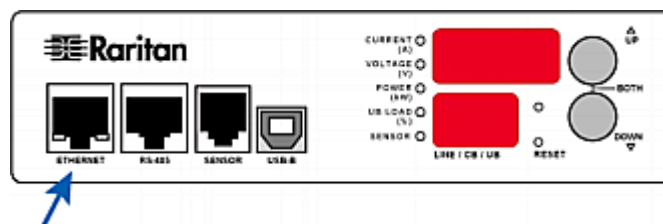
### Connecting the PXE to Your Network

To remotely administer the PXE, you must connect the PXE to your local area network (LAN). The PXE device does not support the wireless networking so you must establish a wired connection.

► **To make a wired connection:**

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

See this diagram for the ETHERNET port location.



---

### Initial Network Configuration via CLI

After the PXE 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 the USB connection. To configure the network settings using the web interface, see **Modifying the Network Configuration** (on page 68).

► **To configure the PXE device:**

1. On the computer connected to the PXE, 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 PXE.
4. The PXE 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. The default networking mode is the "wired" mode. Do not change this mode.



- b. 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	<pre>network interface LANInterfaceSpeed &lt;option&gt;</pre> <p>&lt;option&gt; = <i>auto</i>, <i>10Mbps</i>, or <i>100Mbps</i>.</p>
LAN interface duplex mode	<pre>network interface LANInterfaceDuplexMode &lt;mode&gt;</pre> <p>&lt;mode&gt; = <i>half</i>, <i>full</i> or <i>auto</i>.</p>

---

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

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

---

- c. 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	<pre>network ip proto &lt;protocol&gt;</pre> <p>&lt;protocol&gt; = <i>v4Only</i>, <i>v6Only</i> or <i>both</i></p>
IP address returned by the DNS server	<pre>network ip dnsResolverPreference &lt;resolver&gt;</pre> <p>&lt;resolver&gt; = <i>preferV4</i> or <i>preferV6</i></p>

- d. 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	<pre>network ipv4 ipConfigurationMode &lt;mode&gt;</pre> <p>&lt;mode&gt; = <i>dhcp</i> (default) or <i>static</i></p>

To set	Use this command
IPv6 configuration method	<pre>network ipv6 ipConfigurationMode &lt;mode&gt;</pre> <p>&lt;mode&gt; = <i>automatic</i> (default) or <i>static</i></p>

- 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)	<pre>network &lt;version&gt; preferredHostName &lt;name&gt;</pre> <p>&lt;name&gt; = preferred host name</p>

---

*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	<pre>network &lt;version&gt; ipAddress &lt;ip address&gt;</pre> <p>&lt;ip address&gt; = static IP address</p>
IPv4 subnet mask	<pre>network ipv4 subnetMask &lt;netmask&gt;</pre> <p>&lt;netmask&gt; = subnet mask</p>
IPv4 or IPv6 gateway	<pre>network &lt;version&gt; gateway &lt;ip address&gt;</pre> <p>&lt;ip address&gt; = gateway's IP address</p>

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.

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

The IP address configured may take seconds to take effect.

---

## Bulk Configuration Methods

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

► **Use a bulk configuration file:**

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

See **Bulk Configuration** (on page 196).

► **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 PXE after connecting them to the network.

See **Bulk Configuration or Firmware Upgrade via DHCP/TFTP** (on page 351).

---

## Installing Cable Retention Clips on Outlets (Optional)

If your PXE 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 your reseller. Make sure you use a clip that fits the power cord snugly to facilitate the installation or removal operation (for servicing).



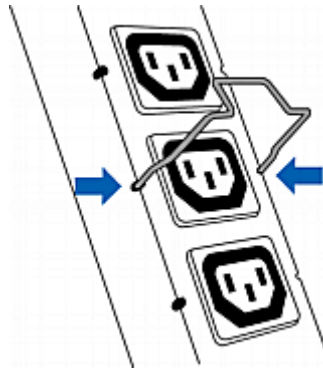
---

*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 430).*

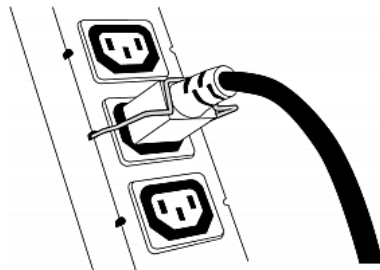
---

► **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 Environmental Sensor Packages

The PXE 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 PXE 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 23)
- **DPX2 Sensor Packages** (on page 29)
- **DPX3 Sensor Packages** (on page 31)
- **DX Sensor Packages** (on page 34)

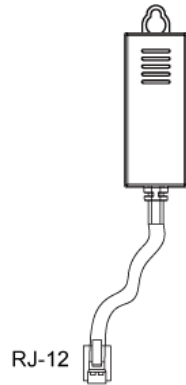
### In This Chapter

DPX Sensor Packages .....	23
DPX2 Sensor Packages .....	29
DPX3 Sensor Packages .....	31
DX Sensor Packages .....	34
Using an Optional DPX3-ENVHUB4 Sensor Hub.....	36
Mixing Diverse Sensor Types .....	38

---

## 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 28).

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

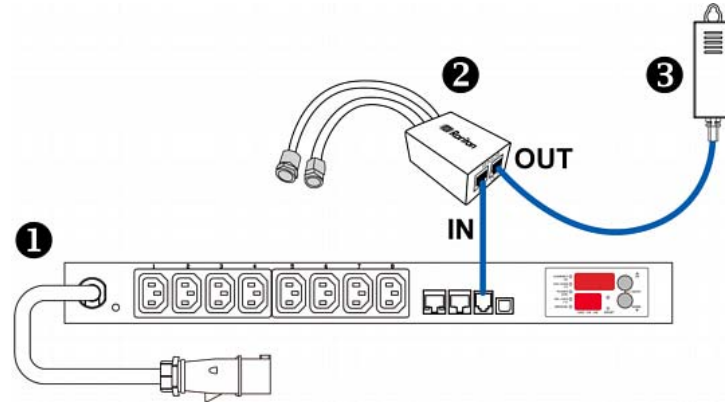
► **To connect a DPX sensor package with a factory-installed sensor cable:**

- Plug the sensor cable's RJ-12 connector into the RJ-12 SENSOR port on the PXE.

► **To connect a DPX differential air pressure sensor:**

1. Plug one end of a Raritan-provided phone cable into the IN port of a differential air pressure sensor.
2. Plug the other end of this phone cable into the RJ-12 SENSOR port on the PXE.

3. If intended, connect one DPX sensor package to the OUT port of the differential air pressure sensor. It can be any DPX sensor package, such as a DPX-T3H1.



①	The PXE device
②	Raritan differential air pressure sensors
③	One DPX sensor package (optional)

### Using an Optional DPX-ENVHUB4 Sensor Hub

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

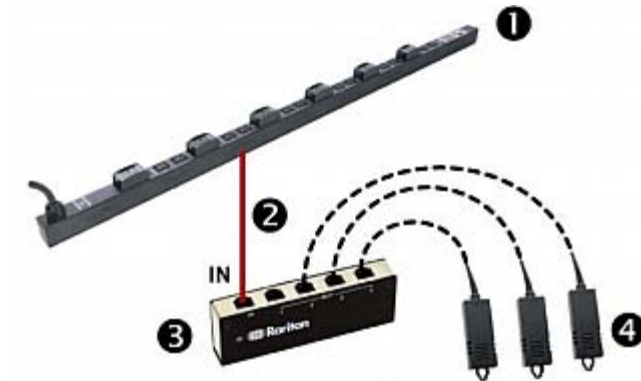
DPX-ENVHUB4 sensor hubs CANNOT be cascaded. You can only connect one hub to each SENSOR port on the PXE.

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

1. Connect the DPX-ENVHUB4 sensor hub to the PXE.
  - a. Plug one end of the Raritan-provided phone cable (4-wire, 6-pin, RJ-12) into the IN port (Port 1) of the hub.
  - b. Plug the other end of the cable into the RJ-12 SENSOR port of the PXE.
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 PXE device
2	Raritan-provided phone cable
3	DPX-ENVHUB4 sensor hub
4	DPX sensor packages

---

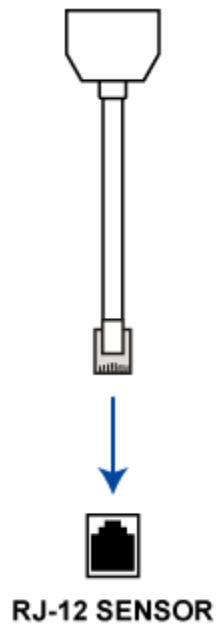
### Using an Optional DPX-ENVHUB2 cable

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

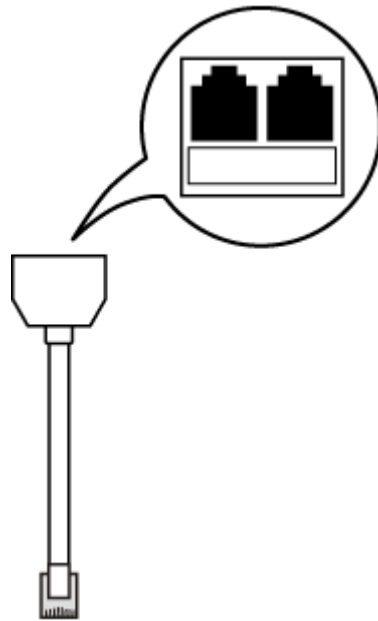
This cable supports DPX sensor packages only. Do NOT connect DPX2, DPX3 or DX sensor packages to it.

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

1. Plug the connector of this cable directly into the PXE device's RJ-12 SENSOR port.



2. The cable has two RJ-12 sensor ports. Connect DPX sensor packages to the cable's sensor ports.



3. Repeat the above steps if there are additional SENSOR ports on your PXE.

### Supported Maximum DPX Sensor Distances

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

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

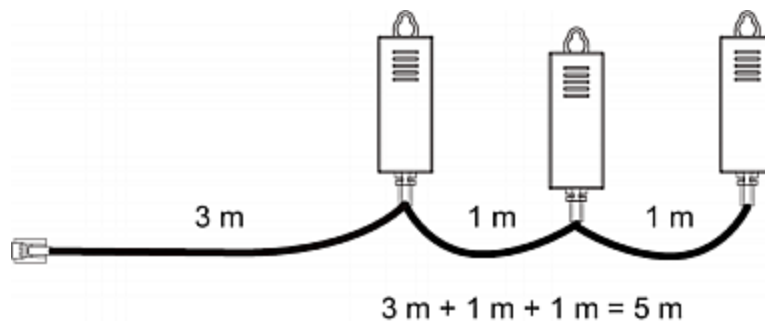
#### ► Sensor Connection Restrictions:

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

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



- The total cabling length between the PXE 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.

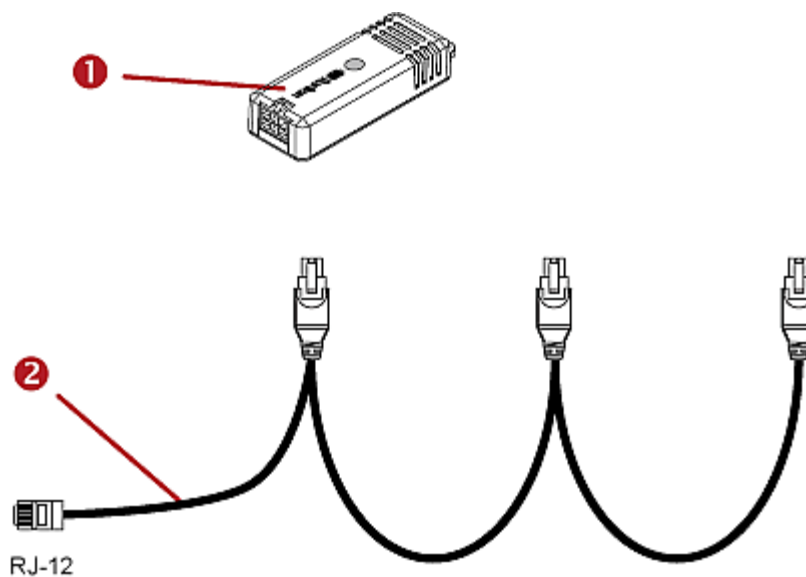
PXE → 33' (10 m) cable → 1 sensor hub → 16' (5 m) cable → Up to 4 DPX-T3H1 sensor packages

---

## 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/>).



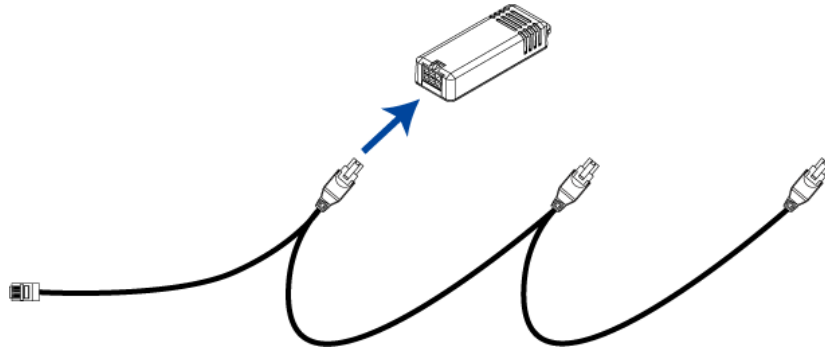
Item	
①	DPX2 sensor package
②	DPX2 sensor cable with one RJ-12 connector and three head connectors

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

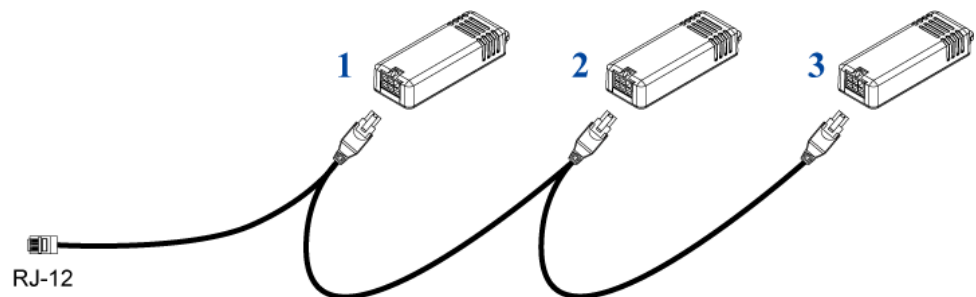
**Warning:** If there are free head connectors between a DPX2 sensor cable's RJ-12 connector and the final attached DPX2 sensor package, the sensor packages following the free head connector(s) on the same cable do NOT work properly. Therefore, always occupy all head connectors prior to the final sensor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

► **To connect DPX2 sensor packages to the PXE:**

1. Connect a DPX2 sensor package to the first head connector of the DPX2 sensor cable.



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



---

*Tip: If the number of sensors you are connecting is less than the number of head connectors on your sensor cable, connect them to the first one or first two head connectors to ensure that there are NO free head connectors prior to the final DPX2 sensor package attached.*

---

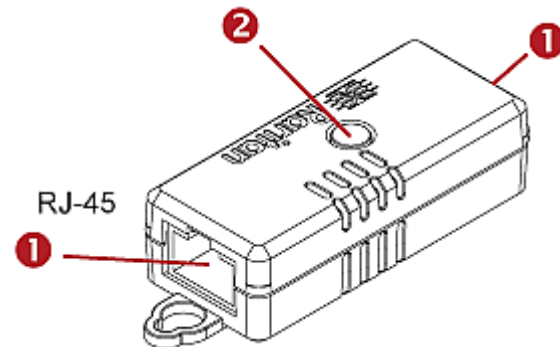
3. Plug the RJ-12 connector of the DPX2 sensor cable into the RJ-12 SENSOR port on the PXE.

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 35).

## DPX3 Sensor Packages

A DPX3 sensor package features the following:

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

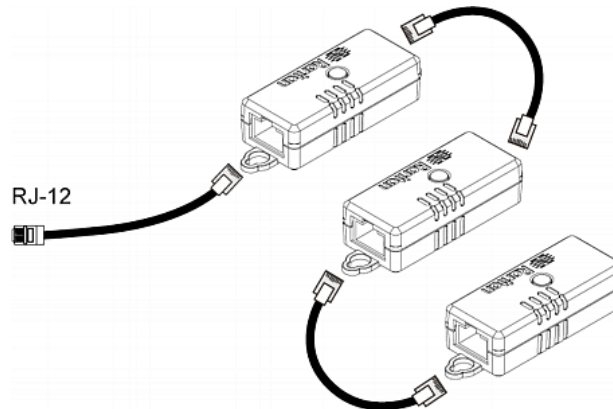


Numbers	Components
①	RJ-45 ports, each of which is located on either end of a DPX3 sensor package.
②	LED for indicating the sensor status.

### ► To connect DPX3 sensor packages to the PXE:

1. Connect an RJ-12 to RJ-45 adapter cable to the DPX3 sensor package.
  - Connect the adapter's RJ-45 connector to either RJ-45 port of the DPX3 sensor package.
2. If you want to cascade DPX3 sensor packages, get an additional standard network patch cable (CAT5e or higher) and then:
  - a. Plug one end of the cable into the remaining RJ-45 port on the prior DPX3.
  - b. Plug the other end into either RJ-45 port on an additional DPX3.

Repeat the same steps to cascade more DPX3 sensor packages.



3. Connect the first DPX3 sensor package to the PXE.
  - Plug the adapter cable's RJ-12 connector into the RJ-12 SENSOR port on the PXE.

---

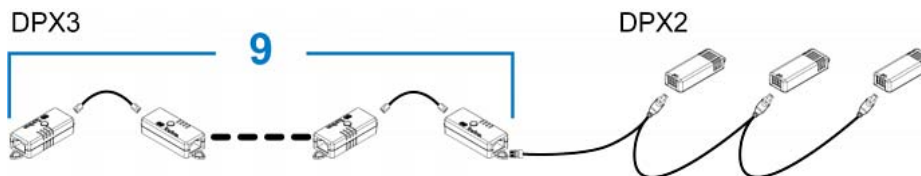
### Connecting a DPX2 Sensor Package to DPX3

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:**

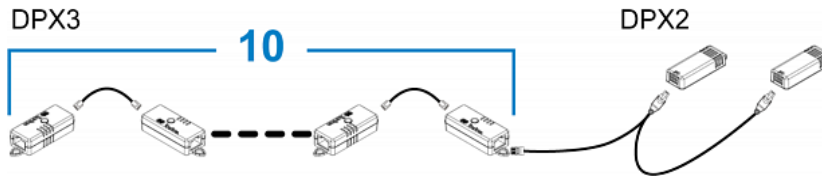
A maximum of nine DPX3 sensor packages can be cascaded because  $12-3=9$ .





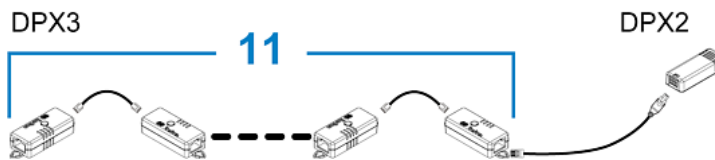
► **When connecting a DPX2 sensor package containing two DPX2 sensors:**

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/>).

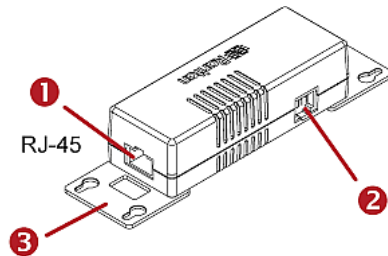
You can cascade up to 12 DX sensor packages.

When cascading DX, remember that the PXE 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 PXE.

For example, if you cascade 12 DX packages, and each package contains 3 functions (a function is a sensor or actuator), the PXE does NOT manage the last 4 functions because the total 36 ( $12 \times 3 = 36$ ) 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 193) and **Managing Environmental Sensors or Actuators** (on page 182).*

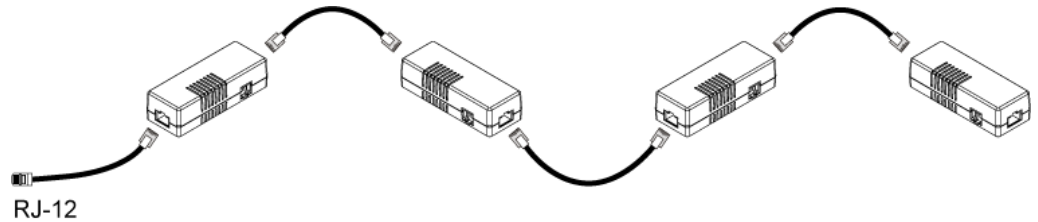


Numbers	Components
①	RJ-45 ports, each of which is located on either end of a DX sensor package.
②	RJ-12 port, which is reserved for future use and now blocked.
③	Removable rackmount brackets.

### ► Connect DX to the PXE:

1. Connect an RJ-12 to RJ-45 adapter cable which is shipped with a DX sensor package to the DX.
  - Connect the adapter's RJ-45 connector to either RJ-45 port of the DX.

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



3. Connect the first DX sensor package to the PXE.
  - Plug the adapter cable's RJ-12 connector into the RJ-12 SENSOR port of the PXE.
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 35).

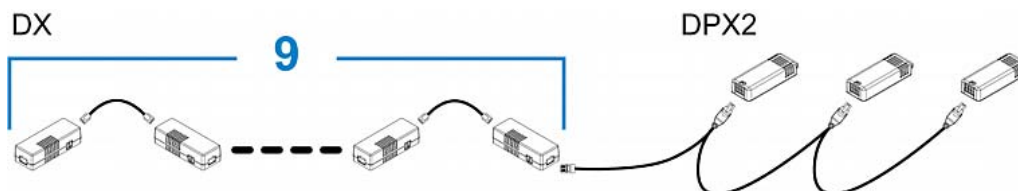
### Connecting a DPX2 Sensor Package to DX

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.

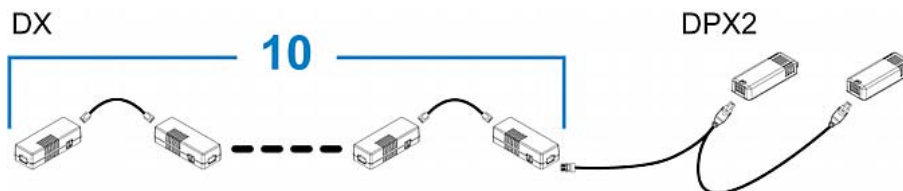
#### ► When connecting a DPX2 sensor package containing three DPX2 sensors:

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



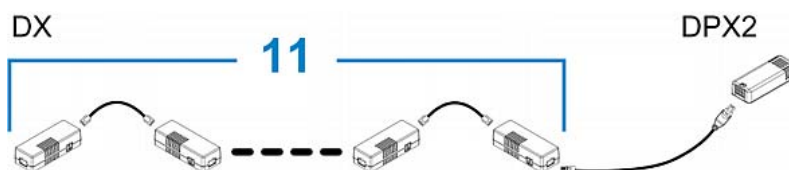
► **When connecting a DPX2 sensor package containing two DPX2 sensors:**

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 PXE, 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.

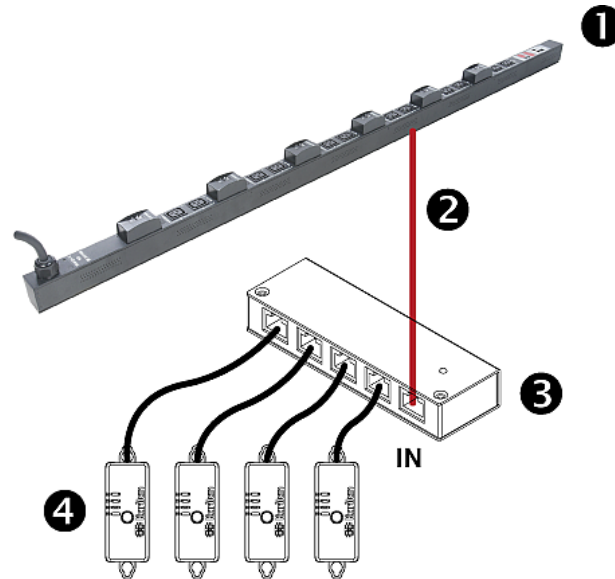
To connect diverse types of sensor packages to this sensor hub, you must follow the combinations shown in the section titled **Mixing Diverse Sensor Types** (on page 38).

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

1. Connect the DPX3-ENVHUB4 sensor hub to the PXE using an RJ-12 to RJ-45 adapter cable.
  - a. Plug the RJ-45 connector of this cable into the IN port (Port 1) of the hub.
  - b. Plug the RJ-12 connector of this cable into the RJ-12 SENSOR port of the PXE.

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 PXE
2	RJ-12 to RJ-45 adapter cable
3	DPX3-ENVHUB4 sensor hub
4	Any Raritan sensor packages

## Mixing Diverse Sensor Types

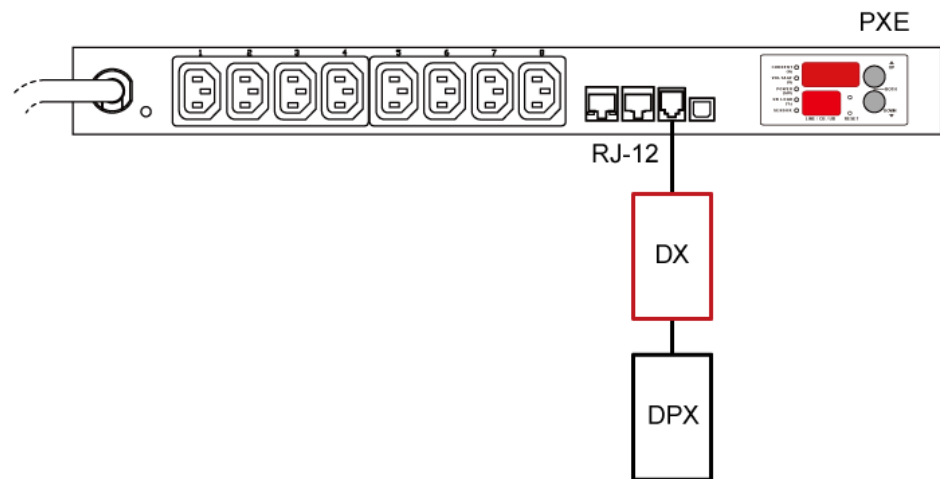
You can mix DPX, DPX2, DPX3 and DX sensor packages on one PXE according to the following sensor combinations. In some scenarios, the DPX3-ENVHUB4 sensor hub is required.

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

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

### ► 1 DX + 1 DPX:

- An RJ-12 to RJ-45 adapter cable is required for connecting the DX sensor package to the PXE.
- It is strongly recommended to use an RJ-12 to RJ-45 adapter to connect the DPX sensor package to the DX sensor package.

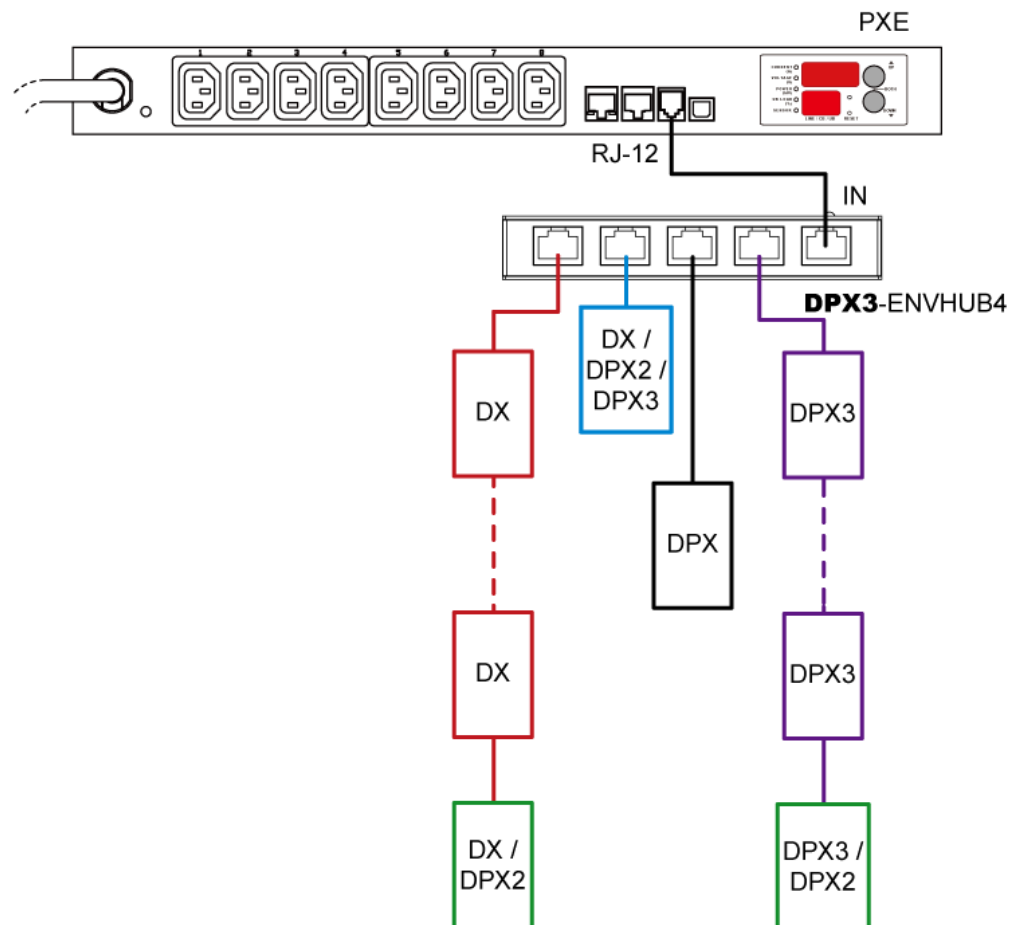


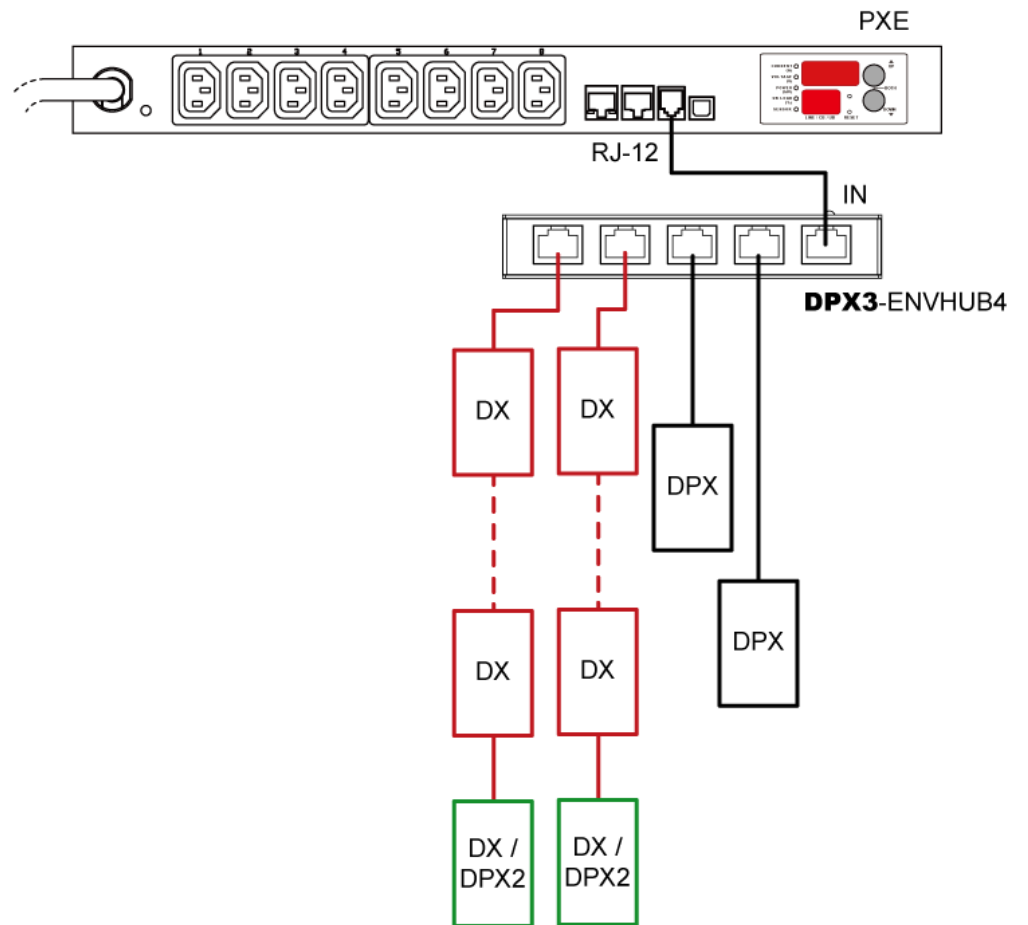
### ► Diverse combinations via the DPX3-ENVHUB4 sensor hub:

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

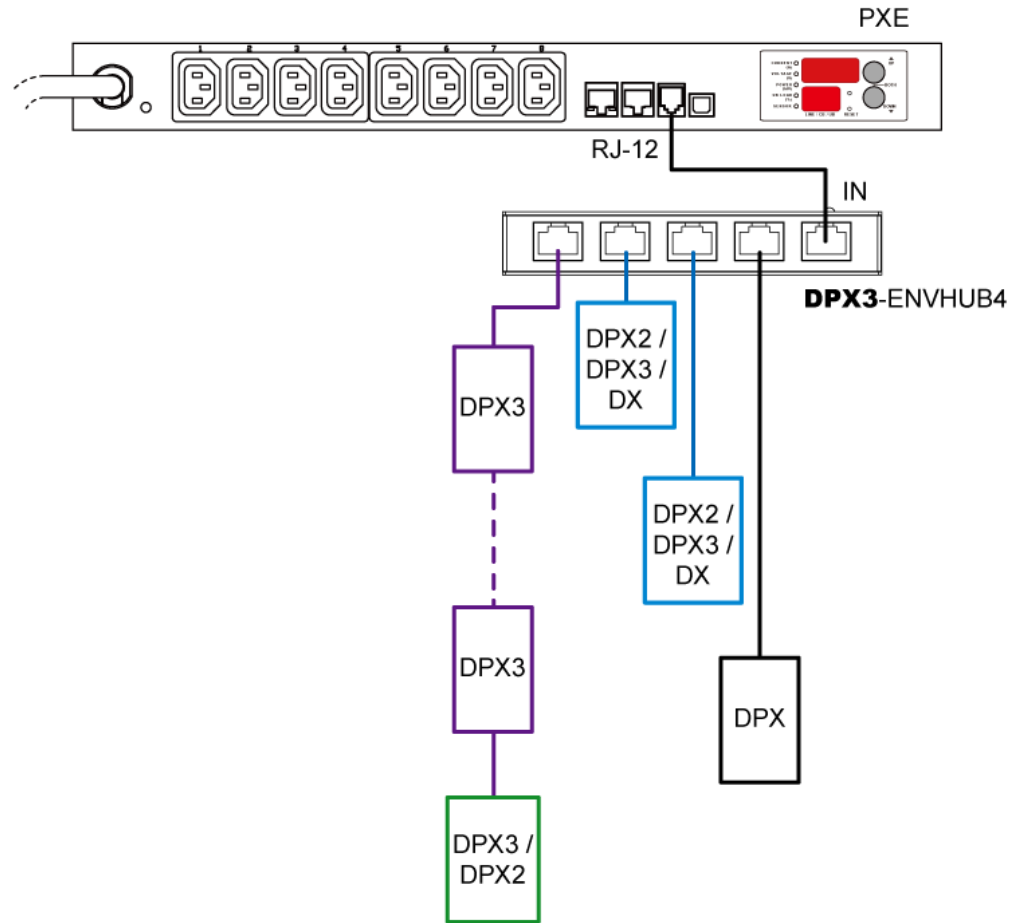
- An RJ-12 to RJ-45 adapter is recommended to connect a DPX or DPX2 sensor package to DPX3-ENVHUB4.
- In the following diagrams, the sensor package in "green" can be replaced by a DPX2 sensor package. The sensor package in "blue" can be one DPX2, DPX3 or DX sensor package.
- An RJ-12 to RJ-45 adapter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

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









► **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 32) or **Connecting a DPX2 Sensor Package to DX** (on page 35).

## Chapter 5 Using the PDU

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

- Description of the LEDs and ports on the PDU
- How to use the front panel display
- How the overcurrent protector (a circuit breaker) works

### In This Chapter

Panel Components .....	42
Circuit Breakers.....	47

---

### Panel Components

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

- Power cord
- Outlets
- Connection ports
- LED display
- Reset button

---

#### Power Cord

Most of Raritan PDUs come with an installed power cord, which is ready to be plugged into an appropriate receptacle for receiving electricity. Such devices cannot be rewired by the user.

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

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

---

#### Outlets

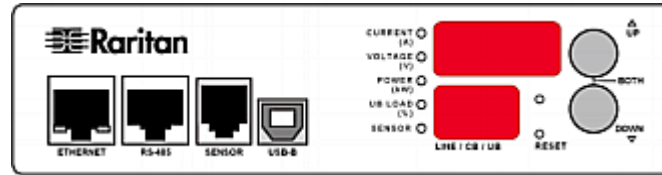
The total number of outlets varies from model to model.

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

Outlet LEDs are not available.

### Connection Ports

There are 4 ports located on the front panel of the PDU as shown below.



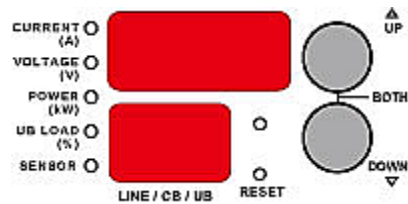
The table below explains the function of each port.

Port	Used for...
USB-B	Establishing a USB connection between a computer and the PXE for using the command line interface or performing the disaster recovery. For disaster recovery instructions, contact Raritan Technical Support.
RS-485	Reserved for a future release.
SENSOR (RJ-12)	<p>Connection to one of the following devices:</p> <ul style="list-style-type: none"> <li>Raritan's environmental sensor package(s).</li> <li>Raritan's sensor hub, which expands the number of a sensor port to four ports.</li> </ul>
ETHERNET	<p>Connecting the PXE to your company's network.</p> <p>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 PXE device remotely using the web interface.</p> <p>There are two small LEDs adjacent to the port:</p> <ul style="list-style-type: none"> <li>Green indicates a physical link and activity.</li> <li>Yellow indicates communications at 10/100 BaseT speeds.</li> </ul>

## LED Display

The LED display is located on the side where outlets are available.

These diagrams show the LED display on different types of PDUs. Note that the LED display might slightly vary according to the PDU you purchased.



The LED display consists of:

- A row displaying three digits
- A row displaying two digits
- Up and Down buttons
- Five LEDs for measurement units

*Note: When a PXE device powers up, it proceeds with the power-on self test and software loading for a few moments. When the software has completed loading, the LED display illuminates.*

## Three-Digit Row

The three-digit row shows the readings for the selected component. Values that may appear include:

- Active power or unbalanced load of the inlet
- Current, voltage, or active power of the selected line

*Note: L1 voltage refers to the L1-L2 or L1-N voltage, L2 voltage refers to the L2-L3 or L2-N voltage, and L3 voltage refers to the L3-L1 or L3-N voltage.*

- The text “FuP,” which indicates that the **F**irmware **uP**grade is being performed

**LEDs for Measurement Units**

Five small LED indicators are on the LED display: four measurement units LEDs and one Sensor LED.

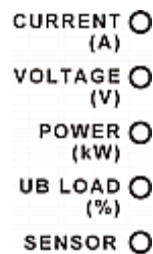
The measurement units vary according to the readings that appear in the three-digit row. They are:

- Amp (A) for current
- Volt (V) for voltage
- Kilowatt (kW) for active power
- Percentage (%) of the unbalanced load

One of the measurement unit LEDs will be lit to indicate the unit for the value currently shown in the three-digit row.

The Sensor LED is lit only when PXE detects the physical connection of any environmental sensor.

The five LEDs look similar to this diagram but may slightly vary according to the model you purchased.

**Two-Digit Row**

The two-digit row shows the number of the currently selected line or inlet. Values that may appear include:

- L<sub>x</sub>: This indicates the selected line, where x is the line number. For example, L2 represents Line 2.

---

*Note: For a single-phase model, L1 current represents the Unit Current.*

---

- AP: This indicates the selected inlet's active power.

**Automatic Mode**

When left alone, the LED display cycles through the line readings at intervals of 10 seconds, as available for your PXE. This is the Automatic Mode.

### Manual Mode

You can press the Up or Down button to enter the Manual Mode so that a particular line or the inlet's active power is selected to show specific readings.

► **To operate the LED display:**

1. Press the Up or Down button until the desired line's number is selected in the two-digit row. Or you can press either button to select the inlet's active power, which is shown as *AP*.
  - Pressing the  $\Delta$  (UP) button moves up one selection.
  - Pressing the  $\nabla$  (DOWN) button moves down one selection.
2. When selecting a line, you can press the Up and Down buttons simultaneously to switch between voltage, active power and current readings.
  - Current of the selected component is shown in the three-digit row. Simultaneously the CURRENT(A) LED is lit. See **LEDs for Measurement Units** (on page 45).
  - When the voltage is displayed, the VOLTAGE(V) LED is lit. It is displayed for about five seconds, after which the current reading re-appears.
  - When the active power is displayed, the POWER(kW) LED is lit. It is displayed for about five seconds, after which the current reading re-appears.
3. When selecting the inlet (AP), it displays the active power reading.
  - When the active power is displayed, the POWER(kW) LED is lit.

---

*Note: The LED display returns to the Automatic Mode after 20 seconds elapse since the last time any button was pressed.*

---

### Reset Button

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

Pressing this reset button restarts the PXE device's software without any loss of power to outlets. This operation also power cycles the LED display, causing the LED display to go blank and then return to normal.

The following image indicates the locations of the reset button on the PXE device.



## Circuit Breakers

PXE 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.

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.

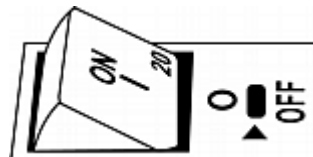
Depending on the model you purchased, the circuit breaker may use a button- or handle-reset mechanism.

### 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 PXE 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.



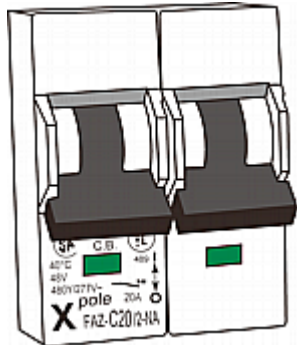
---

### 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:**

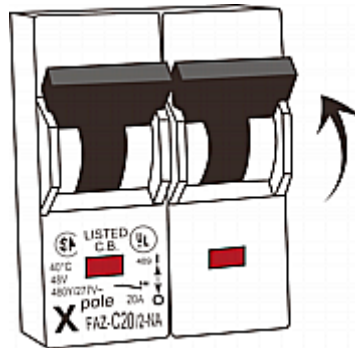
1. Lift the hinged cover over the breaker.
2. Check if the colorful rectangle or triangle below the operating handle is GREEN, indicating that the breaker has tripped.



3. Examine your PXE and the connected equipment to remove or resolve the cause that results in the overload or short circuit. **This step is required, or you cannot proceed with the next step.**



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



## Chapter 6 Using the Web Interface

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

### In This Chapter

Supported Web Browsers.....	50
Logging in to the Web Interface .....	51
Logout.....	54
Introduction to the Web Interface .....	55
Viewing the Dashboard .....	64
Device Management.....	66
User Management .....	91
Setting Up Roles.....	96
Forcing HTTPS Encryption.....	99
Access Security Control .....	99
Setting Up a TLS Certificate .....	114
Setting Up External Authentication.....	120
Outlet Management .....	128
Inlet and Overcurrent Protector Management.....	129
Setting Power Thresholds .....	133
Event Rules and Actions .....	135
Managing Event Logging.....	171
Viewing Connected Users .....	172
Monitoring Server Accessibility.....	173
Environmental Sensors and Actuators .....	178
Bulk Configuration .....	196
Backup and Restore of PXE Device Settings.....	199
Network Diagnostics.....	200
Downloading Diagnostic Information.....	201
Firmware Upgrade.....	202
Accessing the Help.....	204

---

### 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 PXE, 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 91).

---

### 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:

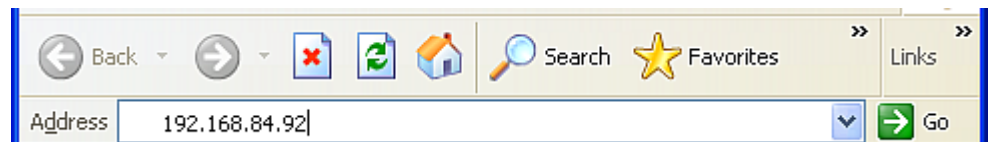
*http(s)://<ip address>*

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

---

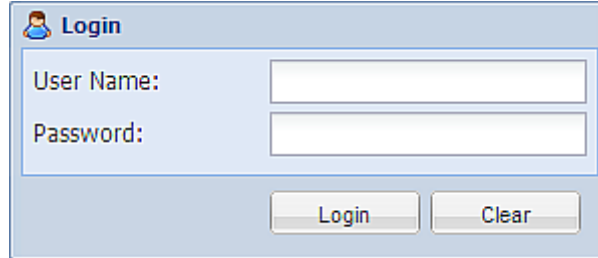
*Tip: If the link-local addressing has been enabled, you can type pdu.local instead of an IP address. See **APIPA and Link-Local Addressing** (on page 2).*

---



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.



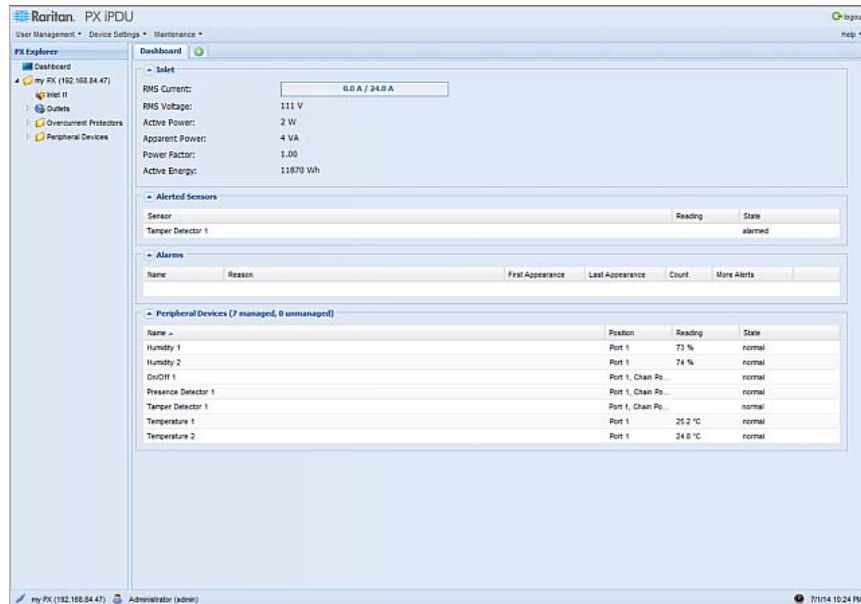
*Note: If needed, click Clear to clear either the inputs or any error message that appears.*

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 PXE page opens.

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



**Raritan PXE**

User Management • Device Settings • Maintenance

**FX Explorer**

- my PX (192.168.0.47)
- my PX II
- Outlets
- Overcurrent Protection
- Peripheral Devices

**Dashboard**

**Alert**

RMS Current: 0.0 A / 24.0 A

RMS Voltage: 111 V

Active Power: 2 W

Apparent Power: 4 VA

Power Factor: 1.00

Active Energy: 11870 Wh

**Alerted Sensors**

Sensor	Reading	State
Tamper Detector 1		alarmed

**Alarms**

Name	Reason	First Appearance	Last Appearance	Count	More Alerts
------	--------	------------------	-----------------	-------	-------------

**Peripheral Devices (7 managed, 0 unmanaged)**

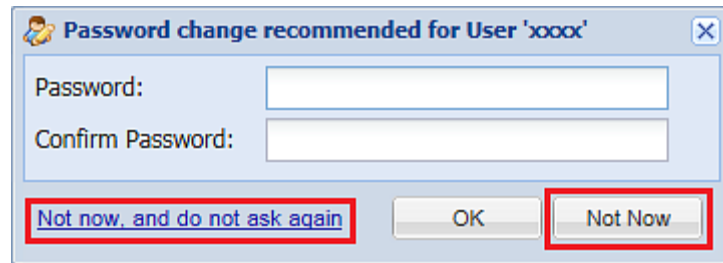
Name	Position	Reading	State
Humidity 1	Port 1	75 %	normal
Humidity 2	Port 1	74 %	normal
On/Off 1	Port 1, Chan Po...		normal
Presence Detector 1	Port 1, Chan Po...		normal
Tamper Detector 1	Port 1, Chan Po...		normal
Temperature 1	Port 1	25.2 °C	normal
Temperature 2	Port 1	24.0 °C	normal

my PX (192.168.0.47) Administrator (admin) 7/1/14 10:24 PM

► **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.

---

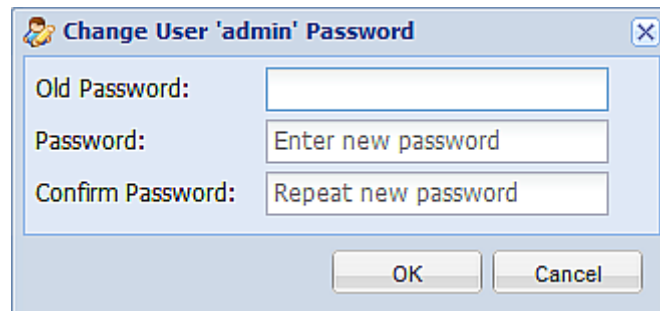
### Changing Your Password

You must have the Change Own Password permission to change your own password. See **Setting Up Roles** (on page 96).

You must have Administrator Privileges to change other users' passwords. See **Modifying a User Profile** (on page 94).

► **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 PXE 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 PXE 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.

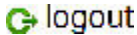

The PXE does NOT support other browser password managers.

---

## Logout

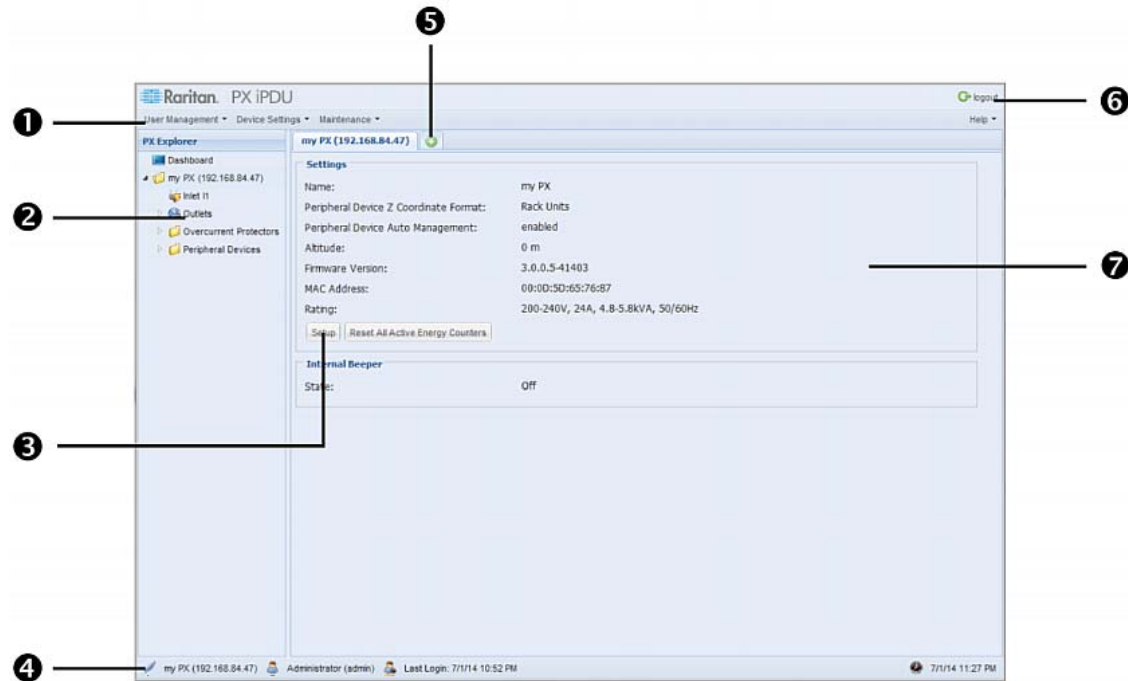
After finishing your tasks with the PXE, you should log out to prevent others from accessing the web interface.

### ► To log out of the web interface:

1. Do one of these:
  - Click "logout" on the top-right corner of the web interface.  
The image shows a green circular icon with a white arrow pointing right, followed by the word "logout" in a bold, black, sans-serif font.
  - 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
<b>1</b>	Menus
<b>2</b>	PX Explorer pane
<b>3</b>	Setup button*
<b>4</b>	Status bar
<b>5</b>	Add Page icon
<b>6</b>	Logout button
<b>7</b>	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 PXE 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	C1 to Cn**
	Peripheral Devices folder	A list of connected environmental sensors

\* The folder is named "my PX" by default. The name can be customized. See **Naming the PDU** (on page 68).

\*\* n represents the final number of that component.

### ► To navigate through the tree:

1. To expand any folders, see **Expanding the Tree** (on page 57).
2. To show any tree item's data, click on that item. See **Add Page Icon** (on page 59).



## Expanding the Tree

The icons representing all components implemented on or connected to the PXE 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.*

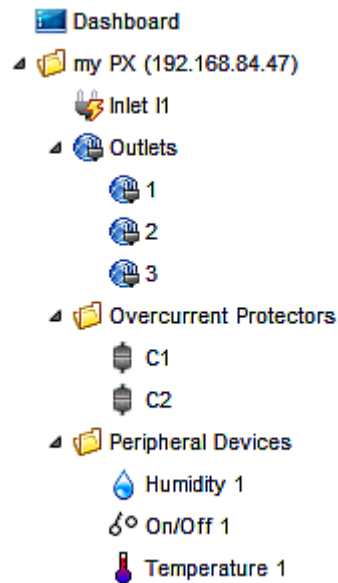
---

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.

---

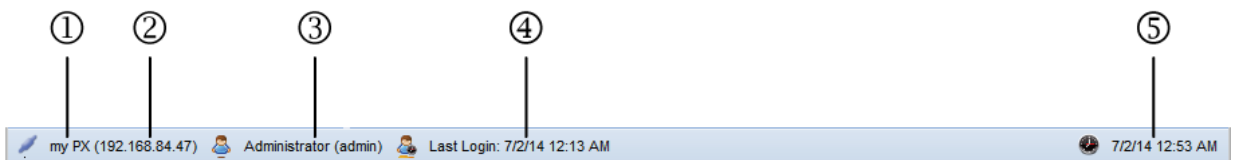
### Setup Button

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 PXE device. The default is "my PX." See **Naming the PDU** (on page 68).

2. **IP address:**

The numbers enclosed in parentheses is the IP address assigned to the PXE device. See **Initial Network Configuration via CLI** (on page 16) or **Modifying Network Settings** (on page 69).

---

*Tip: The presence of the device name and IP address in the status bar indicates the connection to the PXE 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 PXE 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 PXE 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.

---

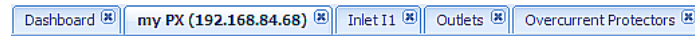
**Add Page Icon**

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.

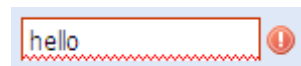
---

### 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.

See the table for the meaning of each color:

Color	State
White	<p>The background is white in one of the following scenarios:</p> <ul style="list-style-type: none"> <li>For a numeric sensor, no thresholds have been enabled.</li> <li>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.</li> <li>For a discrete (on/off) sensor, the sensor state is normal.</li> <li>The sensor is unavailable or unmanaged.</li> </ul>
Yellow	<p>The reading drops below the lower warning threshold or rises above the upper warning threshold.</p>
Red	<p>The meaning of the red color varies depending on the sensor type:</p> <ul style="list-style-type: none"> <li>For a numeric sensor, this color indicates the reading drops below the lower critical threshold or rises above the upper critical threshold.</li> <li>For a discrete (on/off) sensor, this color indicates the sensor is in the "alarmed" state.</li> </ul>

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

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

For information on the thresholds, see **Setting Power Thresholds** (on page 133) and **Configuring Environmental Sensors or Actuators** (on page 184).

**Browser-Defined Shortcut Menu**

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

Back
Forward
Save Background As...
Set as Background
Copy Background
Set as Desktop Item...
Select All
Paste
Create Shortcut
Add to Favorites...
View Source
Encoding ▶
Print
Refresh
Append to Existing PDF
Convert to Adobe PDF
Export to Microsoft Excel
Properties

## 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 PXE device's status.

The page is divided into various sections according to the component type, such as inlet and peripheral devices.

---


*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 61).*

---


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

Alerted Sensors		
Sensor	Reading	State
Inlet I1 L1-L2 RMS Voltage	427 V	above upper warning
Temperature 1	20.7 °C	below lower warning
Temperature 2	20.2 °C	below lower warning
On/Off 1		alarmed



For the background color meanings in this section, see ***The Yellow- or Red-Highlighted Sensors*** (on page 61).

## 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 136).

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

Below is the illustration of the alarms list.

Alarms						
Name	Reason	First Appearance	Last Appearance	Count	More Alerts	
Alarm - mail	Peripheral device 'Temperature 1' in slot '1' unavailable.	5/11/13 5:19 AM	5/11/13 5:19 AM	1	2 more reasons	<a href="#">Details</a>
Alarm - SMS message	Peripheral device 'Temperature 2' in slot '3' asserted 'above upper critical' at 77.8 deg F.	5/11/13 5:36 AM	5/11/13 5:36 AM	1	-	<a href="#">Details</a>

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	<ul style="list-style-type: none"> <li>A dash is displayed when there is only one event triggering this alert.</li> <li>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.</li> </ul>
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

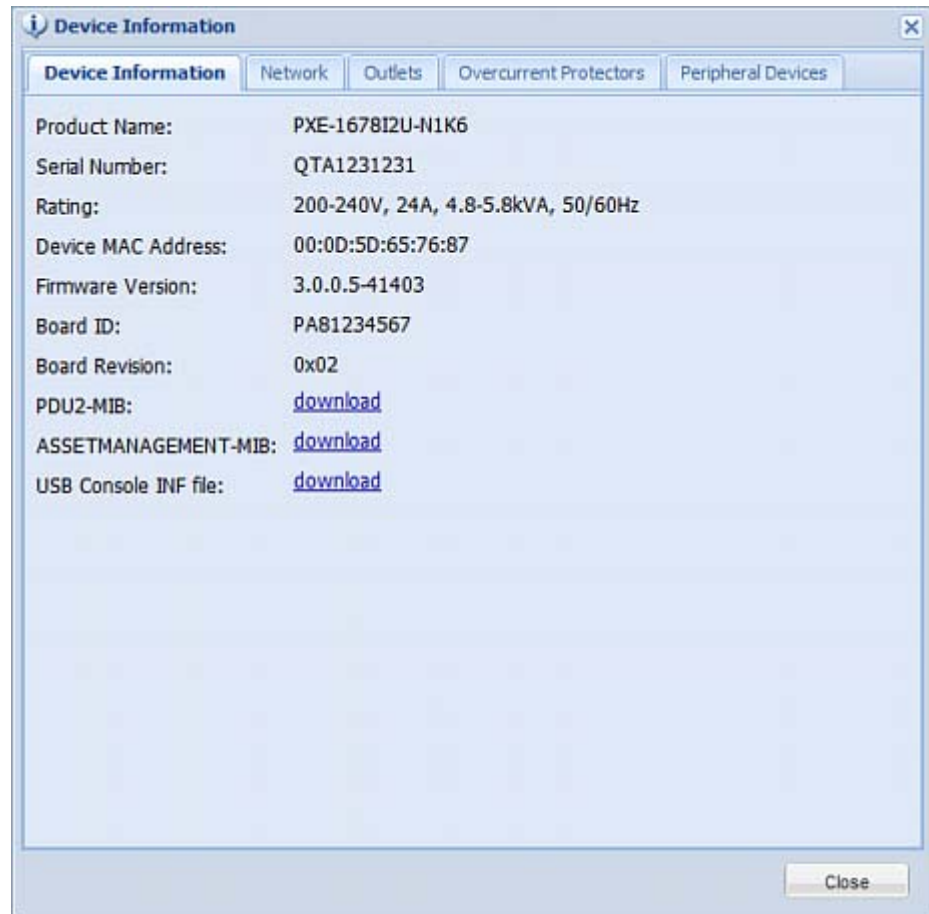
Using the web interface, you can retrieve basic hardware and software information, give the PXE a new device name, set the system date and time, and modify network settings that were entered during the initial configuration process.

## Displaying PDU Information

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

### ► To display the 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.

Tab	Data
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.
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.

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

---

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

---

### Naming the PDU

The default name for PXE 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 the Network Interface Settings

The PXE device only supports the wired networking mode. The wireless networking mode is NOT supported.

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 PXE 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 PXE 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.*

---

### Modifying Network Settings

The PXE was configured for network connectivity during the installation and configuration process. See **Configuring the PXE** (on page 11). If necessary, you can modify any network settings later.

### **Selecting the Internet Protocol**

The PXE 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 70).

#### **► 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	<p>To auto-configure the PXE, select DHCP.</p> <p>With DHCP selected, you can enter a preferred DHCP host name, which is optional. Type the host name in the Preferred Hostname field.</p> <p>The host name:</p> <ul style="list-style-type: none"> <li>▪ Consists of alphanumeric characters and/or hyphens</li> <li>▪ Cannot begin or end with a hyphen</li> <li>▪ Cannot contain more than 63 characters</li> <li>▪ Cannot contain punctuation marks, spaces, and other symbols</li> </ul> <p>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.</p>
Static	<p>To manually assign an IP address, select Static, and enter the following information in the corresponding fields:</p> <ul style="list-style-type: none"> <li>▪ IP address</li> <li>▪ Netmask</li> <li>▪ Default gateway</li> <li>▪ Primary DNS server</li> <li>▪ Secondary DNS server (optional)</li> <li>▪ DNS Suffix (optional)</li> </ul> <p>If your local network contains two subnets and IP forwarding has been enabled, you can click Append to add static routes so that your PXE can communicate with the other subnet. Each static route requires:</p> <ul style="list-style-type: none"> <li>▪ Destination: IP address of the other subnet and subnet mask using the format "IP address/subnet mask."</li> <li>▪ Next Hop: IP address of the next hop router.</li> </ul> <p>See <b>Static Route Examples</b> (on page 74) for illustrations.</p>

4. Click OK.

---

*Note: The PXE supports a maximum of 3 DNS servers. If two IPv4 DNS servers and two IPv6 DNS servers are available, the PXE 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 70).

#### **► 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	<p>To auto-configure the PXE, select Automatic.</p> <p>With this option selected, you can enter a preferred host name, which is optional. Type the host name in the Preferred Hostname field.</p> <p>The host name:</p> <ul style="list-style-type: none"> <li>▪ Consists of alphanumeric characters and/or hyphens</li> <li>▪ Cannot begin or end with a hyphen</li> <li>▪ Cannot contain more than 63 characters</li> <li>▪ Cannot contain punctuation marks, spaces, and other symbols</li> </ul> <p>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.</p>
Static	<p>To manually assign an IP address, select Static, and enter the following information in the corresponding fields:</p> <ul style="list-style-type: none"> <li>▪ IP address</li> <li>▪ Default gateway</li> <li>▪ Primary DNS server</li> <li>▪ Secondary DNS server (optional)</li> <li>▪ DNS Suffix (optional)</li> </ul> <p>If your local network contains two subnets and IP</p>



Option	Description
	<p>forwarding has been enabled, you can click Append to add static routes so that your PXE can communicate with the other subnet. Each static route requires:</p> <ul style="list-style-type: none"><li>▪ Destination: IP address of the current subnet and prefix length using the format "IP address/prefix."</li><li>▪ Next Hop: IP address of the next hop router.</li></ul> <p>See <b>Static Route Examples</b> (on page 74) for illustrations.</p>

4. Click OK.

---

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

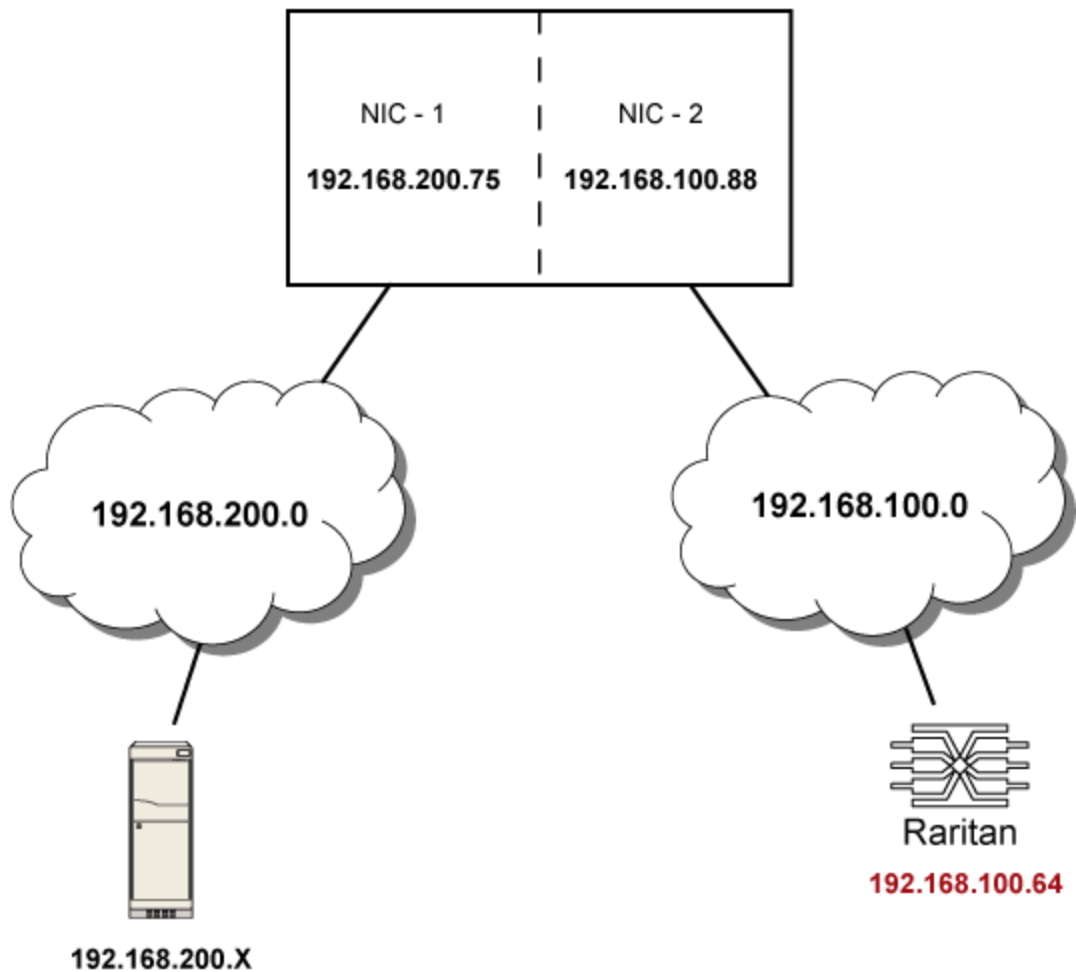
---

### 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 PXE devices in the examples use static IP addresses.

#### ► IPv4 example:

- Your PXE: 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

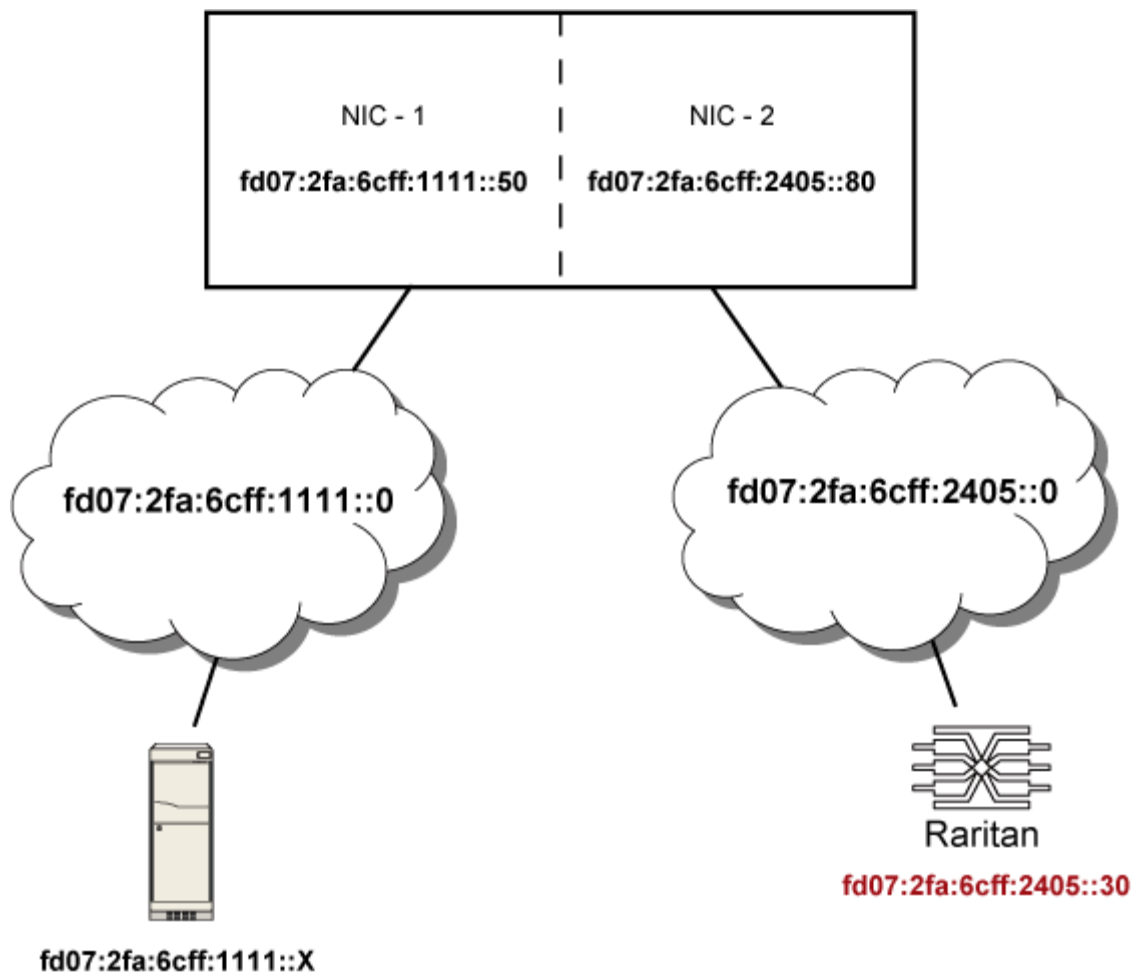


In this example, NIC-2 (192.168.100.88) is the next hop router for your PXE to communicate with any device in the other subnet 192.168.200.0. In the IPv4 "Append new Route" dialog, you should specify:

- Destination: 192.168.200.0/24
- Next Hop: 192.168.100.88

► **IPv6 example:**

- Your PXE: *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 PXE 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 PXE may fail to connect to the given host.

Therefore, DNS server settings are important for external authentication. With appropriate DNS settings, the PXE 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 120).

---

#### **Modifying Network Service Settings**

The PXE 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 218).

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 PXE 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 PXE device so it is a more secure protocol than HTTP.

By default, any access to the PXE 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 PXE 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.*

---

### 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 91).

### 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.

## Configuring SNMP Settings

You can enable or disable SNMP communication between an SNMP manager and the PXE device.

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 135).

### ► To configure SNMP communication:

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

The image shows the 'SNMP Settings' dialog box with the 'General' tab selected. The 'Notifications' tab is also visible. The 'SNMP v1 / v2c Settings' section has 'SNMP v1 / v2c:' checked (enable), 'Read Community String:' set to 'public', and 'Write Community String:' empty. The 'SNMP v3 Settings' section has 'SNMP v3:' unchecked (disable). The 'MIB-II System Group' section has 'sysContact:', 'sysName:', and 'sysLocation:' fields, all of which are empty. At the bottom, there is a 'Download MIB' button and 'OK' and 'Cancel' buttons.

2. Enable or disable "SNMP v1 / v2c" and/or "SNMP v3" by clicking the corresponding "enable" checkbox. For details, see **Enabling SNMP** (on page 207).
  - 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 PXE 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 215).*

---

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 210)
  - **SNMPv3 Notifications** (on page 212)
5. Click OK.

---

*Tip: The SNMP notification destinations can be also set in the Event Rule Settings dialog. See **Modifying an Action** (on page 170).*

---

### **Changing Modbus/TCP Settings**

You can enable or disable the Modbus/TCP access to the PXE 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 PXE 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 PXE. 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 69).*

---

#### ► 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 PXE 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 PXE 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 PXE follows the NTP server sanity check per the IETF RFC. If your PXE has problems synchronizing with a Windows NTP server, see **Windows NTP Server Synchronization Solution** (on page 85).

---

*Note: If you are using Sunbird's Power IQ to manage the PXE, you must configure Power IQ and the PXE 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.



- 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.
- 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 PXE follows the NTP RFC so the PXE 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 PXE.

---

*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 PXE. When the NTP synchronization issue occurs, change the dispersion settings to resolve it.

► **To change the Windows NTP's root dispersion settings:**

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

*HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config*

2. *AnnounceFlags* must be set to 0x05 or 0x06.
  - 0x05 = 0x01 (Always time server) and 0x04 (Always reliable time server)
  - 0x06 = 0x02 (Automatic time server) and 0x04 (Always reliable time server)

---

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

---

3. *LocalClockDispersion* must be set to 0.

---

### Setting Default Measurement Units

Default measurement units are applied to the PXE 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 96). If your preferences are different from the default measurement units, your preferences rather than the defaults apply to the PXE 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.

---

### Specifying the Device Altitude

You must specify the PXE 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 437).

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 86).

► **To specify the altitude of the PXE 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 68).*

---

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.

---

### Setting Data Logging

The PXE 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 PXE 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 that the outlet-level measurement data is NOT available for Raritan models described in this User Guide.

---

*Note: The PXE device's SNMP agent must be enabled for this feature to work. See **Enabling SNMP** (on page 207). 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 PXE in Step 4, it is NOT recommended.**

---

### Configuring SMTP Settings

The PXE 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 171).

---

*Note: See **Event Rules and Actions** (on page 135) 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.

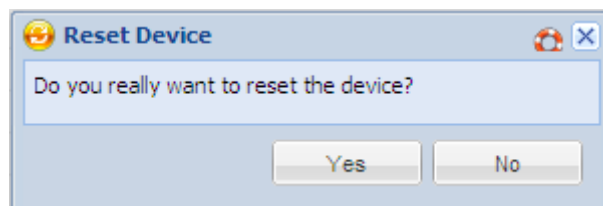
---

### Rebooting the PXE Device

You can remotely reboot the PXE device via the web interface.

#### ► To reboot the device:

1. Choose Maintenance > Unit Reset. The Reset Device dialog appears.



2. Click Yes to reset the PXE.
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 PXE 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 PXE 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 PXE:**

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 68).*

---

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 PXE 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 131).*

---

---

### Internal Beeper State

The PXE does NOT have an internal beeper so the 'Internal Beeper' section on the PDU page always shows "Off."

---

### 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 PXE device so that this device becomes part of the Cisco EnergyWise domain.

The Cisco EnergyWise feature implemented on the PXE 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 PXE 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 PXE is queried in the Cisco EnergyWise domain. The polling interval ranges from 30 to 600 seconds. Default is 180 seconds.
7. Click OK.

---

## User Management

The PXE 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 96).

---

*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	<p>The name the user enters to log in to the PXE.</p> <ul style="list-style-type: none"> <li>▪ 4 to 32 characters</li> <li>▪ Case sensitive</li> <li>▪ Spaces are NOT permitted.</li> </ul>

Field	Type this...
Full Name	The user's first and last names.
Password, Confirm Password	<ul style="list-style-type: none"> <li>▪ 4 to 64 characters</li> <li>▪ Case sensitive</li> <li>▪ Spaces are permitted.</li> </ul>
Telephone Number	The user's telephone number
eMail Address	The user's email address <ul style="list-style-type: none"> <li>▪ Up to 64 characters</li> <li>▪ Case sensitive</li> </ul>

4. Select the Enabled checkbox. Enabled users can log in to the PXE 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 51).*

---

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 79).*

---

- 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: <ul style="list-style-type: none"> <li>▪ NoAuthNoPriv: No authentication and no privacy.</li> <li>▪ AuthNoPriv: Authentication and no privacy.</li> <li>▪ AuthPriv: Authentication and privacy. This is the default.</li> </ul>
Use Password as	<i>This checkbox is configurable only if AuthNoPriv</i>

Field	Description
Authentication Pass Phrase	<i>or AuthPriv is selected.</i> 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	<i>This checkbox is configurable only if AuthPriv is selected.</i> 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: <ul style="list-style-type: none"> <li>▪ MD5</li> <li>▪ SHA-1 (default)</li> </ul>
Privacy Protocol	Click the drop-down arrow and select the desired privacy protocol from the list. Two protocols are available: <ul style="list-style-type: none"> <li>▪ DES (default)</li> <li>▪ AES-128</li> </ul>

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 77).
  - 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 96) 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 97).
    - *Create a new role by clicking the Manage Roles button:* See **Creating a Role** (on page 97).

---

*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 96).*

---

---

### 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 91).
  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 97).
  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 PXE 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 91).*

---

*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 86) for information on changing default measurement units.*

---

► **To change the measurement units applied to your PXE 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 PXE 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

The Operator role is assigned to a newly created user profile by default. See **Creating a User Profile** (on page 91).

---

## Creating a Role

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

### ► To create a role:

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

---

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

---

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

Now you can assign the new role to any users. See **Creating a User Profile** (on page 91) or **Modifying a User Profile** (on page 94).

---

## Modifying a Role

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

### ► To modify a role:

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

---

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

---

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

---

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

---

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

---

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

---

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

---

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

---

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

---

### Deleting a Role

You can delete any role other than the Admin role.

► **To delete a role:**

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

---

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

---

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

---

### Forcing HTTPS Encryption

You can force all accesses to the PXE via HTTP to be redirected to HTTPS. See **Changing HTTP(S) Settings** (on page 76).

---

### Access Security Control

The PXE 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 114) and **Setting Up External Authentication** (on page 120).*

---

---

#### Configuring the Firewall

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

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

By default the firewall is disabled.

► **To configure the firewall:**

1. Enable the firewall. See **Enabling the Firewall** (on page 100).

2. Set the default policy. See **Changing the Default Policy** (on page 100).
3. Create firewall rules specifying which addresses to accept and which ones to discard. See **Creating Firewall Rules** (on page 101).

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 PXE 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 PXE or receive any data from the PXE.

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 PXE to all IP addresses.
- Drop: Discards traffic sent from the PXE to all IP addresses, without sending any failure notification to the destination host.
- Reject: Discards traffic sent from the PXE 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 PXE, 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 PXE 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 PXE.

- **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	<ul style="list-style-type: none"> <li>▪ Click Append. The "Append new Rule" dialog appears.</li> <li>▪ Type an IP address and subnet mask in the IP/Mask field.</li> <li>▪ Select Accept, Drop or Reject from the drop-down list in the Policy field. <ul style="list-style-type: none"> <li>▪ Accept: Accepts traffic from/to the specified IP address(es).</li> <li>▪ Drop: Discards traffic from/to the specified IP address(es), without sending any failure notification to the source or destination host.</li> <li>▪ 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.</li> </ul> </li> <li>▪ Click OK.</li> </ul> <p>The system automatically numbers the rule.</p>

Action	Procedure
Insert a rule between two existing rules	<ul style="list-style-type: none"><li>▪ 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.</li><li>▪ Click Insert. The "Insert new Rule" dialog appears.</li><li>▪ Type an IP address and subnet mask in the IP/Mask field.</li><li>▪ Select Accept, Drop or Reject from the drop-down list in the Policy field.<ul style="list-style-type: none"><li>▪ Accept: Accepts traffic from/to the specified IP address(es).</li><li>▪ Drop: Discards traffic from/to the specified IP address(es), without sending any failure notification to the source or destination host.</li><li>▪ 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.</li></ul></li><li>▪ Click OK.</li></ul> <p>The system inserts the rule and automatically rennumbers the following rules.</p>

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

**Configure IP Access Control Settings**

**IPv4** | IPv6

Enable IPv4 Access Control: ☒

**Inbound Rules**

Default Policy: Accept

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

Append Insert Edit Delete

**Outbound Rules**

Default Policy: Accept

#	IP/Mask	Policy
1	192.168.88.88/24	REJECT

Append Insert Edit Delete

OK Cancel

- 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:

- 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 PXE 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 PXE 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 338).*

---

#### ► 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 PXE 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 PXE, 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 PXE.*

---

### Enabling Strong Passwords

Use of strong passwords makes it more difficult for intruders to crack user passwords and access the PXE 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 PXE 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 PXE restricted service agreement (security banner) if you want to require users to read and accept a security agreement when they log in to the PXE.

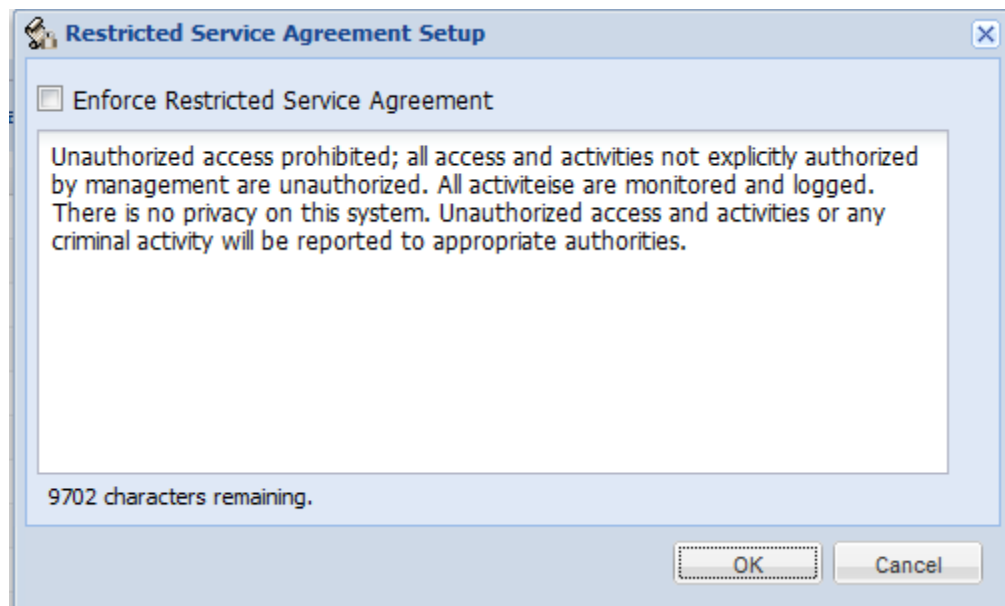
A default agreement is provided. You can edit or replace the default text as needed by typing directly in the security dialog or pasting text into it.

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 157)

#### ► 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 PXE. Do either of the following, or you cannot successfully log in to the PXE:

- 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 110).
2. Set the default policy. See **Changing the Default Policy** (on page 111).
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 111).

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	<ul style="list-style-type: none"> <li>▪ Click Append. The "Append new Rule" dialog appears.</li> <li>▪ Type a starting IP address in the Starting IP Address field.</li> <li>▪ Type an ending IP address in the Ending IP Address field.</li> <li>▪ Select a role from the drop-down list in the Role field. This rule applies to members of this role only.</li> <li>▪ Select Allow or Deny from the drop-down list in the Policy field. <ul style="list-style-type: none"> <li>▪ Allow: Accepts traffic from the specified IP address range when the user is a member of the specified role</li> <li>▪ Deny: Drops traffic from the specified IP address range when the user is a member of the specified role</li> </ul> </li> <li>▪ Click OK.</li> </ul> <p>The system automatically numbers the rule.</p>
Insert a rule between two existing rules	<ul style="list-style-type: none"> <li>▪ 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.</li> <li>▪ Click Insert. The "Insert new Rule" dialog appears.</li> <li>▪ Type a starting IP address in the Starting IP Address field.</li> <li>▪ Type an ending IP address in the Ending IP Address field.</li> <li>▪ Select a role from the drop-down list in the Role field. This rule applies to members of this role only.</li> <li>▪ Select Allow or Deny from the drop-down list in the Policy field. <ul style="list-style-type: none"> <li>▪ Allow: Accepts traffic from the specified IP address range when the user is a member of the specified role</li> <li>▪ Deny: Drops traffic from the specified IP address range when the user is a member of the specified</li> </ul> </li> </ul>



Action	Do this...
	<p>role</p> <ul style="list-style-type: none"> <li>Click OK.</li> </ul> <p>The system inserts the rule and automatically renumbers the following rules.</p>

- 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:

- Choose Device Settings > Security > Role Based Access Control. The Configure Role Based Access Control Settings dialog appears.
- To modify the IPv4 firewall rules, click the IPv4 tab. To modify the IPv6 firewall rules, click the IPv6 tab.
- 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.
- Select the rule to be modified in the rules list.
- Click Edit or double-click the rule. The Edit Rule dialog appears.
- Make changes to the information shown.
- 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:

- Choose Device Settings > Security > Role Based Access Control. The Configure Role Based Access Control Settings dialog appears.
- To sort the IPv4 firewall rules, click the IPv4 tab. To sort the IPv6 firewall rules, click the IPv6 tab.
- 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.
- Select a specific rule by clicking it.
- 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 PXE, 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 PXE 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 99) for instructions on forcing users to employ TLS when connecting to the PXE.*

---

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

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

---

### Certificate Signing Request

When appropriate certificate and key files for the PXE are NOT available, one of the alternatives is to create a CSR and private key on the PXE 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 PXE 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 <b>ISO website</b> ( <a href="http://www.iso.org/iso/country_codes/iso_3166_code_lists.htm">http://www.iso.org/iso/country_codes/iso_3166_code_lists.htm</a> ).
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 PXE 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 PXE device's response.
Self Sign	<b>For requesting a certificate signed by the CA, ensure this checkbox is NOT selected.</b>
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 PXE 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 PXE 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 PXE 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 PXE 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 <b>ISO website</b> ( <a href="http://www.iso.org/iso/country_codes/iso_3166_code_lists.htm">http://www.iso.org/iso/country_codes/iso_3166_code_lists.htm</a> ).
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 PXE 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 PXE device's response.
Self Sign	<b>Ensure this checkbox is selected, which indicates that you are creating a self-signed certificate.</b>
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 PXE device, click "Delete Key and Certificate".
6. If you installed the self-signed certificate in Step 5, after the installation completes, the PXE 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 PXE 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 PXE device for backup or other operations. For example, you can install the files on a replacement PXE device, add the certificate to your browser and so on.

► **To download the certificate and key files from the PXE 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 PXE 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 PXE 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 PXE must be authenticated. The PXE supports the access using one of the following authentication mechanisms:

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

By default, the PXE 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 PXE with information about the external Authentication and Authorization (AA) server.

If both local and external authentication is needed, create user profiles on the PXE in addition to providing the external AA server's data.

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

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 PXE 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 PXE. 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 171).

---

*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 PXE 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 PXE to verify the validity of the selected LDAP server certificate. For example, the PXE 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 PXE 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 PXE 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 PXE, 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 PXE 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 PXE 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 PXE 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 PXE 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 388).

For more information on RADIUS configuration, see **RADIUS Configuration Illustration** (on page 403).

---

#### Sorting the Access Order

The order of the authentication server list determines the access priority of remote authentication servers. The PXE 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 PXE device successfully connects to one of the listed servers.

---

*Note: After successfully connecting to one external authentication server, the PXE 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 PXE 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 PXE authenticates users against the local database stored on the PXE 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 PXE follows these rules for authentication:

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

The PXE allows you to remotely customize the name of each outlet or check the receptacle type of each outlet through the web interface.

---

### 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. Click Outlets in the PX Explorer pane, and the Outlets page opens in the right pane.
2. Select the outlet you want in the right pane. Or you can select the desired outlet in the PX Explorer pane to open that outlet's page.
3. Click Setup in the right pane. The setup dialog for the selected outlet appears.



4. Type a name in the Outlet Name field.
5. Click OK.

---

### Checking Outlet-Specific Data

To find out each outlet's name, label, and receptacle type, you can check the Outlets page or each individual outlet's page.

---

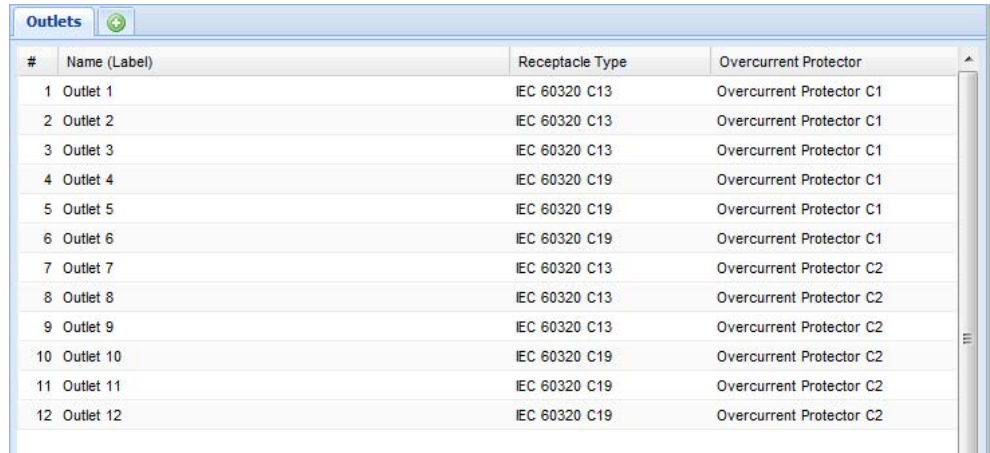
*Tip: More outlet information is available by choosing Maintenance > Device Information. See **Displaying PDU Information** (on page 67).*

---

#### ► To check the information of all outlets:

- Click Outlets in the PX Explorer pane, and the Outlets page opens in the right pane.

All outlets are listed with outlet-specific information.



#	Name (Label)	Receptacle Type	Overcurrent Protector
1	Outlet 1	IEC 60320 C13	Overcurrent Protector C1
2	Outlet 2	IEC 60320 C13	Overcurrent Protector C1
3	Outlet 3	IEC 60320 C13	Overcurrent Protector C1
4	Outlet 4	IEC 60320 C19	Overcurrent Protector C1
5	Outlet 5	IEC 60320 C19	Overcurrent Protector C1
6	Outlet 6	IEC 60320 C19	Overcurrent Protector C1
7	Outlet 7	IEC 60320 C13	Overcurrent Protector C2
8	Outlet 8	IEC 60320 C13	Overcurrent Protector C2
9	Outlet 9	IEC 60320 C13	Overcurrent Protector C2
10	Outlet 10	IEC 60320 C19	Overcurrent Protector C2
11	Outlet 11	IEC 60320 C19	Overcurrent Protector C2
12	Outlet 12	IEC 60320 C19	Overcurrent Protector C2

#### ► To check the information of an individual outlet:

1. Expand the Outlets folder to show all outlets in the PX Explorer pane. See **Expanding the Tree** (on page 57).
2. Click the desired outlet in the PX Explorer pane. Its page opens in the right pane, with that outlet's details shown.

---

## 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 133).*

---

---

### 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 PXE 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.

---

### 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 61).*

---

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.

---

### **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 57).
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.

---

### **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 PXE 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 PXE has multiple inlets, expand the Inlet folder in the PX Explorer pane to show all inlets. See **Expanding the Tree** (on page 57). If your PXE 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 90).*

---

---

### **Disabling an Inlet (for Multi-Inlet PDUs)**

The PXE, if it has more than one inlet, enables all inlets by default so that the PXE 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.*

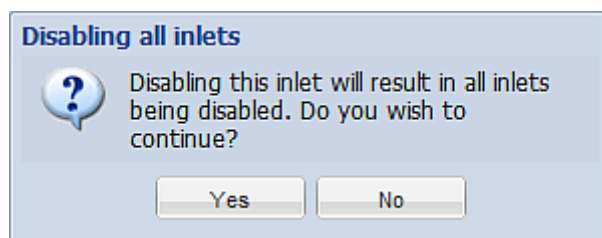
---

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 PXE 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 61).

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 440).

---

*Note: After setting the thresholds, remember to configure event rules. See **Event Rules and Actions** (on page 135).*

---

## 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 445).
7. To set the assertion timeout, type a numeric value in the Assertion Timeout (samples) field. See ***"To Assert" and Assertion Timeout*** (on page 443).
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.**

---

---

## 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 PXE is shipped with four built-in event rules, which cannot be deleted.

- **System Event Log Rule:** This causes ANY event occurred to the PXE 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 PXE. It is disabled by default.
- **System Tamper Detection Alarmed:** This causes the PXE to send alarm notifications if a DX tamper sensor has been connected and the PXE detects that the tamper sensor enters the alarmed state.
- **System Tamper Detection Unavailable:** This causes the PXE to send alarm notifications if a DX tamper sensor has been connected and the PXE 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 PXE does in certain situations and is composed of two parts:

- **Event:** This is the situation where the PXE 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 PXE 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 PXE 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 PXE 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 65).

---

*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 <b>Action Group</b> (on page 137).
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 <b>Alarm</b> (on page 138).
Log event message	Records the selected events in the internal log. See <b>Log an Event Message</b> (on page 140).



Action	Function
Send email	Emails a textual message. See <b>Send EMail</b> (on page 140).
Send SNMP notification	Sends SNMP traps or informs to one or multiple SNMP destinations. See <b>Send an SNMP Notification</b> (on page 141).
Syslog message	Makes the PXE automatically forward event messages to the specified syslog server. See <b>Syslog Message</b> (on page 143).
Send sensor report	Reports the readings or status of the selected sensors, including internal or external sensors. See <b>Send Sensor Report</b> (on page 145).
Switch peripheral actuator	Switches on or off the mechanism or system connected to the specified actuator. See <b>Switch Peripheral Actuator</b> (on page 146).

---

*Note: The PXE does NOT support the connection of an external beeper, modem, or webcam so do NOT select unsupported actions, including "External beeper," "Send snapshots via SMTP," "Send SMS message" and "Record snapshots to webcam storage."*

---

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 PXE 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 65).





#### **► 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

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 PXE 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.

### **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.

### **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 PXE placeholders. The placeholders represent information is pulled from the PXE 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 164) 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 88) for the information of each field. Default messages are sent based on the event. See **Default Log Messages** (on page 157) 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 164) 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 PXE 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. <ul style="list-style-type: none"> <li>• Select the authentication protocol - MD5 or SHA</li> <li>• Enter the authentication passphrase and then confirm the authentication passphrase</li> </ul>
"authPriv"	Select this if authentication and privacy protocols are required. <ul style="list-style-type: none"> <li>• Select the authentication protocol - MD5 or SHA</li> <li>• Enter the authentication passphrase and confirm the authentication passphrase</li> <li>• Select the Privacy Protocol - DES or AES</li> <li>• Enter the privacy passphrase and then confirm the privacy passphrase</li> </ul>

### **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 PXE 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 171).

#### **► 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	<ul style="list-style-type: none"> <li>▪ In the UDP Port field, specify an appropriate port number. Default is 514.</li> <li>▪ Select the "Legacy BSD Syslog Protocol (UDP only)" checkbox if applicable.</li> </ul>
TCP	<p>If NO TLS certificate is required, type an appropriate port number in the TCP Port field.</p> <p>If a TLS certificate is required, select the "Enable Secure Syslog over TLS" checkbox, and then do the following:</p> <ol style="list-style-type: none"> <li>a. Specify an appropriate port number in the "TCP Port (TLS)" field. Default is 6514.</li> <li>b. In the CA Certificate field, click Browse to select a TLS certificate. After installing the certificate, you may: <ul style="list-style-type: none"> <li>▪ Click Show to view its contents.</li> <li>▪ Click Remove to delete it if it is inappropriate.</li> </ul> </li> <li>c. Determine whether to select the "Allow expired and not yet valid certificates" checkbox. <ul style="list-style-type: none"> <li>▪ To always send the event message to the specified syslog server after a TLS certificate has been installed, select this checkbox.</li> <li>▪ 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.</li> </ul> </li> </ol>

8. Click OK.



**Send Sensor Report**


You may set the PXE 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 PXE, 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 164).*

---

#### **Switch Peripheral Actuator**

If you have any actuator connected to the PXE, you can set up the PXE 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 PXE, see **DX Sensor Packages** (on page 34).*


---

#### **► 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.

### 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 PXE 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	<p>Available radio buttons include "Asserted," "Deasserted" and "Both."</p> <ul style="list-style-type: none"> <li>▪ Asserted: The PXE takes the action only when the event occurs. This means the status of the described event transits from FALSE to TRUE.</li> <li>▪ Deasserted: The PXE takes the action only when the event condition disappears. This means the status of the described event transits from TRUE to FALSE.</li> <li>▪ Both: The PXE takes the action both when the event occurs (asserts) and when the event condition disappears (deasserts).</li> </ul>
Discrete (on/off) sensor state change	<p>Available radio buttons include "Alarmed/Open/On," "No longer alarmed/Closed/Off" and "Both."</p> <ul style="list-style-type: none"> <li>▪ Alarmed/Open/On: The PXE takes the action only when the chosen sensor enters the alarmed, open or on state.</li> <li>▪ No longer alarmed/Closed/Off: The PXE takes the action only when the chosen sensor returns to the normal, closed or off state.</li> <li>▪ Both: The PXE takes the action whenever the chosen sensor switches its state.</li> </ul>

Event types	Radio buttons
Sensor availability	<p>Available radio buttons include "Unavailable," "Available" and "Both."</p> <ul style="list-style-type: none"> <li>Unavailable: The PXE takes the action only when the chosen sensor is NOT detected and becomes unavailable.</li> <li>Available: The PXE takes the action only when the chosen sensor is detected and becomes available.</li> <li>Both: The PXE takes the action both when the chosen sensor becomes unavailable or available.</li> </ul>
Network interface link state	<p>Available radio buttons include "Link state is up," "Link state is down" and "Both."</p> <ul style="list-style-type: none"> <li>Link state is up: The PXE takes the action only when the network link state changes from down to up.</li> <li>Link state is down: The PXE takes the action only when the network link state changes from up to down.</li> <li>Both: The PXE takes the action whenever the network link state changes.</li> </ul>
Function enabled or disabled	<p>Available radio buttons include "Enabled," "Disabled" and "Both."</p> <ul style="list-style-type: none"> <li>Enabled: The PXE takes the action only when the chosen function is enabled.</li> <li>Disabled: The PXE takes the action only when the chosen function is disabled.</li> <li>Both: The PXE takes the action when the chosen function is either enabled or disabled.</li> </ul>
User logon state	<p>Available radio buttons include "Logged in," "Logged out," and "Both."</p> <ul style="list-style-type: none"> <li>Logged in: The PXE takes the action only when the selected user logs in.</li> <li>Logged out: The PXE takes the action only when the selected user logs out.</li> <li>Both: The PXE takes the action both when the selected user logs in and logs out.</li> </ul>

Event types	Radio buttons
Restricted service agreement	<p>Available radio buttons include "Accepted," "Declined," and "Both."</p> <ul style="list-style-type: none"> <li>Accepted: The PXE takes the action only when the specified user accepts the restricted service agreement.</li> <li>Declined: The PXE takes the action only when the specified user rejects the restricted service agreement.</li> <li>Both: The PXE takes the action both when the specified user accepts or rejects the restricted service agreement</li> </ul>
Server monitoring event	<p>Available radio buttons include "Monitoring started," "Monitoring stopped," and "Both."</p> <ul style="list-style-type: none"> <li>Monitoring started: The PXE takes the action only when the monitoring of any specified server starts.</li> <li>Monitoring stopped: The PXE takes the action only when the monitoring of any specified server stops.</li> <li>Both: The PXE takes the action when the monitoring of any specified server starts or stops.</li> </ul>
Server reachability	<p>Available radio buttons include "Unreachable," "Reachable," and "Both."</p> <ul style="list-style-type: none"> <li>Unreachable: The PXE takes the action only when any specified server becomes inaccessible.</li> <li>Reachable: The PXE takes the action only when any specified server becomes accessible.</li> <li>Both: The PXE takes the action when any specified server becomes either inaccessible or accessible.</li> </ul>

Event types	Radio buttons
Device connection or disconnection, such as a USB-cascaded slave device	<p>Available radio buttons include "Connected," "Disconnected" and "Both."</p> <ul style="list-style-type: none"> <li>Connected: The PXE takes the action only when the selected device is physically connected to it.</li> <li>Disconnected: The PXE takes the action only when the selected device is physically disconnected from it.</li> <li>Both: The PXE takes the action both when the selected device is physically connected to it and when it is disconnected.</li> </ul>

*Note: The PXE does NOT support events related to asset management, modem, webcam, USB-cascading, power metering controller and Schrott LHX/SHX devices.*

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 PXE 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 PXE 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
<b>Minutes</b>	The frequency in minutes ranges from every minute, every 5 minutes, every 10 minutes and so on until every 30 minutes.
<b>Hourly</b>	The hourly option sets the timing to either of the following: <ul style="list-style-type: none"> <li>▪ 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.</li> <li>▪ 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.</li> </ul>
<b>Daily</b>	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.
<b>Weekly</b>	Both the day and time must be specified for the weekly option. Days range from Sunday to Monday.
<b>Monthly</b>	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.
<b>Yearly</b>	This option requires three settings: <ul style="list-style-type: none"> <li>▪ Month - January through December.</li> <li>▪ Date - 1 to 31.</li> <li>▪ Time - the value is specified in 24-hour format.</li> </ul>

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 136).

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**

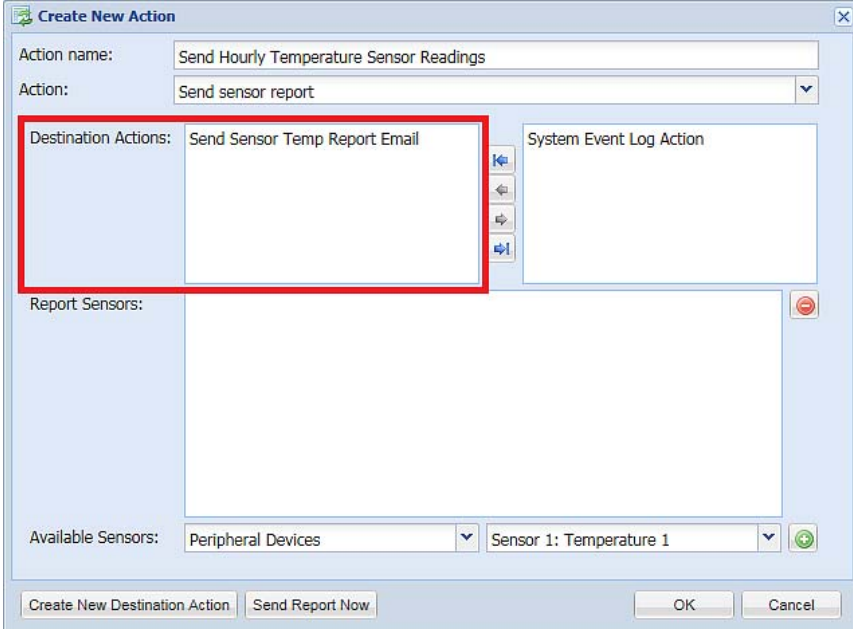
Below is an example of a scheduled action set to send a temperature sensor report via email hourly.

In this example,

- 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).
- 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.
- 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:**

- If you have not already done so, create the destination action 'Send Sensor Temp Report Email', which is performed when the 'Send Hourly Temperature Sensor Readings' action occurs.



**Create New Action**

Action name:

Action:

Destination Actions:

Report Sensors:

Available Sensors:

- 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 140).

**Create New Action**

Action name: Send Sensor Temp Report Email

Action: Send Email

Recipients email addresses: sensor\_reporting@raritan.com

☒ Use Default SMTP Server

Server Name: mail.raritan.info

Sender Email Address: test-mkr@peppercon.de

☐ Use Custom SMTP Settings

☒ Use Custom Log Message

Hourly sensor report

2. Create the 'Send sensor report' action -- *Send Hourly Temperature Sensor Readings*.
  - a. Choose Device Settings > Event Rules. The Event Rule Settings dialog appears.
  - b. Click the Actions tab > New.
  - c. Enter the following information.

- Type the action's name -- *Send Hourly Temperature Sensor Readings*.
- Select the 'Send sensor report' action.
- Select the destination action 'Send Sensor Temp Report Email'.
- Add the desired temperature sensor(s) from the Available Sensors list to the Report Sensors box.

The screenshot shows the 'Create New Action' dialog box. The 'Action name' field is filled with 'Send Hourly Temperature Sensor Readings'. The 'Action' dropdown menu is set to 'Send sensor report', which is highlighted with a red rectangular box. Below this, the 'Destination Actions' section shows two options: 'Send Sensor Temp Report Email' and 'System Event Log Action'. The 'Report Sensors' section is currently empty. At the bottom, the 'Available Sensors' dropdown is set to 'Peripheral Devices', and a specific sensor, 'Sensor 1: Temperature 1', is selected and highlighted with a red rectangular box. The dialog box includes standard buttons at the bottom: 'Create New Destination Action', 'Send Report Now', 'OK', and 'Cancel'.

- d. Click OK. For details, see ***Send Sensor Report*** (on page 145).
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 152).

Then the PXE 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 PXE events occur (are TRUE) or, in some cases, do not occur (are FALSE). See **Send Email** (on page 140) 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]:[SNMPMANAGER PORT] 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 incorrect system clock.	
Energywise > Enabled	User '[USERNAME]' from host '[USERIP]' enabled EnergyWise.	User '[USERNAME]' from host '[USERIP]' disabled EnergyWise.
Peripheral Device Slot > * > Numeric Sensor > Unavailable	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' unavailable.	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' available.
Peripheral Device Slot > * > Numeric Sensor > Above upper critical	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].
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].



Event/Context	Default Assertion Message when the Event = TRUE	Default Assertion Message when the Event = FALSE*
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]'. [REASON]	
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 > * > Above upper critical	Sensor '[POLESENSOR]' on pole '[INLETPOLE]' of inlet '[INLET]' asserted 'above upper critical'.	Sensor '[POLESENSOR]' on pole '[INLETPOLE]' of inlet '[INLET]' 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'.

Event/Context	Default Assertion Message when the Event = TRUE	Default Assertion Message when the Event = FALSE*
		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.	
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	User '[TARGETUSER]' modified by	

Event/Context	Default Assertion Message when the Event = TRUE	Default Assertion Message when the Event = FALSE*
modified	user '[USERNAME]' from host '[USERIP]'.	
User Administration > User deleted	User '[TARGETUSER]' deleted by user '[USERNAME]' from host '[USERIP]'.	
User Administration > Password changed	Password of user '[TARGETUSER]' changed by user '[USERNAME]' from host '[USERIP]'.	
User Administration > Password settings changed	Password settings changed by user '[USERNAME]' from host '[USERIP]'.	
User Administration > Role added	Role '[TARGETROLE]' added by user '[USERNAME]' from host '[USERIP]'.	
User Administration > Role modified	Role '[TARGETROLE]' modified by user '[USERNAME]' from host '[USERIP]'.	
User Administration > Role deleted	Role '[TARGETROLE]' deleted by user '[USERNAME]' from host '[USERIP]'.	
Webcam Management > Webcam attached	Webcam '[WEBCAMNAME]' ('[WEBCAMUVCID]') added to port '[WEBCAMUSBPORT]'.	
Webcam Management > Webcam detached	Webcam '[WEBCAMNAME]' ('[WEBCAMUVCID]') removed from port '[WEBCAMUSBPORT]'.	
Webcam Management > Webcam settings changed	Webcam '[WEBCAMNAME]' settings changed by user '[USERNAME]'.	
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 PXE does NOT support events related to asset management, modem, webcam, USB-cascading, power metering controller and Schroff LHX/SHX devices.*

---

### 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
[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

Placeholder	Definition
[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
[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

Placeholder	Definition
[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
[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 PXE 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 PXE 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 Inlet-Level Event Rule

In this example, we want the PXE 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 209).*

---

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.

---

### 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 PXE 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 PXE 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 PXE to send out SMTP messages when one of the selected events listed on the Device menu occurs. Note that <Any sub-event> under the Device menu includes the event "Sending SMTP message failed."

Event selected	Action included
Device > Any sub-event	Send email

---

### Modifying an Event Rule

You can change an event rule's event, action, trigger condition and other settings, if any.

---

*Exception: Events and actions selected in the built-in event rules are not changeable, including System Event Log Rule, System SNMP Notification Rule, System Tamper Detection Alarmed, and System Tamper Detection Unavailable.*

---

#### ► To modify an event rule:

1. Choose Device Settings > Event Rules. The Event Rule Settings dialog appears.
2. On the Rules tab, select the event rule that you want to modify and click Edit, or simply double-click that rule.
3. To disable the event rule, deselect the Enabled checkbox.
4. To change the event, click the desired tab in the Event field and select a different item from the pull-down menu or submenu.



For example, in a user activity event rule for the "admin" user, you can click the "admin" tab to display a pull-down submenu showing all user names, and then select a different user name or all users (shown as <Any user>).

The screenshot shows a configuration window for a rule named "Example rule". The "Enabled" checkbox is checked. Under the "Event" section, "User Activity" is selected, and a pull-down menu is open showing a list of users: "admin", "tester", "John", "Mary", "<Any user>", and "<Any sub-event>". A red arrow points to the "admin" option in this menu. To the right, "Authentication failure" is also visible. Under the "Actions" section, there are two lists: "Selected actions" containing "System SNMP" and "Available actions" containing "System Event Log Action" and "System Tamper Alarm".

5. If the "Trigger condition" field is available, you may select a radio button other than the current selection to change the rule triggering condition.
6. To change the action(s), do any of the following in the Actions field:
  - To add any action, select it from the "Available actions" list box, and click . To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.
  - To add all actions, click .
  - To remove any action, select it from the "Selected actions" list box, and click to move it back to the "Available actions" list box. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.
  - To remove all actions, click .
  - To create a new action, click Create New Action. The newly created action will be moved to the "Selected actions" list box once it is created. See **Creating Actions** (on page 136) 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 PXE to generate an alert. The measurement then returns to a value within the threshold, but the PXE does not generate an alert message for the Deassertion event. Such scenarios can occur due to the hysteresis tracking the PXE uses. See *"To De-assert" and Deassertion Hysteresis* (on page 445).

---

## Managing Event Logging

By default, the PXE 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 PXE 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 Connected Users

You can see which users are connected to the PXE device and their status. If you have administrator privileges, you can terminate any user's connection to the PXE 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.

Column	Description
Client Type	<p>The interface through which the user is being connected to the PXE.</p> <ul style="list-style-type: none"> <li>▪ Web GUI: Refers to the PXE web interface.</li> <li>▪ CLI: Refers to the command line interface (CLI).</li> </ul> <p>The information in parentheses following "CLI" indicates how this user is connected to the CLI.</p> <ul style="list-style-type: none"> <li>- <i>Serial</i>: Represents the local connection (serial RS-232 or USB).</li> <li>- <i>SSH</i>: Represents the SSH connection.</li> <li>- <i>Telnet</i>: Represents the Telnet connection.</li> </ul>
Idle Time	<p>The length of time for which a user remains idle.</p> <p>The unit "min" represents minutes.</p>

2. To disconnect any user, click the corresponding Disconnect button.
  - a. A dialog appears, prompting you to confirm the operation.

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.

---

## Monitoring Server Accessibility

You can monitor whether specific IT devices are alive by having the PXE 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

PXE can monitor the accessibility of any type of IT equipment, such as database servers, remote authentication servers, power distribution units (PDUs), and so on.

PXE 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 PXE 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 135).*

---

#### ► To add IT equipment for ping monitoring:

1. Choose Device Settings > Server Reachability. The Server Reachability dialog appears.
2. Click New. The Add New Server dialog appears.
3. By default, the "Enable ping monitoring for this server" checkbox is selected. If not, select it to enable this feature.
4. Provide the information required.

Field	Description
IP address/hostname	IP address or host name of the IT equipment which you want to monitor.
Number of successful pings to enable feature	The number of successful pings required to declare that the monitored equipment is "Reachable." Valid range is 0 to 200.
Wait time (in seconds) after successful ping	The wait time before sending the next ping if the previous ping was successfully responded. Valid range is 5 to 600 (seconds).
Wait time (in seconds) after unsuccessful ping	The wait time before sending the next ping if the previous ping was not responded. Valid range is 3 to 600 (seconds).
Number of consecutive unsuccessful pings for failure	The number of consecutive pings without any response before the monitored equipment is declared "Unreachable." Valid range is 1 to 100.

Field	Description
Wait time (in seconds) before resuming pinging after failure	The wait time before the PXE 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 PXE 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 PXE 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 PXE to make sure that PDU is properly operating all the time, and the PXE 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 PXE 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 PXE 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 PXE 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 PXE stops pinging the target PDU for 60 seconds (1 minute) after the PDU inaccessibility is declared. After 60 seconds, the PXE 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 PXE 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 209).*

---

---

### 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 PXE 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 PXE device and the monitored equipment is not reliably established yet.
---------------------------------	--

4. Click Close to quit the dialog.

---

## Environmental Sensors and Actuators

The PXE can monitor the environmental conditions, such as temperature and humidity, where environmental sensors are placed. If an actuator is connected to the PXE, you can use it to control a system or mechanism.

### ► To add environmental sensors and actuators:

1. Physically connect environmental sensor packages to the PXE device. See **Connecting Environmental Sensor Packages** (on page 22).
2. Log in to the PXE web interface. The PXE 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 179).
4. The PXE 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 182).
5. Configure the sensors and actuators. See **Configuring Environmental Sensors or Actuators** (on page 184). 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 179) and **Matching the Position** (on page 180) in the PXE 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 PXE.

► **To identify each detected environmental sensor or actuator via serial numbers:**

1. Click Peripheral Devices in the left pane.
2. Match the serial number from the tag to those listed in the sensor table.

Peripheral Devices									
ID	Name	Position	Serial Number	Type	Channel	Actuator	Reading	State	
1	Temperature 1	Port 1	AEI7A00022	Temperature			24.2 °C	normal	
2	Humidity 1	Port 1	AEI7A00022	Humidity			60 %	normal	
3	Temperature 2	Port 1	AEI7A00021	Temperature			24.4 °C	normal	
4	Humidity 2	Port 1	AEI7A00021	Humidity			59 %	normal	
5	On/Off 1	Port 1	PRC0190292	Contact (On/Off)	1			normal	
6	On/Off 2	Port 1	PRC0190292	Contact (On/Off)	2			normal	

**Matching the Position**

DPX2, DPX3 and DX sensor packages can be daisy chained. The PXE 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 PXE 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 PXE devices with only one SENSOR port, it always shows "Port 1."*

---

#### ▶ DPX2, DPX3 and DX sensor position information:

The PXE 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 PXE 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 PXE assigns ID numbers randomly because this option assumes that users do not care about the sequence. In this case, see the Channel column to identify each channel correctly. For example, CC1 or DC1 is Channel 1, CC2 or DC2 is Channel 2, and so on.

Peripheral Devices									
<input type="checkbox"/>	ID	Name	Position	Serial Number	Type	Channel	Actuator	Reading	State
<input type="checkbox"/>	1	On/Off 1	Port 1, Chain Position 1	QU74592507	Contact (On/Off)	5			normal
<input type="checkbox"/>	2	On/Off 2	Port 1, Chain Position 1	QU74592507	Contact (On/Off)	4			normal
<input type="checkbox"/>	3	On/Off 3	Port 1, Chain Position 1	QU74592507	Contact (On/Off)	3			normal
<input type="checkbox"/>	4	On/Off 4	Port 1, Chain Position 1	QU74592507	Contact (On/Off)	2			normal
<input type="checkbox"/>	5	On/Off 5	Port 1, Chain Position 1	QU74592507	Contact (On/Off)	1			normal
<input type="checkbox"/>	6	Powered Dry Contact 1	Port 1, Chain Position 1	QU74592507	Powered Dry Contact	2	✓		off
<input type="checkbox"/>	7	Powered Dry Contact 2	Port 1, Chain Position 1	QU74592507	Powered Dry Contact	1	✓		off

### Managing Environmental Sensors or Actuators

The PXE 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 PXE device can manage a maximum of 32 environmental sensors or actuators.

When there are less than 32 managed sensors or actuators, the PXE 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 194).*

#### ► 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 179).*

---

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 PXE 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 PXE 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 193).*

---

► **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<sup>3</sup>).



---

*Note: Prior to release 3.1.0, only relative humidity values are available.*

---

Relative humidity sensors can be "automatically" managed but absolute humidity sensors CANNOT. You must "manually" manage absolute humidity sensors if absolute humidity measurements are required.

Relative and absolute humidity values of the same humidity sensor share the same serial number and port position as illustrated below.

4	Relative Humidity 1	Port 1	AEI7A00022	 Relative Humidity	66 %	normal
5	Absolute Humidity 1	Port 1	AEI7A00022	 Absolute Humidity	14.7 g/m <sup>3</sup>	normal

However, relative and absolute values of the same humidity sensor DO NOT share the same ID number. The above diagram shows that the two values have different ID numbers -- one is 4 and the other is 5.

---

### Configuring Environmental Sensors or Actuators

You can change the default name to easily identify the managed sensor or actuator, and describe its location with X, Y and Z coordinates.

► **To configure environmental sensors or actuators:**

1. Click Peripheral Devices in the left pane.
2. Select the sensor or actuator that you want to configure.
3. Click Setup in the right pane. The "Setup of peripheral device <serial number> (<sensor type>)" dialog appears, where <serial number> is its serial number and <sensor type> is its type.

For example, *Setup of peripheral device AEI7A00022 (Temperature)*.

4. Configure available fields properly.



Fields	Description
Name	Assign a name for identification.
Description	Type any descriptive text as needed.
Location (X, Y and Z)	Describe the sensor's or actuator's location by assigning alphanumeric values to the X, Y and Z coordinates. See <b><i>Describing the Sensor's or Actuator's Location</i></b> (on page 187).  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 <b><i>Setting the Z Coordinate Format</i></b> (on page 186).
Binary Sensor Subtype	This field is available only when the selected sensor is a contact closure sensor. Select one of the following sensor types: <ul style="list-style-type: none"> <li>▪ Contact: The detector/switch is designed to detect the door lock or door open/closed status.</li> <li>▪ Smoke Detection: The detector/switch is designed to detect the appearance of smoke.</li> <li>▪ Water Detection: The detector/switch is designed to detect the appearance of water on the floor.</li> <li>▪ Vibration: The detector/switch is designed to detect the vibration in the floor.</li> </ul>
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 PXE 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 440) 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 445).

- To set the assertion timeout, type a numeric value in the Assertion Timeout (samples) field. See **"To Assert" and Assertion Timeout** (on page 443).

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 187).

---

*Note: The Upper Critical and Lower Critical values are points at which the PXE 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 188).*

---

### 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 68).*

---

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 PXE MIB. To configure and retrieve these values over the CLI, see **Using the Command Line Interface** (on page 218).*

---

### 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 184).

#### ► To change the default threshold settings:

1. Click Peripheral Devices in the left pane.

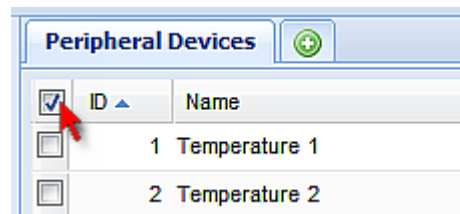
2. Click Default Thresholds Setup on the Peripheral Devices page. A dialog appears, showing a list of all numeric environmental sensor types.
3. Select the desired sensor type.
4. Click Edit or double-click that sensor type to adjust its threshold settings, deassertion hysteresis or assertion timeout.
  - 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 445).
  - To set the assertion timeout, type a numeric value in the Assertion Timeout (samples) field. See **"To Assert" and Assertion Timeout** (on page 443).
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 184).
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 PXE 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 61).


#### ► 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 PXE 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 PXE 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:

$$\text{Lower Warning threshold} \leq \text{Reading} < \text{Upper Warning threshold}$$


---

*Note: The symbol  $\leq$  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:

$$\text{Reading} < \text{Lower Critical Threshold}$$

### **"below lower warning" State**

This state means a numeric sensor's reading is below the lower warning threshold as indicated below:

$$\text{Lower Critical Threshold} \leq \text{Reading} < \text{Lower Warning Threshold}$$

---

*Note: The symbol  $\leq$  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:

$$\text{Upper Warning Threshold} \leq \text{Reading} < \text{Upper Critical Threshold}$$

---

*Note: The symbol  $\leq$  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:

$$\text{Upper Critical Threshold} <= \text{Reading}$$

---

*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 PXE 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 PXE device stops retrieving the sensor's reading and/or state. This procedure also applies if you want to unmanage an actuator.

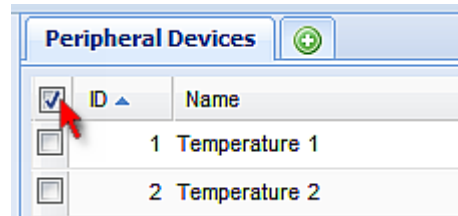
**► To release a managed sensor or actuator:**

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 194).
- If it is no longer connected to the PXE, 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 193).

---

### 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 PXE automatically brings newly-connected environmental sensors and actuators under management after detecting them.

When this feature is disabled, the PXE 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 68).*

---

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.*

---

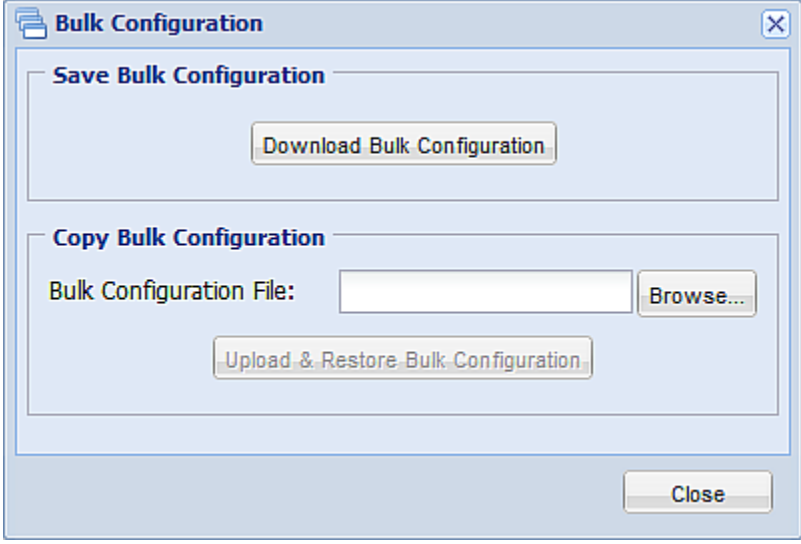
3. Click "Switch on" or "Switch off" to turn on or off the selected actuators. Confirm you want to switch when prompted.

---

## Bulk Configuration

The Bulk Configuration feature lets you save the settings of a configured PXE device to your PC. You can use this configuration file to copy that configuration to other PXE devices of the same model and firmware version.

You must have the Administrator Privileges or "Unrestricted View Privileges" to save and copy the PXE configurations.

A screenshot of a web-based dialog box titled "Bulk Configuration". The dialog has a light blue background and a standard window border with a close button (X) in the top right corner. It is divided into two main sections. The first section, titled "Save Bulk Configuration", contains a single button labeled "Download Bulk Configuration". The second section, titled "Copy Bulk Configuration", contains a text input field labeled "Bulk Configuration File:" followed by a "Browse..." button. Below this is a button labeled "Upload & Restore Bulk Configuration". At the bottom right of the dialog is a "Close" button.

---

*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 PXE device's all settings, use the Backup/Restore feature instead. See **Backup and Restore of PXE Device Settings** (on page 199).*

---

---

*Tip: For the alternative to configure multiple PXE devices, see **Bulk Configuration or Firmware Upgrade via DHCP/TFTP** (on page 351).*

---

---

### Saving the PXE Configuration

A source device is an already configured PXE device that is used to create a configuration file containing the settings that can be shared between PXE 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 PXE 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 385).*

---

---

### Copying the PXE Configuration

A target device is the PXE device that loads another PXE device's configuration file.

Copying a source PXE device's configuration to a target device adjusts the target PXE device's settings to match those of the source PXE device. In order to successfully copy a source PXE device's configuration:

- The user must be the Admin user. Or the Admin role is assigned to the user.
- The target PXE device must be running the same firmware version as the source PXE device.
- The target PXE device must be of the same model type as the source PXE 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 PXE 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 202).
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 PXE device resets and the Login page re-appears, indicating that the configuration copy is complete.

---

*Note: On startup, the PXE 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 385).*

---

## Backup and Restore of PXE Device Settings

Different from the Bulk Configuration file, the backup file contains device-specific data like network settings. To back up or restore PXE device settings, you should perform the Backup/Restore feature.

All PXE information is captured in the XML backup file except for the device logs and TLS certificate.

---

*Note: To perform the bulk configuration among multiple PXE devices, perform the Bulk Configuration feature instead. See **Bulk Configuration** (on page 196).*

---

### ► To download a backup PXE 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 PXE 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 PXE device resets and the Login page re-appears, indicating that the restore is complete.

---

*Note: On startup, the PXE 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 386).*

---

---

## Network Diagnostics

The PXE 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 340).*

---

---

### 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 PXE 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.

---

## Firmware Upgrade

You may upgrade your PXE 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 PXE Firmware

When performing the firmware upgrade, the PXE keeps each outlet's power status unchanged so no server operation is interrupted.

You must be the system administrator or log in to the user profile with the Firmware Update permission to update the PXE firmware.

Before starting the upgrade, read the release notes downloaded from the Raritan website's **Support page** (<http://www.raritan.com/support/>). If you have any questions or concerns about the upgrade, contact Raritan Technical Support BEFORE upgrading.

Warning: Do NOT perform the firmware upgrade over a wireless network connection.

### Firmware Update via Web Interface

After downloading the latest firmware, log in to the PXE 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 PXE 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 PXE shows three digits: 'FuP' or 'FUP.'
  - No users can successfully log in to the PXE.
  - 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 PXE 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 PXE 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 207) in the User Guide.*

---



---

*Tip: There are other alternatives to update the firmware. See **Firmware Update via SCP** (on page 384), and **Bulk Configuration or Firmware Upgrade via DHCP/TFTP** (on page 351).*

---

#### **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 PXE 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 PXE 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 PXE 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 PXE firmware file is required in the recovery procedure.

---

## Accessing the Help

The Help menu provides:

- Current firmware and software packages information
- A link to the PXE help

---

### Retrieving Software Packages Information

You can check the current firmware version and the information of all open source packages embedded in the PXE 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 PXE 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 Scriptlets. Consult your browser help for information on enabling these features.

#### ► To use the PXE 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 PXE for use with an SNMP manager. The PXE 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 .....	207
Configuring Users for Encrypted SNMP v3 .....	208
Configuring SNMP Notifications .....	209
SNMP Gets and Sets .....	214

---

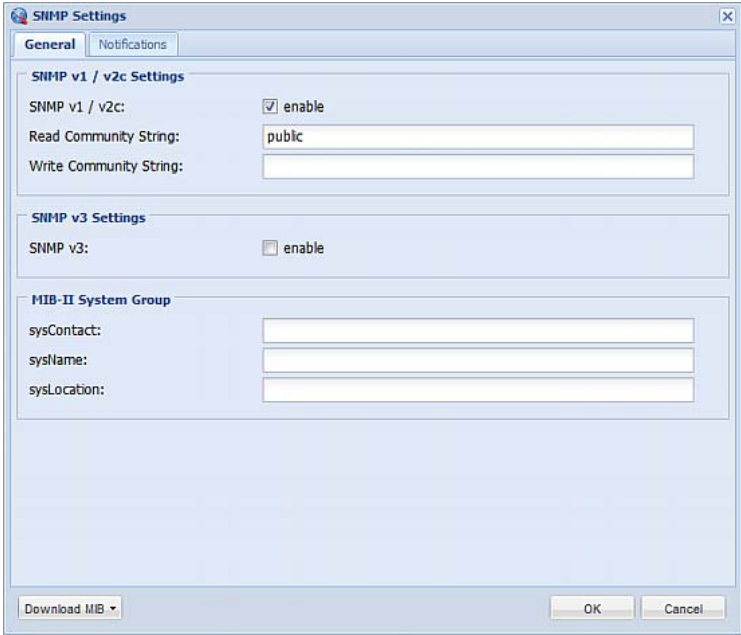
### Enabling SNMP

By default, SNMP v1/v2c is enabled on the PXE so the PXE 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.

The image shows the 'SNMP Settings' dialog box with the 'General' tab selected. It contains sections for 'SNMP v1 / v2c Settings' (with 'enable' checked and 'Read Community String' set to 'public'), 'SNMP v3 Settings' (with 'enable' unchecked), and 'MIB-II System Group' (with empty fields for 'sysContact:', 'sysName:', and 'sysLocation:'). At the bottom are 'Download MIB', 'OK', and 'Cancel' buttons.

General	
<b>SNMP v1 / v2c Settings</b>	
SNMP v1 / v2c:	<input checked="" type="checkbox"/> enable
Read Community String:	public
Write Community String:	
<b>SNMP v3 Settings</b>	
SNMP v3:	<input type="checkbox"/> enable
<b>MIB-II System Group</b>	
sysContact:	
sysName:	
sysLocation:	
Download MIB ▼	
OK Cancel	

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 PXE via the SNMP v3 protocol. See **Configuring Users for Encrypted SNMP v3** (on page 208).*

---

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 PXE is used by the SNMP manager.

---

*Important: You must download the SNMP MIB for your PXE 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 215).*

---

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 PXE.

► **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 91).



5. Click OK. The user is now set up for encrypted SNMP v3 communication.

---

## Configuring SNMP Notifications

The PXE automatically keeps an internal log of events that occur. See **Event Rules and Actions** (on page 135). These events can also be used to send SNMP v2c or v3 notifications to a third-party destination.

The PXE 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 PXE release. This ensures your SNMP manager has the correct MIB for the release you are using. See **Downloading SNMP MIB** (on page 215).*

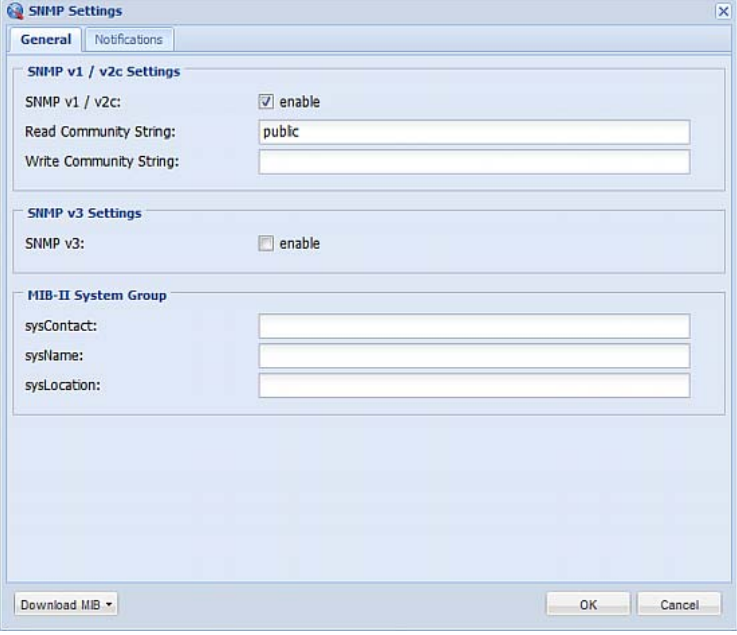
---

---

## SNMPv2c Notifications

► **To configure the PXE to send SNMP notifications:**

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

The image shows the 'SNMP Settings' dialog box with the 'General' tab selected. The dialog has a title bar with a close button. Inside, there are three main sections: 'SNMP v1 / v2c Settings', 'SNMP v3 Settings', and 'MIB-II System Group'. The 'SNMP v1 / v2c Settings' section has a checkbox for 'enable' which is checked, and two text input fields for 'Read Community String' (containing 'public') and 'Write Community String'. The 'SNMP v3 Settings' section has a checkbox for 'enable' which is unchecked. The 'MIB-II System Group' section has three text input fields for 'sysContact:', 'sysName:', and 'sysLocation:'. At the bottom, there is a 'Download MIB' button with a dropdown arrow, and 'OK' and 'Cancel' buttons.

2. On the Notifications tab, select the Enabled checkbox to enable the SNMP notification feature.

3. From the Notification Type drop-down, select the type of SNMP notification.

**SNMP Settings**

General **Notifications**

**SNMP Notification Settings**

☒ Enabled

Notification Type: SNMPv2c Inform

Timeout (sec): 3

Number of Retries: 5

Host 1	Port 1	Community 1
<input type="text"/>	<span>162</span>	<input type="text"/>
Host 2	Port 2	Community 2
<input type="text"/>	<span>162</span>	<input type="text"/>
Host 3	Port 3	Community 3
<input type="text"/>	<span>162</span>	<input type="text"/>

Please use the [Device Settings > Event Rules](#) Dialog for a more detailed trap setup.

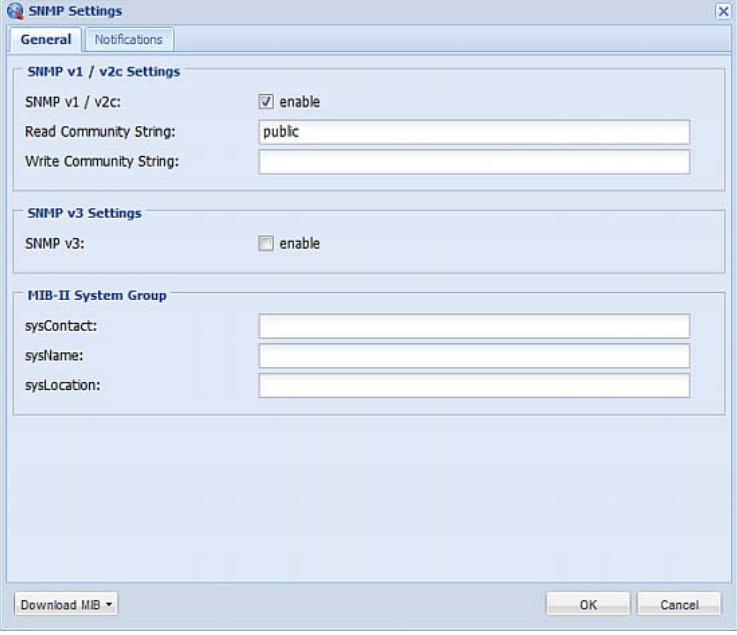
Download MIB OK Cancel

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 PXE and all SNMP management stations.
8. Click OK.

## SNMPv3 Notifications

► **To configure the PXE to send SNMPv3 notifications:**

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

The image shows the 'SNMP Settings' dialog box with the 'General' tab selected. The dialog is divided into three main sections: 'SNMP v1 / v2c Settings', 'SNMP v3 Settings', and 'MIB-II System Group'. In the 'SNMP v1 / v2c Settings' section, the 'enable' checkbox is checked, the 'Read Community String' is set to 'public', and the 'Write Community String' is empty. In the 'SNMP v3 Settings' section, the 'enable' checkbox is unchecked. The 'MIB-II System Group' section contains three empty text boxes for 'sysContact:', 'sysName:', and 'sysLocation:'. At the bottom left is a 'Download MIB' button with a dropdown arrow, and at the bottom right are 'OK' and 'Cancel' buttons.

**SNMP Settings**

**General** | Notifications

**SNMP v1 / v2c Settings**

SNMP v1 / v2c: ☒ enable

Read Community String: public

Write Community String:

**SNMP v3 Settings**

SNMP v3: ☐ enable

**MIB-II System Group**

sysContact:

sysName:

sysLocation:

Download MIB ▼ OK Cancel

2. On the Notifications tab, select the Enabled checkbox to enable the SNMP notification feature.

3. From the Notification Type drop-down, select the type of SNMP notification.

**SNMP Settings**

General **Notifications**

**SNMP Notification Settings**

☒ Enabled

Notification Type: **SNMPv3 Trap**

EngineID: 0x800035ae807d2169e2c57b650fe806a88a721995ad507d9a499d2128734e8e01

Host:

Port: 162

UserID:

Timeout (sec): 3

Number of Retries: 5

Security Level: authPriv

Authentication Protocol: SHA

Authentication Passphrase:

Confirm Authentication Passphrase:

Privacy Protocol: AES

Privacy Passphrase:

Confirm Privacy Passphrase:

Please use the [Device Settings > Event Rules](#) Dialog for a more detailed trap setup.

Download MIB

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. <ul style="list-style-type: none"> <li>• Select the authentication protocol - MD5 or SHA</li> <li>• Enter the authentication passphrase and then confirm the authentication passphrase</li> </ul>
"authPriv"	Select this if authentication and privacy protocols are required. <ul style="list-style-type: none"> <li>• Select the authentication protocol - MD5 or SHA</li> <li>• Enter the authentication passphrase and confirm the authentication passphrase</li> <li>• Select the Privacy Protocol - DES or AES</li> <li>• Enter the privacy passphrase and then confirm the privacy passphrase</li> </ul>

---

## SNMP Gets and Sets

In addition to sending notifications, the PXE is able to receive SNMP get and set requests from third-party SNMP managers.

- Get requests are used to retrieve information about the PXE, 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 PXE device name. When you change the SNMP system name, the device name shown in the web interface is also changed.*

---

The PXE 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 PXE MIB.

---

### The PXE MIB

The SNMP MIB file is required for using your PXE device with an SNMP manager. An SNMP MIB file describes the SNMP functions.

### Downloading SNMP MIB

The SNMP MIB file for the PXE can be easily downloaded from the web interface. There are two ways to download the SNMP MIB file.

---

*Note: The PXE device does not support the asset management feature so you can ignore the Asset Management-related function.*

---

► **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 PXE power management.
  - ASSETMANAGEMENT-MIB: The SNMP MIB file for asset management.
4. Click Save to save the file onto your computer.

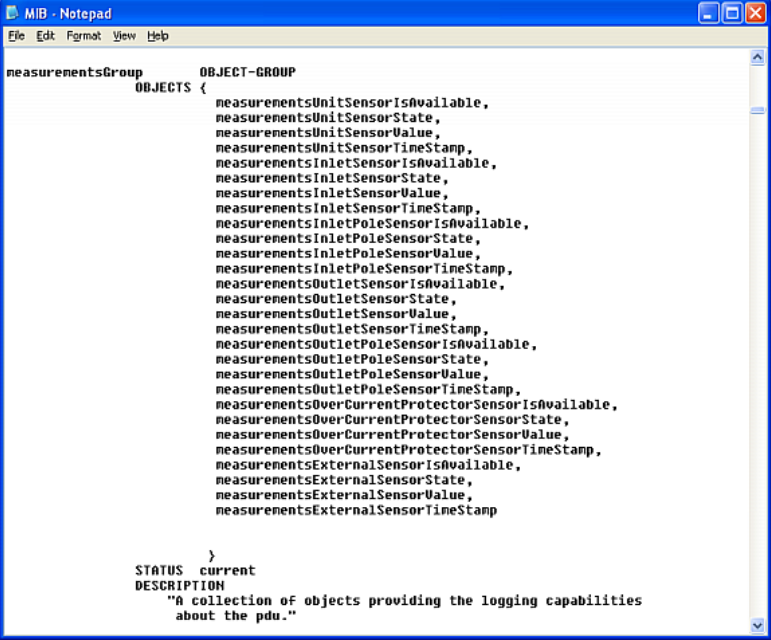
► **File download via the Device Information dialog:**

1. Choose Maintenance > Device Information.
2. Click the "download" link in the PDU2-MIB or ASSETMANAGEMENT-MIB field to download the desired SNMP MIB file.
3. Click Save to save the file onto your computer.

## Layout

Opening the MIB reveals the custom objects that describe the PXE 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.



```

measurementsGroup      OBJECT-GROUP
                        OBJECTS {
                            measurementsUnitSensorIsAvailable,
                            measurementsUnitSensorState,
                            measurementsUnitSensorValue,
                            measurementsUnitSensorTimeStamp,
                            measurementsInletSensorIsAvailable,
                            measurementsInletSensorState,
                            measurementsInletSensorValue,
                            measurementsInletSensorTimeStamp,
                            measurementsInletPoleSensorIsAvailable,
                            measurementsInletPoleSensorState,
                            measurementsInletPoleSensorValue,
                            measurementsInletPoleSensorTimeStamp,
                            measurementsOutletSensorIsAvailable,
                            measurementsOutletSensorState,
                            measurementsOutletSensorValue,
                            measurementsOutletSensorTimeStamp,
                            measurementsOutletPoleSensorIsAvailable,
                            measurementsOutletPoleSensorState,
                            measurementsOutletPoleSensorValue,
                            measurementsOutletPoleSensorTimeStamp,
                            measurementsOverCurrentProtectorSensorIsAvailable,
                            measurementsOverCurrentProtectorSensorState,
                            measurementsOverCurrentProtectorSensorValue,
                            measurementsOverCurrentProtectorSensorTimeStamp,
                            measurementsExternalSensorIsAvailable,
                            measurementsExternalSensorState,
                            measurementsExternalSensorValue,
                            measurementsExternalSensorTimeStamp
                        }
                        STATUS current
                        DESCRIPTION
                            "A collection of objects providing the logging capabilities
                            about the pdu."

```

For example, the measurementsGroup group contains objects for sensor readings of PXE 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 PXE to generate a warning and send an SNMP notification when certain parameters are exceeded. See **Setting Power Thresholds** (on page 133) for a description of how thresholds work.

---

*Note: When configuring the thresholds via SNMP set commands, ensure the value of upper critical threshold is higher than that of upper warning threshold.*

---

### A Note about Enabling Thresholds

When enabling previously disabled thresholds via SNMP, make sure you set a correct value for all thresholds that are supposed to be enabled prior to actually enabling them. Otherwise, you may get an error message.

## Chapter 8 Using the Command Line Interface

This section explains how to use the command line interface (CLI) to administer a PXE device.

### In This Chapter

About the Interface .....	218
Logging in to CLI .....	219
Logging out of CLI .....	221
Help Command.....	222
Querying Available Parameters for a Command.....	223
Showing Information .....	223
Clearing Information .....	246
Configuring the PXE Device and Network.....	247
Actuator Control Operations.....	336
Unblocking a User .....	338
Resetting the PXE .....	338
Network Troubleshooting.....	340
Retrieving Previous Commands.....	343
Automatically Completing a Command .....	343

---

### About the Interface

The PXE 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 PXE device
- Display the PXE and network information, such as the device name, firmware version, IP address, and so on
- Configure the PXE 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 76).*

---

---

## 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 PXE 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 PXE. 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 221) 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 PXE.

---

### 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 76) in the User Guide.
2. Launch an SSH or Telnet client and open a console window. A login prompt appears.

```
login as: █
```

3. Type a name and press Enter. The name is case sensitive.

---

*Note: If using the SSH client, the name must NOT exceed 25 characters. Otherwise, the login fails.*

---

Then you are prompted to enter a password.

```
login as: admin
admin@192.168.84.88's password: █
```

4. Type a password and press Enter. The password is case sensitive.
5. After properly entering the password, the # or > system prompt appears. See **Different CLI Modes and Prompts** (on page 221) 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 PXE.

---

### 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 PXE device, the **>** prompt appears.
- **Administrator Mode:** When you log in as an administrator, who has full permissions to configure the PXE 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 PXE device and network configurations. See **Entering Configuration Mode** (on page 247).
- **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 340).

---

### Closing a Local Connection

Close the window or terminal emulation program when you finish accessing a PXE device over the local connection.

When accessing or upgrading multiple PXE devices, do not transfer the local connection cable from one device to another without closing the local connection window first.

---

### 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.

---

## 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 223).*

---

---

## 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 PXE 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 221).*

---

---

### 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. <i>Tip: You can also type the command without adding this option "all" to get the same data.</i>
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 PXE is a slave device connected to the LAN via the master PXE device, the `show network mode` command displays wired(USB) instead of wired.*

---

The PXE device does NOT support the wireless networking mode so the network mode never shows "wireless."

### 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.  <i>Tip: You can also type the command without adding this option "all" to get the same data.</i>
http	Only displays the TCP port for the HTTP service.
https	Only displays the TCP port for the HTTPS service.
telnet	Only displays the settings of the Telnet service.
ssh	Only displays the settings of the SSH service.
snmp	Only displays the SNMP settings.
modbus	Only displays the settings of the Modbus/TCP service.
zeroconfig	Only displays the settings of the zero configuration advertising.

---

### PDU Configuration

This command shows the PDU configuration, such as the device name, firmware version 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.  <i>Tip: You can also type the command without adding this option "all" to get the same data.</i>
A specific outlet number	Displays the information for the specified outlet only.

*Displayed information:*

- Without the parameter "details," only the outlet name is displayed.
- With the parameter "details," more outlet information is displayed in addition to the outlet name, such as the outlet rating.

### Inlet Information

This command syntax shows the inlet information.

```
#          show inlets <n>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#          show inlets <n> details
```

*Variables:*

- <n> is one of the options: *all*, or a number.

Option	Description
all	Displays the information for all inlets.  <i>Tip: You can also type the command without adding this option "all" to get the same data.</i>
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. <i>Tip: You can also type the command without adding this option "all" to get the same data.</i>
A specific overcurrent protector number	Displays the information for the specified overcurrent protector only.

#### Displayed information:

- Without the parameter "details," only the circuit breaker name is displayed.
- With the parameter "details," more circuit breaker information is displayed in addition to the name, such as the rating and circuit breaker type.

---

### Date and Time Settings

This command shows the current date and time settings on the PXE 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 PXE 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 PXE. See **Existing User Profiles** (on page 239) 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.  <i>Tip: You can also type the command without adding this option "all" to get the same data.</i>
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 PXE 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..*

---

### 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.  <i>Tip: You can also type the command without adding this option "all" to get the same data.</i>
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 PXE web interface or CLI. It is an integer starting at 1.

*Displayed information:*

- Without the parameter "details," only the actuator ID, type and state are displayed.
- With the parameter "details," more information is displayed in addition to the ID number and actuator state, such as the serial number and X, Y, and Z coordinates.

---

### Environmental Sensor 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
```



### Inlet Sensor Threshold Information

This command syntax shows the specified inlet sensor's threshold-related information.

```
#          show sensor inlet <n> <sensor type>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#          show sensor inlet <n> <sensor type> details
```

*Variables:*

- <n> is the number of the inlet whose sensors you want to query. For a single-inlet PDU, <n> is always 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.

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
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.

---

### 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 PXE 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
	<i>Tip: You can also type the command without adding this option "all" to get the same data.</i>

*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 PXE.

```
#          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.  <i>Tip: You can also type the command without adding this option "all" to get the same data.</i>
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.  <i>Tip: You can also type the command without adding this option "all" to get the same data.</i>
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.

---

### EnergyWise Settings

This command shows the PXE device's current configuration for Cisco® EnergyWise.

```
#          show energywise
```



## Event Log

The command used to show the event log begins with `show eventlog`. You can add either the *limit* or *class* parameters or both to show specific events.

► **Show the last 30 entries:**

```
# show eventlog
```

► **Show a specific number of last entries in the event log:**

```
# show eventlog limit <n>
```

► **Show a specific type of events only:**

```
# show eventlog class <event_type>
```

► **Show a specific number of last entries associated with a specific type of events only:**

```
# show eventlog limit <n> class <event_type>
```

*Variables:*

- <n> is one of the options: *all* or a number.

Option	Description
all	Displays all entries in the event log.
An integer number	Displays the specified number of last entries in the event log. The number ranges between 1 to 10,000.

- <event\_type> is one of the following event types.

Event type	Description
all	All events.
device	Device-related events, such as system starting or firmware upgrade event.
userAdministration	User management events, such as a new user profile or a new role.
userActivity	User activities, such as login or logout.
pdu	Displays PDU-related events, such as entry or exit of the load shedding mode.
sensor	Internal or external sensor events, such as state changes of any sensors.

Event type	Description
serverMonitor	Server-monitoring records, such as a server being declared reachable or unreachable.
timerEvent	Scheduled action events.
energywise	Cisco EnergyWise-related events, such as enabling the support of the EnergyWise function.

---

*Note: You can ignore the following event types in the CLI because the PXE does not support them: `assetManagement`, `cardReader`, `lhx`, `modem`, `transferSwitch` and `webcam`.*

---



---

### 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. <i>Tip: You can also type the command without adding this option "0" to get all data.</i>
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: PXE-1847
Firmware version: 2.2.10.5-30940
#
```

**Example 4 - In-Depth PDU Information**

More information is displayed when typing the *show pdu details* command.

```
# show pdu
PDU 'my PX'
Model: PXE-1847
Firmware version: 2.2.10.5-30940
# show pdu details
PDU 'my PX'
Model: PXE-1847
Firmware version: 2.2.10.5-30940
Serial number: PA61234567

Voltage rating: 200-240V
Current rating: 32A
Frequency rating: 50/60Hz
Power rating: 6.4-7.7kVA

Sensor data retrieval: Enabled
Measurements per log entry: 60

External sensor Z coordinate format: Rack units
Device altitude: 3000 m
#
```

---

**Clearing Information**

You can use the clear commands to remove unnecessary data from the PXE.

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 221).*

---

**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.

---

## Configuring the PXE Device and Network

To configure the PXE 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 221).*

---

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 247).

---

---

### 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 221).

---

## 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 PXE device.

### Changing the PDU Name

This command changes the PXE 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.

### 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 87).



### 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 87).

### Specifying the Device Altitude

This command specifies your PXE device's altitude above sea level (in meters). You must specify the PXE 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 437).

```
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.

Option	Description
freeForm	Any alphanumeric string can be used for specifying the Z coordinate.

---

*Note: After determining the format for the Z coordinate, you can set a value for it. See **Setting the Z Coordinate** (on page 317).*

---

### 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 194).

### 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 - Data Logging Enabled**

The following command enables the data logging feature.

```
config:# pdu dataRetrieval enable
```

---

## 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 PXE 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 PXE 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 PXE device.

An IP protocol configuration command begins with *network ip*.

**Enabling IPv4 or IPv6**

This command determines which IP protocol is enabled on the PXE.

```
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 PXE.

```
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.

**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 PXE device.

```
config:# network ipv4 ipAddress <ip address>
```

Variables:

- <ip address> is the IP address being assigned to your PXE 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 255).

```
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 255).

```
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 PXE supports a maximum of 3 DNS servers. If two IPv4 DNS servers and two IPv6 DNS servers are available, the PXE 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 PXE 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 PXE device.

```
config:# network ipv6 ipAddress <ip address>
```

Variables:

- <ip address> is the IP address being assigned to your PXE 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 259).

```
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 259).

```
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 PXE supports a maximum of 3 DNS servers. If two IPv4 DNS servers and two IPv6 DNS servers are available, the PXE 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 PXE 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 PXE 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 PXE selects the optimum transmission mode through auto-negotiation.
half	Half duplex: Data is transmitted in one direction (to or from the PXE 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 PXE via HTTP to be redirected to HTTPS.
false	No HTTP access is redirected to HTTPS.

**Changing the Telnet Configuration**

You can enable or disable the Telnet service, or change its TCP port using the CLI commands.

A Telnet command begins with *network services telnet*.

**Enabling or Disabling Telnet**

This command enables or disables the Telnet service.

```
config:#    network services telnet enabled <option>
```

*Variables:*

- <option> is one of the options: *true* or *false*.

Option	Description
true	The Telnet service is enabled.
false	The Telnet service is disabled.

**Changing the Telnet Port**

This command changes the Telnet port.

```
config:# network services telnet port <n>
```

*Variables:*

- <n> is a TCP port number between 1 and 65535. The default Telnet port is 23.

**Changing the SSH Configuration**

You can enable or disable the SSH service, or change its TCP port using the CLI commands.

An SSH command begins with *network services ssh*.

**Enabling or Disabling SSH**

This command enables or disables the SSH service.

```
config:# network services ssh enabled <option>
```

*Variables:*

- <option> is one of the options: *true* or *false*.

Option	Description
true	The SSH service is enabled.
false	The SSH service is disabled.

**Changing the SSH Port**

This command changes the SSH port.

```
config:# network services ssh port <n>
```

*Variables:*

- <n> is a TCP port number between 1 and 65535. The default SSH port is 22.



**Determining the SSH Authentication Method**

This command syntax determines the SSH authentication method.

```
config:# network services ssh authentication <auth_method>
```

*Variables:*

- <option> is one of the options: *passwordOnly*, *publicKeyOnly* or *passwordOrPublicKey*.

Option	Description
passwordOnly	Enables the password-based login only.
publicKeyOnly	Enables the public key-based login only.
passwordOrPublicKey	Enables both the password- and public key-based login. This is the default.

If the public key authentication is selected, you must type a valid SSH public key for each user profile to log in over the SSH connection. See ***Specifying the SSH Public Key*** (on page 304).

**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 81) 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 - 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 PXE.

```
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 269).*

---

► **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 <i>2015-11-30</i> 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 <i>13:50:20</i> 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 PXE and then shows the result. For instructions on specifying NTP servers via CLI, see **Setting NTP Parameters** (on page 270).

To perform this command successfully, you must:

- Own the "Change Date/Time Settings" permission.
- Customize NTP servers. See **Setting NTP Parameters** (on page 270).
- Make the customized NTP servers override the DHCP-assigned ones. See **Overriding DHCP-Assigned NTP Servers** (on page 270).

This command is available either in the administrator/user mode or in the configuration mode. See **Different CLI Modes and Prompts** (on page 221).

#### ► 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 PXE 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 335).*

---

### **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: <i>new rule's number = the specified rule number</i>
insertBelow	Inserts the new rule below the specified rule number. Then: <i>new rule's number = the specified rule number + 1</i>

- <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 PXE. Do either of the following, or you cannot successfully log in to the PXE:

- 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 247).*

---

### 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 335).

**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 PXE 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 335).

► **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 335).

#### 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 minLength <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 maxLength <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 335).

---

### **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: <i>new rule's number = the specified rule number</i>
insertBelow	Inserts the new rule below the specified rule number. Then: <i>new rule's number = the specified rule number + 1</i>

- <rule\_number> is the number of the existing rule which you want to insert the new rule above or below.

### Modifying a Role-Based Access Control Rule

Depending on what to modify in an existing rule, the command syntax varies.

- *IPv4 commands*

#### ► Modify a rule's IPv4 address range:

```
config:# security roleBasedAccessControl ipv4 rule modify <rule_number>
startIpAddress <start_ip> endIpAddress <end_ip>
```

#### ► Modify an IPv4 rule's role:

```
config:# security roleBasedAccessControl ipv4 rule modify <rule_number> role <role>
```

► **Modify an IPv4 rule's policy:**

```
config:# security roleBasedAccessControl ipv4 rule modify <rule_number> policy  
<policy>
```

► **Modify all contents of an existing IPv4 rule:**

```
config:# security roleBasedAccessControl ipv4 rule modify <rule_number>  
startIpAddress <start_ip> endIpAddress <end_ip> role <role> policy <policy>
```

- *IPv6 commands*

► **Modify a rule's IPv6 address range:**

```
config:# security roleBasedAccessControl ipv6 rule modify <rule_number>  
startIpAddress <start_ip> endIpAddress <end_ip>
```

► **Modify an IPv6 rule's role:**

```
config:# security roleBasedAccessControl ipv6 rule modify <rule_number> role <role>
```

► **Modify an IPv6 rule's policy:**

```
config:# security roleBasedAccessControl ipv6 rule modify <rule_number> policy  
<policy>
```

► **Modify all contents of an existing IPv6 rule:**

```
config:# security roleBasedAccessControl ipv6 rule modify <rule_number>
startIpAddress <start_ip> endIpAddress <end_ip> role <role> policy <policy>
```

*Variables:*

- <rule\_number> is the number of the existing rule that you want to modify.
- <start\_ip> is the starting IP address.
- <end\_ip> is the ending IP address.
- <role> is one of the existing roles.
- <policy> is one of the options: *allow* or *deny*.

Policy	Description
allow	Accepts traffic from the specified IP address range when the user is a member of the specified role
deny	Drops traffic from the specified IP address range when the user is a member of the specified role

### Deleting a Role-Based Access Control Rule

These commands remove a specific rule from the list.

#### ► IPv4 commands

```
config:# security roleBasedAccessControl ipv4 rule delete <rule_number>
```

#### ► IPv6 commands

```
config:# security roleBasedAccessControl ipv6 rule delete <rule_number>
```

*Variables:*

- <rule\_number> is the number of the existing rule that you want to remove.

### Examples

This section illustrates several security configuration examples.

#### **Example 1 - IPv4 Firewall Control Configuration**

The following command sets up two parameters of the IPv4 access control feature.

```
config:# security ipAccessControl ipv4 enabled true defaultPolicyIn accept
        defaultPolicyOut accept
```

*Results:*

- The IPv4 access control feature is enabled.
- The default policy for inbound traffic is set to "accept."
- The default policy for outbound traffic is set to "accept."

**Example 2 - Adding an IPv4 Firewall Rule**

The following command adds a new IPv4 access control rule and specifies its location in the list.

```
config:# security ipAccessControl ipv4 rule add 192.168.84.123/24 accept
        insertAbove 5
```

*Results:*

- A new IPv4 firewall control rule is added to accept all packets sent from the IPv4 address 192.168.84.123.
- The newly-added rule is inserted above the 5th rule. That is, the new rule becomes the 5th rule, and the original 5th rule becomes the 6th rule.

**Example 3 - User Blocking**

The following command sets up two user blocking parameters.

```
config:# security userBlocking maximumNumberOfFailedLogins 5 blockTime 30
```

*Results:*

- The maximum number of failed logins is set to 5.
- The user blocking time is set to 30 minutes.

**Example 4 - Adding an IPv4 Role-based Access Control Rule**

The following command creates a new IPv4 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.

**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 PXE 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 PXE.

```
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 PXE 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 335).*

---



**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, PXE 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 247).
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 335).

► **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 PXE 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 335).

► **Enable or disable the SNMP v3 access to PXE 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 310).

**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 335).

---

*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 PXE user interfaces for all users via CLI, see **Setting Default Measurement Units** (on page 306).*

---

► **Set the preferred temperature unit:**

```
config:# user modify <name> preferredTemperatureUnit <option1>
```

*Variables:*

- <name> is the name of the user whose settings you want to change.
- <option1> is one of the options: *C* or *F*.

Option	Description
C	This option displays the temperature in Celsius.
F	This option displays the temperature in Fahrenheit.

► **Set the preferred length unit:**

```
config:# user modify <name> preferredLengthUnit <option2>
```

*Variables:*

- <name> is the name of the user whose settings you want to change.
- <option2> is one of the options: *meter* or *feet*.

Option	Description
meter	This option displays the length or height in meters.
feet	This option displays the length or height in feet.

► **Set the preferred pressure unit:**

```
config:# user modify <name> preferredPressureUnit <option3>
```

*Variables:*

- <name> is the name of the user whose settings you want to change.
- <option3> is one of the options: *pascal* or *psi*.

Option	Description
pascal	This option displays the pressure value in Pascals (Pa).
psi	This option displays the pressure value in psi.

**Specifying the SSH Public Key**

If the SSH key-based authentication is enabled, specify the SSH public key for each user profile using the following procedure.

► **To specify or change the SSH public key for a specific user:**

1. Type the SSH public key command as shown below and press Enter.  

```
config:# user modify <name> sshPublicKey
```
2. The system prompts you to enter the contents of the SSH public key. Do the following to input the contents:
  - a. Open your SSH public key with a text editor.
  - b. Copy all contents in the text editor.



- c. Paste the contents into the terminal.
- d. Press Enter.

► **To remove an existing SSH public key:**

- 1. Type the same command as shown above.
- 2. When the system prompts you to input the contents, press Enter without typing or pasting anything.

**Example**

The following procedure illustrates how to change the SSH public key for the user "assistant."

- 1. Verify that you have entered the configuration mode. See **Entering Configuration Mode** (on page 247).
- 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 PXE 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 247).

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 PXE 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 335).

---

*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 PXE user interfaces for a specific user via CLI, see **Changing Measurement Units** (on page 303).*

---

#### ► 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 310).
- <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. All PXE models do NOT support features and privileges associated with the LHX/SHX, modem, web cam and transfer switch.

Privilege	Description
acknowledgeAlarms	Acknowledge Alarms
adminPrivilege	Administrator Privileges
changeAssetStripConfiguration	Change Asset Strip Configuration
changeAuthSettings	Change Authentication Settings
changeDateTimeSettings	Change Date/Time Settings
changeExternalSensorsConfiguration	Change Peripheral Device Configuration
changeLhxConfiguration	Change LHX/SHX Configuration
changeModemConfiguration	Change Modem Configuration
changeNetworkSettings	Change Network Settings
changePassword	Change Own Password
changePduConfiguration	Change Pdu, Inlet, Outlet & Overcurrent Protector Configuration
changeSecuritySettings	Change Security Settings
changeSnmpSettings	Change SNMP Settings
changeUserSettings	Change Local User Management
changeWebcamSettings	Change Webcam Configuration
clearLog	Clear Local Event Log
firmwareUpdate	Firmware Update
performReset	Reset (Warm Start)
switchActuator**	Switch Actuator
switchTransferSwitch	Switch Transfer Switch
viewEventSetup	View Event Settings
viewEverything	Unrestricted View Privileges
viewLog	View Local Event Log

Privilege	Description
viewSecuritySettings	View Security Settings
viewSnmpSettings	View SNMP Settings
viewUserSettings	View Local User Management
viewWebcamSettings	View Webcam Snapshots and Configuration

\*\* The "switchActuator" privilege requires an argument that is separated with a colon. The argument could be:

- All actuators, that is,  
`switchActuator:all`
- An actuator's ID number. For example:  
`switchActuator:1`  
`switchActuator:2`  
`switchActuator:3`
- A list of comma-separated ID numbers of different actuators. For example:  
`switchActuator:1,3,6`

---

*Note: The ID number of each actuator is shown in the PXE 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 310).
- <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 310).
- <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 328).

---

### 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 PXE 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 328).*

---

### 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 PXE 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 PXE 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 PXE 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 PXE 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 249).*

---

### 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 PXE 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 PXE 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 PXE 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 335).

► **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 <sup>3</sup> (that is, g/m³)
relativeHumidity	%
temperature	Degrees Celsius (°C) or Fahrenheit (°F), depending on your measurement unit settings.
airPressure	Pascal (Pa) or psi, depending on your measurement unit settings.
airFlow	m/s
vibration	g

- <hy\_value> is the deassertion hysteresis value applied to the specified sensor type.
- <as\_value> is the assertion timeout value applied to the specified sensor type. It ranges from 0 to 100 (samples).



**Example - Default Upper Thresholds for Temperature**

It is assumed that your preferred measurement unit for temperature is set to degrees Celsius. Then the following command sets the default Upper Warning threshold to 20°C and Upper Critical threshold to 24°C for all temperature sensors.

```
config:# defaultThresholds temperature upperWarning 20
        upperCritical 24
```

**Sensor Threshold Configuration Commands**

A sensor configuration command begins with *sensor*. You can use the commands to configure the threshold, hysteresis and assertion timeout values for any sensor associated with the following items:

- Inlets
- Inlet poles (for three-phase PDUs only)
- Overcurrent protectors
- Environmental sensors

It is permitted to assign a new value to the threshold at any time regardless of whether the threshold has been enabled.

**Commands for Inlet Sensors**

A sensor configuration command for inlets begins with *sensor inlet*.

You can configure various inlet sensor threshold settings at a time by combining multiple commands. See **Multi-Command Syntax** (on page 335).

► **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 445).
- <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 443).

#### 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 335).

##### ► 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 445).
- <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 443).

### 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 335).

#### ► 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 PXE 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 445).
- <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 443).

#### Examples

This section illustrates several environmental sensor threshold configuration examples.

##### **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 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
```

### 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 335).

► **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 PXE 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 249).*

---

- <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 PXE 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 PXE 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 335).

#### ► 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 PXE 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 PXE 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 PXE 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 PXE 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 PXE 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 PXE is enabled.
- The UDP port is set to 10288.

---

**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 inlet.

```
config:# sensor inlet 1 current upperCritical disable upperWarning 20
```

*Results:*

- The Upper Critical threshold of the inlet's RMS current is disabled.
- The Upper Warning threshold of the inlet's RMS current is set to 20A and enabled at the same time.

---

## 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 221).



---

### 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 PXE 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 PXE 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
```

---

## Unlocking a User

If any user is blocked from accessing the PXE, 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 219).
2. When the Username prompt appears, type `unlock` and press Enter.

Username: `unlock`

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 PXE

You can reset the PXE device to factory defaults or simply restart it using the CLI commands.

---

### Restarting the PDU

This command restarts the PXE device. It is not a factory default reset.

#### ► To restart the PXE device:

1. Ensure you have entered administrator mode and the # prompt is displayed.
2. Type either of the following commands to restart the PXE 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.

---

### 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 PXE:

```
#      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
```

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.

---

### Resetting to Factory Defaults

The following commands restore all settings of the PXE device to factory defaults.

► **To reset PXE settings after login, use either command:**

```
#      reset factorydefaults
      -- OR --
#      reset factorydefaults /y
```

► **To reset PXE settings before login:**

```
Username:  factorydefaults
```

See **Using the CLI Command** (on page 382) for details.

---

## Network Troubleshooting

The PXE 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 221).

---

### 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 PXE 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.



## Appendix A Specifications

### In This Chapter

Maximum Ambient Operating Temperature .....	345
Sensor RJ-12 Port Pinouts .....	345
RS-485 Port Pinouts .....	345

---

### Maximum Ambient Operating Temperature

The maximum ambient operating temperature (TMA) for the PXE is the same for all models.

Specification	Measure
Max Ambient Temperature	45 degrees Celsius

---

### Sensor RJ-12 Port Pinouts

RJ-12 Pin/signal definition			
Pin No.	Signal	Direction	Description
1	+12V	—	Power (500mA, fuse protected)
2	GND	—	Signal Ground
3	—	—	—
4	—	—	—
5	GND	—	Signal Ground
6	1-wire		1-wire signal for external environmental sensor packages

---

### RS-485 Port Pinouts

RS-485 Pin/signal definition			
Pin No.	Signal	Direction	Description
1	—	—	—
2	—	—	—

RS-485 Pin/signal definition			
3	D+	bi-directional	Data +
4	—	—	—
5	—	—	—
6	D-	bi-directional	Data -
7	—	—	—
8	—	—	—

# Appendix B Equipment Setup Worksheet

PXE Series Model \_\_\_\_\_

PXE 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

Appendix B: Equipment Setup Worksheet

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

Appendix B: Equipment Setup Worksheet

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 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 PXE 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 PXE devices to configure or upgrade.

### In This Chapter

Bulk Configuration/Upgrade Procedure .....	351
Configuration Files .....	352
TFTP Requirements .....	361
DHCP IPv4 Configuration in Windows .....	361
DHCP IPv6 Configuration in Windows .....	371
DHCP IPv4 Configuration in Linux .....	378
DHCP IPv6 Configuration in Linux .....	380

---

### Bulk Configuration/Upgrade Procedure

The DHCP/TFTP feature is supported as of release 3.1.0 so make sure that all PXE 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 PXE models and firmware versions. See **Configuration Files** (on page 352) 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 361).
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 PXE.

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 361)
  - **DHCP IPv6 Configuration in Windows** (on page 371)
  - **DHCP IPv4 Configuration in Linux** (on page 378)
  - **DHCP IPv6 Configuration in Linux** (on page 380)
5. Make sure all of the desired PXE devices use DHCP as the IP configuration method and have been *directly* connected to the network.
  6. Re-boot these PXE devices. The DHCP server will execute the commands in the "fwupdate.cfg" file on the TFTP server to configure or upgrade those PXE 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.

---

## 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 354).
- **config.txt:**  
This file is used for configuring device settings. See **config.txt** (on page 357).



- **devices.csv:**

This file is required only when there are device-specific settings to configure for multiple PXE devices. See **devices.csv** (on page 359).

Raritan provides a Mass Deployment Utility, which helps you to quickly generate all configuration files for your PXE. See **Creating Configuration Files via Mass Deployment Utility** (on page 360).

---

### **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 PXE must be able to support them.*

---

#### ▶ **user**

- A required option.
- Specify the name of a user account with Administrator Privileges.
- For a PXE with factory default configuration, set this option to `admin`.

#### ▶ **password**

- A required option.
- Specify the password of the specified admin user.
- For a PXE with factory default configuration, set this option to `raritan`.

#### ▶ **logfile**

- Specify the name of a text file where the PXE will append the log messages when interpreting the TFTP server contents.
- If the specified file does not exist in the TFTP server, 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 PXE detects a problem with the TFTP server contents.

#### ▶ **firmware**

- Specify the name of a firmware binary file used to upgrade your PXE.
- The specified firmware file must be compatible with your PXE and have an official Raritan signature.
- If the specified firmware file is the same as the current firmware version of your PXE, 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 PXE 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 357).

#### ► **device\_list**

- Specify the name of the configuration file listing all PXE 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 359).

#### ► **match**

- Specify a match condition for identifying a line or a PXE 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 PXE to search for the MAC address in the 7th column of the "devices.csv" file.

- The default value is `serial:1`, making the PXE 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 PXE is downloaded to the TFTP server.
- The filename of the diagnostic data written into the TFTP server varies, depending on the PXE firmware version:
  - Filename prior to version 3.0.0: *diag\_<unit-serial>.zip*, where `<unit-serial>` is the serial number of the PXE.
  - Filename as of version 3.0.0: *diag\_<unit-serial>.tgz*

- The PXE utters a short beep when writing the diagnostic data to the TFTP server.

► **factory\_reset**

- Supported as of release 3.0.0.
- If this option is set to `true`, the PXE 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 PXE.

---

*Note: See **Saving the PXE Configuration** (on page 197) 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 PXE.

---

*Note: See **Backup and Restore of PXE Device Settings** (on page 199) 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 354).

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 PXE 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 PXE 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 359)
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 PXE.

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 354).

Every PXE 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 PXE devices:**

- By default, a PXE 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",Value-3
```

```
Value-1,"Value-2
with a line break", Value-3
```

---

### Creating Configuration Files via Mass Deployment Utility

The Mass Deployment Utility is an Excel file that lets you fill in basic information required for the three configuration files, such as the admin account and password.

After entering required information, you can generate all configuration files with only one click, including *fwupdate.cfg*, *config.txt* and *devices.csv*.

#### ► To use the Mass Deployment Utility:

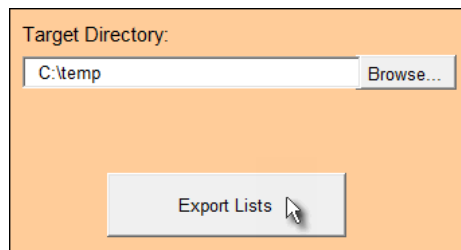
1. Download the Mass Deployment Utility from the Raritan website.
  - The utility is named *mass\_deployment-xxx* (where xxx is the version number).
  - It is available on the PXE section of the **Support page** (<http://www.raritan.com/support/>).
2. Make sure Microsoft Excel's security level has been 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.



The screenshot shows a software interface with an orange background. At the top, it says "Target Directory:". Below this is a text input field containing "C:\temp" and a "Browse..." button to its right. At the bottom center, there is a large button labeled "Export Lists" with a mouse cursor hovering over it.



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 PXE with these files.

---

## 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 351).

If you are going to upload any PXE 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.

---

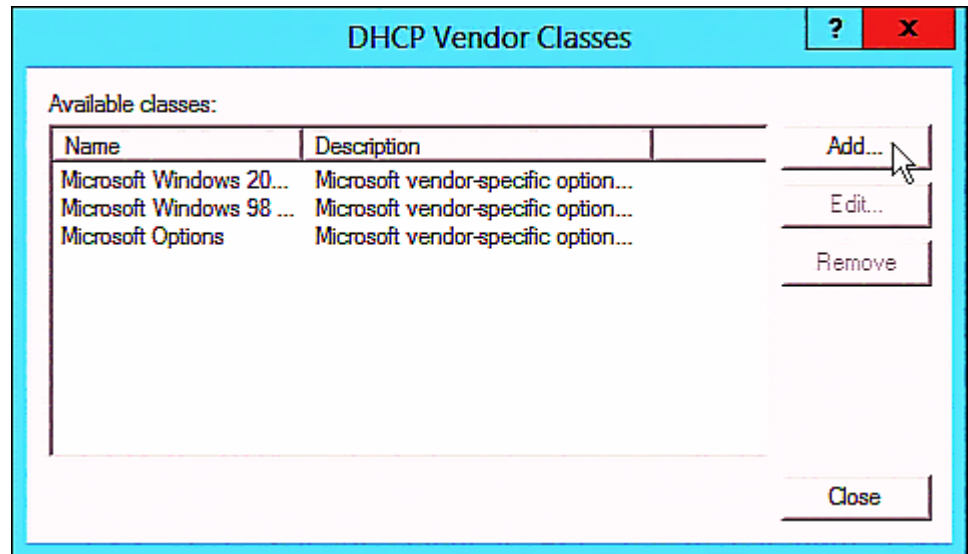
## DHCP IPv4 Configuration in Windows

For those PXE 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:**

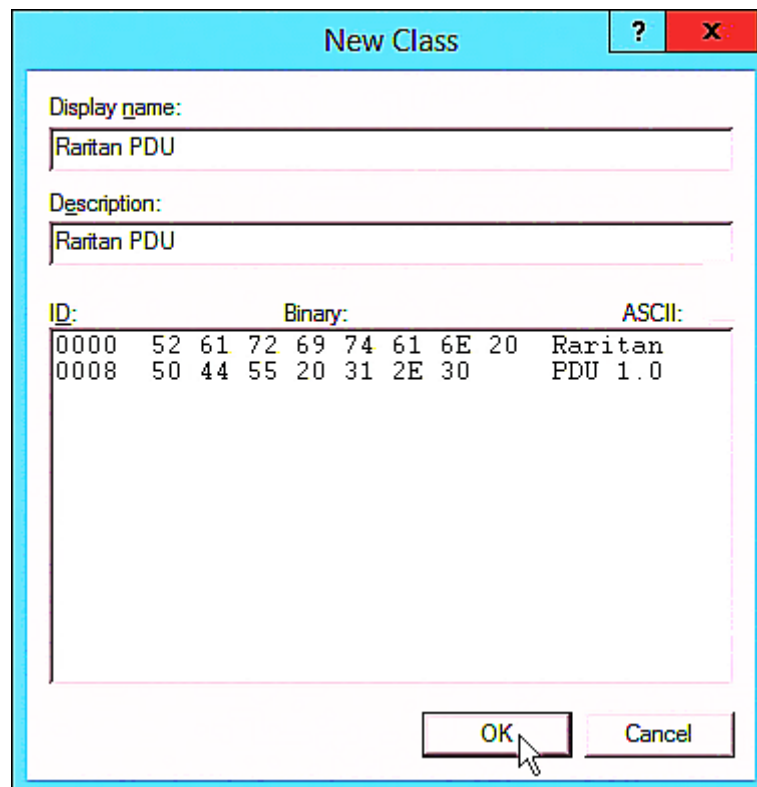
1. Add a new vendor class for Raritan PXE under IPv4.
  - a. Right-click the IPv4 node in DHCP to select Define Vendor Classes.

- 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.

**Predefined Options and Values** ? X

Option class: DHCP Standard Options

Option name: 060 Vendor Class Identifier

Description:

Value

String:

OK Cancel

3. Add three options to the new vendor class "Raritan PDU" in the same dialog.

- a. Select Raritan PDU in the "Option class" field.

**Predefined Options and Values** ? x

Option class: Raritan PDU

Option name: DHCP Standard Options  
Microsoft Windows 2000 Options  
Microsoft Windows 98 Options  
Microsoft Options  
Raritan PDU

Description:

Value

String:

OK Cancel

- 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.

**Option Type** ? x

Class: Raritan PDU

Name: pdu-tftp-server

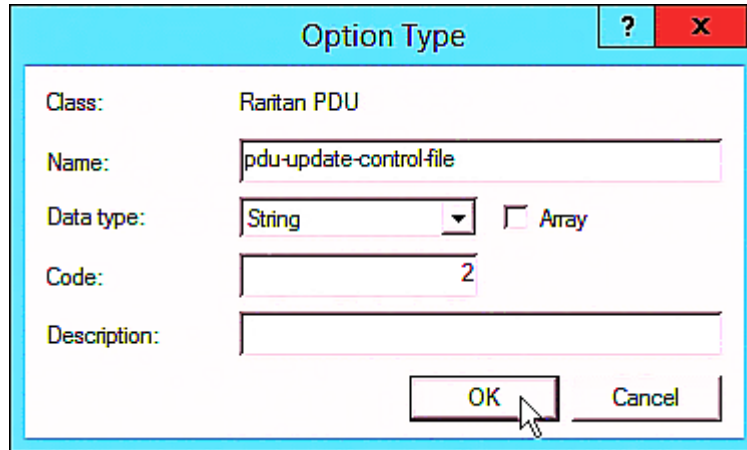
Data type: IP Address ☐ Array

Code: 1

Description:

OK Cancel

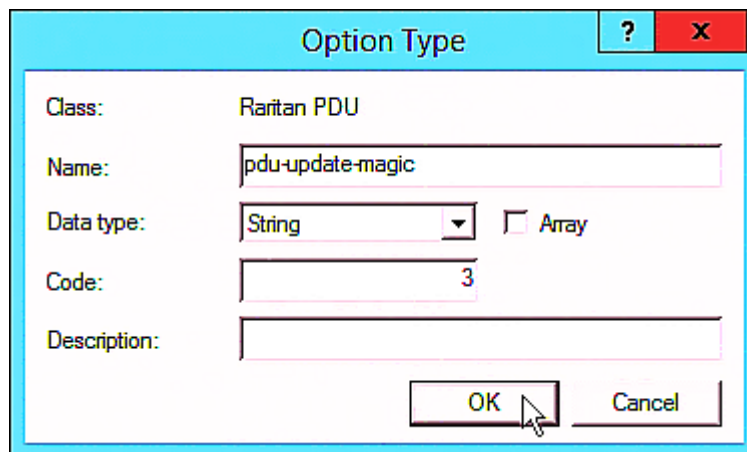
- c. Click Add to add the second option. Type "pdu-update-control-file" in the Name field, select String as the data type, and type 2 in the Code field.



The dialog box is titled "Option Type" and has a light blue header bar with a question mark icon and a red close button. The main area is white. It contains the following fields:

- Class:** Raritan PDU
- Name:** pdu-update-control-file
- Data type:** String (selected in a dropdown menu) and an unchecked checkbox for Array.
- Code:** 2
- Description:** (empty text box)
- Buttons:** OK and Cancel at the bottom right.

- 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.



The dialog box is titled "Option Type" and has a light blue header bar with a question mark icon and a red close button. The main area is white. It contains the following fields:

- Class:** Raritan PDU
- Name:** pdu-update-magic
- Data type:** String (selected in a dropdown menu) and an unchecked checkbox for Array.
- Code:** 3
- Description:** (empty text box)
- Buttons:** OK and Cancel at the bottom right.

4. Create a new policy associated with the "Raritan PDU" vendor class.
- Right-click the Policies node under IPv4 to select New Policy.
  - Specify a policy name, and click Next.

The policy is named "PDU" in this illustration.

**DHCP Policy Configuration Wizard**

**Policy based IP Address and Option Assignment**

This feature allows you to distribute configurable settings (IP address, DHCP options) to clients based on certain conditions (e.g. vendor class, user class, MAC address, etc.).

This wizard will guide you setting up a new policy. Provide a name (e.g. VoIP Phone Configuration Policy) and description (e.g. NTP Server option for VoIP Phones) for your policy.

Policy Name:

Description:

< Back   Next >   Cancel

- c. Click Add to add a new condition.

- d. Select the vendor class "Raritan PDU" in the Value field, click Add and then Ok.

**Add/Edit Condition**

Specify a condition for the policy being configured. Select a criteria, operator and values for the condition.

Criteria: Vendor Class

Operator: Equals

Value(s)

Value: Raritan PDU

☐ Prefix wildcard(\*)

☐ Append wildcard(\*)

Raritan PDU

Ok Cancel

- e. Click Next.

- f. Select DHCP Standard Options in the "Vendor class" field, select "060 Vendor Class Identifier" from the Available Options list, and type "Raritan PDU 1.0" in the "String value" field.

DHCP Policy Configuration Wizard

Configure settings for the policy

If the conditions specified in the policy match a client request, the settings will be applied.

Vendor class:

DHCP Standard Options

Available Options	Description
<input type="checkbox"/> 049 X Window System Display	Array of X Windows Display M...
<input checked="" type="checkbox"/> 060 Vendor Class Identifier	
<input type="checkbox"/> 064 NIS+ Domain Name	The name of the client's NIS+

Data entry

String value:

Raritan PDU 1.0

< Back

Next >

Cancel



- g. Select the "Raritan PDU" in the "Vendor class" field, select "001 pdu-tftp-server" from the Available Options list, and type your TFTP server's IPv4 address in the "IP address" field.

DHCP Policy Configuration Wizard

Configure settings for the policy

If the conditions specified in the policy match a client request, the settings will be applied.

Vendor class:

Raritan PDU

Available Options	Description
<input checked="" type="checkbox"/> 001 pdu-tftp-server	
<input type="checkbox"/> 002 pdu-update-control-file	
<input type="checkbox"/> 003 pdu-update-magic	

Data entry

IP address:

192 . 168 . 85 . 93

< Back

Next >

Cancel

- h. Select "002 pdu-update-control-file" from the Available Options list, and type the filename "fwupdate.cfg" in the "String value" field.

**DHCP Policy Configuration Wizard**

**Configure settings for the policy**  
If the conditions specified in the policy match a client request, the settings will be applied.

Vendor class: Raritan PDU

Available Options	Description
<input checked="" type="checkbox"/> 001 pdu-tftp-server	
<input checked="" type="checkbox"/> 002 pdu-update-control-file	
<input type="checkbox"/> 003 pdu-update-magic	

Data entry

String value:  
fwupdate.cfg

< Back   Next >   Cancel

- 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 PXE 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 PXE. Therefore, you must modify the magic cookie's value in DHCP when intending to execute the "fwupdate.cfg" commands next time.*

---

**DHCP Policy Configuration Wizard**

**Configure settings for the policy**  
If the conditions specified in the policy match a client request, the settings will be applied.

Vendor class: Raritan PDU

Available Options	Description
<input checked="" type="checkbox"/> 001 pdu-tftp-server	
<input checked="" type="checkbox"/> 002 pdu-update-control-file	
<input checked="" type="checkbox"/> 003 pdu-update-magic	

Data entry

String value:  
20150427-0001

< Back
Next >
Cancel

---

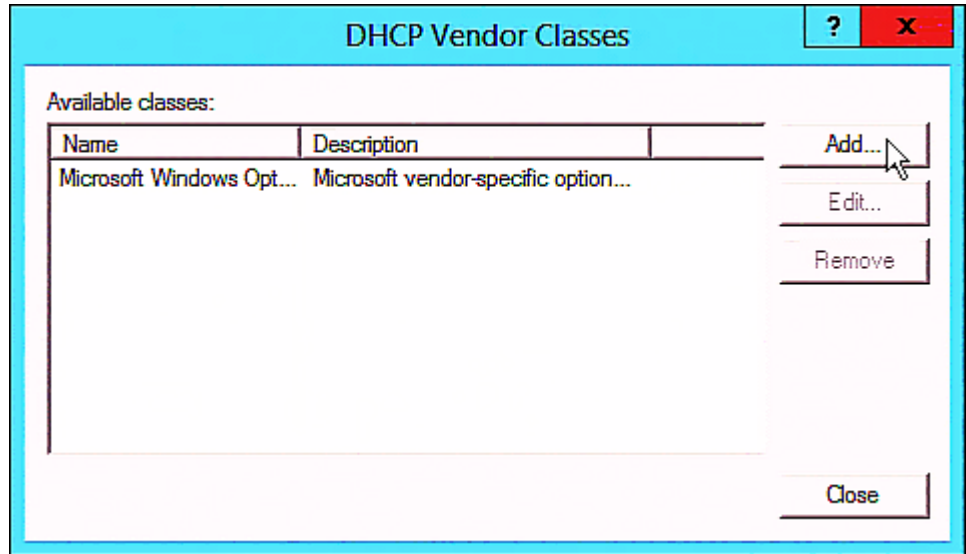
## DHCP IPv6 Configuration in Windows

For those PXE 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 PXE 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.

ID:	Binary:	ASCII:
0000	52 61 72 69 74 61 6E 20	Raritan
0008	50 44 55 20 31 2E 30	PDU 1.0

2. Add three options to the "Raritan PDU 1.0" vendor class.
  - a. Right-click the IPv6 node in DHCP to select Set Predefined Options.

- b. Select Raritan PDU 1.0 in the "Option class" field.

Predefined Options and Values for v6

Option class: Raritan PDU 1.0

Option name: DHCP Standard Options  
Microsoft Windows Options  
Raritan PDU 1.0

Add... Edit... Delete...

Description:

Value

String:

OK Cancel

- c. Click Add to add the first option. Type "pdu-tftp-server" in the Name field, select IP Address as the data type, and type 1 in the Code field.

Option Type

Class: Raritan PDU 1.0

Name: pdu-tftp-server

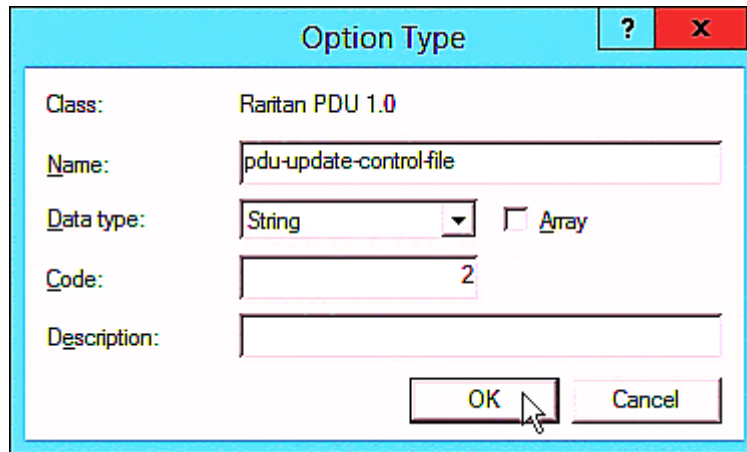
Data type: IP Address ☐ Array

Code: 1

Description:

OK Cancel

- 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.

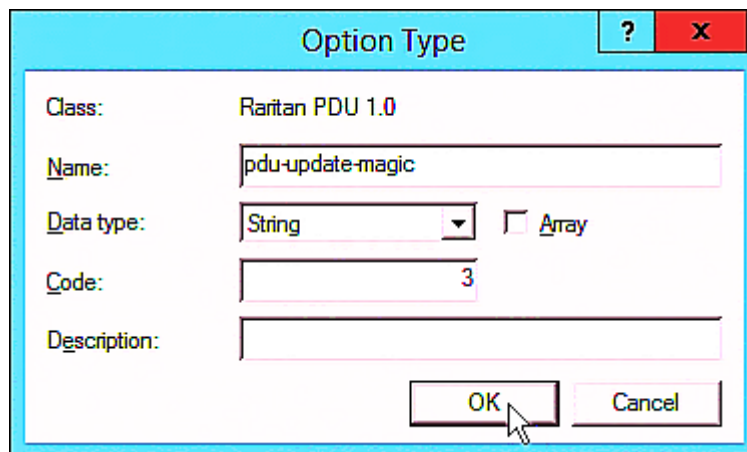


The image shows a dialog box titled "Option Type" with a light blue header bar containing a question mark icon and a red close button. The dialog has a white background with the following fields:
 

- Class:** Raritan PDU 1.0
- Name:** pdu-update-control-file
- Data type:** String (selected in a dropdown menu, with an unchecked checkbox for Array)
- Code:** 2
- Description:** (empty text box)

 At the bottom right, there are two buttons: "OK" and "Cancel". A mouse cursor is pointing at the "OK" button.

- 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.



The image shows a dialog box titled "Option Type" with a light blue header bar containing a question mark icon and a red close button. The dialog has a white background with the following fields:
 

- Class:** Raritan PDU 1.0
- Name:** pdu-update-magic
- Data type:** String (selected in a dropdown menu, with an unchecked checkbox for Array)
- Code:** 3
- Description:** (empty text box)

 At the bottom right, there are two buttons: "OK" and "Cancel". A mouse cursor is pointing at the "OK" button.

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.

The screenshot shows the 'Server Options' dialog box with the 'Advanced' tab selected. The 'Vendor class' is set to 'Raritan PDU 1.0' and the 'User class' is 'Default User Class'. In the 'Available Options' list, '00001 pdu-tftp-server' is selected. The 'IPv6 address' field contains 'fd07:2fa:6cff:1010::200'. The dialog has 'OK', 'Cancel', and 'Apply' buttons at the bottom.

Available Options	Description
<input checked="" type="checkbox"/> 00001 pdu-tftp-server	
<input type="checkbox"/> 00002 pdu-update-control-file	
<input type="checkbox"/> 00003 pdu-update-image	

Data entry

IPv6 address:  
fd07:2fa:6cff:1010::200



- d. Select "00002 pdu-update-control-file" from the Available Options list, and type the filename "fwupdate.cfg" in the "String value" field.

The screenshot shows the 'Server Options' dialog box with the 'Advanced' tab selected. The 'Vendor class' is set to 'Raritan PDU 1.0' and the 'User class' is 'Default User Class'. The 'Available Options' list contains three entries: '00001 pdu-tftp-server', '00002 pdu-update-control-file' (which is selected), and '00003 pdu-update-magic'. The 'String value' field is populated with 'fwupdate.cfg'. The 'Data entry' section is visible below the list.

- 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 PXE 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 PXE. Therefore, you must modify the magic cookie's value in DHCP when intending to execute the "fwupdate.cfg" commands next time.*

---

**Server Options**

General Advanced

Vendor class: Raritan PDU 1.0

User class: Default User Class

Available Options	Description
<input checked="" type="checkbox"/> 00002 pdu-update-control-file	
<input checked="" type="checkbox"/> 00003 pdu-update-magic	

< III >

Data entry

String value:

20150427-6001

OK Cancel Apply

## 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 PXE 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 PXE 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 PXE 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 PXE. 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 PXE 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 PXE 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 PXE. Therefore, you must modify the magic cookie's value in DHCP when intending to execute the "fwupdate.cfg" commands next time.*

---

► IPv6 illustration example in *dhcpd6.conf*:

```
[...]

option space RARITAN code width 2 length width 2 hash size 3;
option RARITAN.pdu-tftp-server code 1 = ip6-address;
option RARITAN.pdu-update-control-file code 2 = text;
option RARITAN.pdu-update-magic code 3 = text;
option vsio.RARITAN code 13742 = encapsulate RARITAN;

[...]

subnet6 xxxx {

[...]
    option RARITAN.pdu-tftp-server 1::2;
    option RARITAN.pdu-update-control-file "fwupdate.cfg";
    option RARITAN.pdu-update-magic "20150123-0001";
[...]
}
```

## Appendix D Resetting to Factory Defaults

For security reasons, the PXE device can be reset to factory defaults only at the local console.

---

**Important: Exercise caution before resetting the PXE 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 forever.**

---

### In This Chapter

Using the CLI Command .....382

---

### Using the CLI Command

The Command Line Interface (CLI) provides a reset command for restoring the PXE to factory defaults. For information on CLI, see **Using the Command Line Interface** (on page 218).

► **To reset to factory defaults after logging in to the CLI:**

1. Connect to the PXE device. See **Logging in to CLI** (on page 219) or **Connecting the PXE to a Computer** (on page 14).
2. Launch a terminal emulation program such as HyperTerminal, Kermit, or PuTTY, and open a window on the PXE. For information on the serial port configuration, see Step 2 of **Initial Network Configuration via CLI** (on page 16).
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 PXE provides an easier way to reset the product to factory defaults in the CLI prior to login.

1. Connect to the PXE and launch a terminal emulation program as described in the above procedure.
2. At the Username prompt in the CLI, type "factorydefaults" and press Enter.

```
Username: factorydefaults
```

3. Type `y` on a confirmation message to perform the reset.

## Appendix E Available SCP Commands

You can perform a Secure Copy (SCP) command to update the PXE firmware, do bulk configuration, or back up and restore the configuration.

### In This Chapter

Firmware Update via SCP .....	384
Bulk Configuration via SCP .....	385
Backup and Restore via SCP .....	386

---

### Firmware Update via SCP

Same as any PXE 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 202).

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 PXE 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 PXE 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 PXE, and shows the transmission speed and percentage.
  4. When the transmission is complete, it shows the following message, indicating that the PXE 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 PXE.
- b. Copy the configuration file to one or multiple destination PXE.

For detailed information on the bulk configuration requirements, see **Bulk Configuration** (on page 196).

► **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 PXE 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 PXE 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 PXE 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 PXE, 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 PXE, 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 PXE 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 PXE 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 PXE 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 PXE, and displays the following message.

Starting restore operation. The connection will be closed now.

► **SCP command examples:**

- Backup example:

```
scp admin@192.168.87.50:/backup_settings.xml
```

- Settings restoration example:

```
scp backup_settings.xml
admin@192.168.87.50:/settings_restore
```

---

*Tip: The PSCP works in a similar way to the SCP so its syntax is similar.*

*Backup operation -- pscp <user name>@<device ip>:/backup\_settings.xml*

*Restoration operation -- pscp backup\_settings.xml <user name>@<device ip>:/settings\_restore*

---

## Appendix F LDAP Configuration Illustration

This section provides an LDAP example for illustrating the configuration procedure using Microsoft Active Directory® (AD). To configure LDAP authentication, four main steps are required:

- a. Determine user accounts and roles (groups) intended for the PXE
- b. Create user groups for the PXE on the AD server
- c. Configure LDAP authentication on the PXE device
- d. Configure roles on the PXE 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 .....	388
Step B. Configure User Groups on the AD Server .....	389
Step C. Configure LDAP Authentication on the PXE Device .....	390
Step D. Configure Roles on the PXE Device .....	392

---

### Step A. Determine User Accounts and Roles

Determine the user accounts and roles (groups) that are authenticated for accessing the PXE. 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 PXE on the AD server, and then make appropriate users members of these groups.

In this illustration, we assume:

- The groups (roles) for the PXE 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 PXE Device

You must enable and set up LDAP authentication properly on the PXE device to use external authentication.

In the illustration, we assume:

- The DNS server settings have been configured properly. See **Modifying Network Settings** (on page 69) and **Role of a DNS Server** (on page 76).
- 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 PXE with the information about the AD server.
  - IP Address / Hostname - Type the domain name *techadssl.com* or IP address *192.168.56.3*.

---

*Important: Without the TLS encryption enabled, you can type either the domain name or IP address in this field, but you must type the fully qualified domain name if the TLS encryption is enabled.*

---

- Use settings from LDAP server - Leave the checkbox deselected.
- Type of LDAP Server - Select "Microsoft Active Directory" from the drop-down list.
- Security - Select "None" since the TLS encryption is not applied in this example.
- Port (None/StartTLS) - Ensure the field is set to 389.
- Port (TLS) and CA Certificate - Skip the two fields since the TLS encryption is not enabled.
- Use Bind Credentials - Do NOT select this checkbox because anonymous bind is used.
- Bind DN, Bind Password and Confirm Bind Password -- Skip the three fields because anonymous bind is used.

- Base DN for Search - Type `dc=techadssl,dc=com` as the starting point where your search begins on the AD server.
- Login Name Attribute - Ensure the field is set to `sAMAccountName` because the LDAP server is Microsoft Active Directory.
- User Entry Object Class - Ensure the field is set to `user` because the LDAP server is Microsoft Active Directory.
- User Search Subfilter - The field is optional. The subfilter information is also useful for filtering out additional objects in a large directory structure. In this example, we leave it blank.
- Active Directory Domain - Type `techadssl.com`.

**Create new LDAP Server Configuration**

IP Address / Hostname:  ⓘ

☐ Use settings from LDAP Server

Select LDAP Server:

Type of LDAP Server:

Security:

Port (None/StartTLS):

Port (TLS):

☒ Enable verification of LDAP Server Certificate

CA Certificate: not set

☐ Allow expired and not yet valid certificates

☐ Anonymous Bind

☐ Use Bind Credentials

Bind DN:

Bind Password:

Confirm Bind Password:

Base DN for Search:

Login Name Attribute:

User Entry Object Class:

User Search Subfilter:

Active Directory Domain:

5. Click OK. The LDAP server is saved.

6. Click OK. The LDAP authentication is activated.

---

*Note: If the PXE 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 PXE and the LDAP server to use the same NTP server(s).*

---

---

## Step D. Configure Roles on the PXE Device

A role on the PXE device determines the system and outlet permissions. You must create the roles whose names are identical to the user groups created for the PXE 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 PXE nor access the outlets.
- Users assigned to the *PX\_Admin* role have the Administrator permissions so they can both configure PXE and access the outlets.

► **To create the *PX\_User* role with appropriate permissions assigned:**

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

---

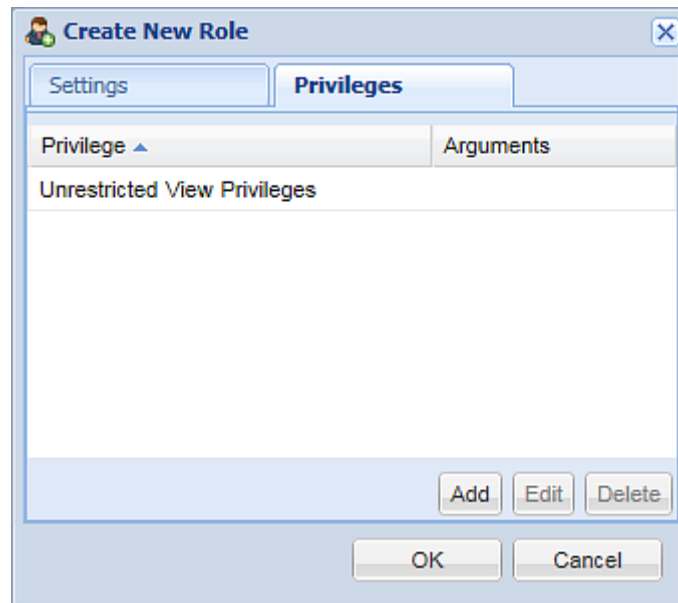
*Tip: You can also access the Manage Roles dialog by clicking the Manage Roles button in the Edit User 'XXX' dialog.*

---

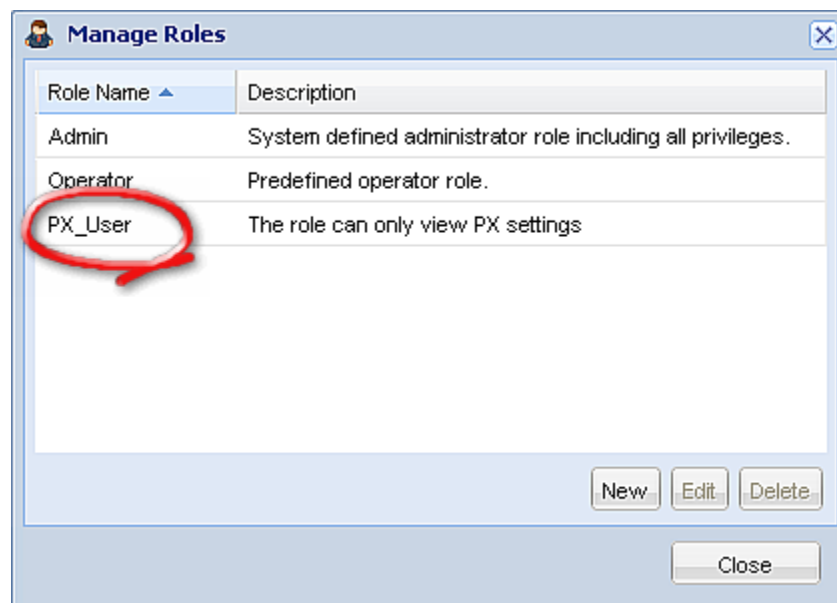
2. Click New. The Create New Role dialog appears.
3. Type *PX\_User* in the Role Name field.
4. Type a description for the *PX\_User* role in the Description field. In this example, we type "The role can only view PX settings" to describe the role.
5. Click the Privileges tab to select "Unrestricted 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.

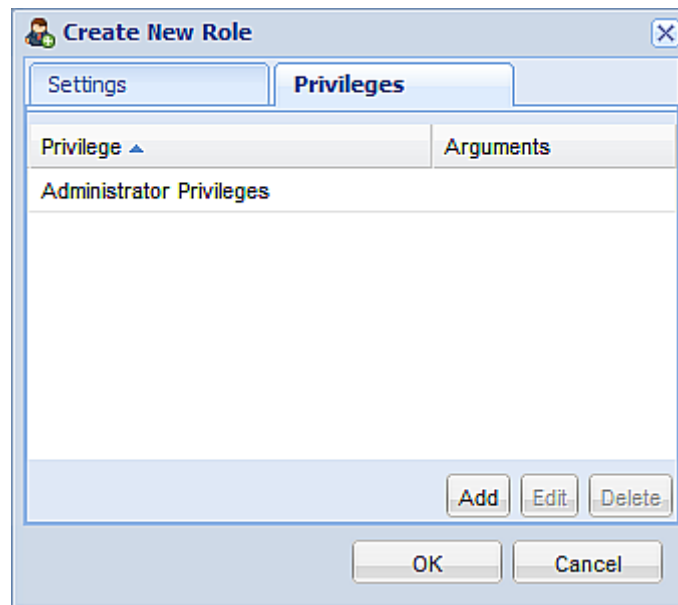


7. Keep the Manage Roles dialog opened to create the PX\_Admin role.

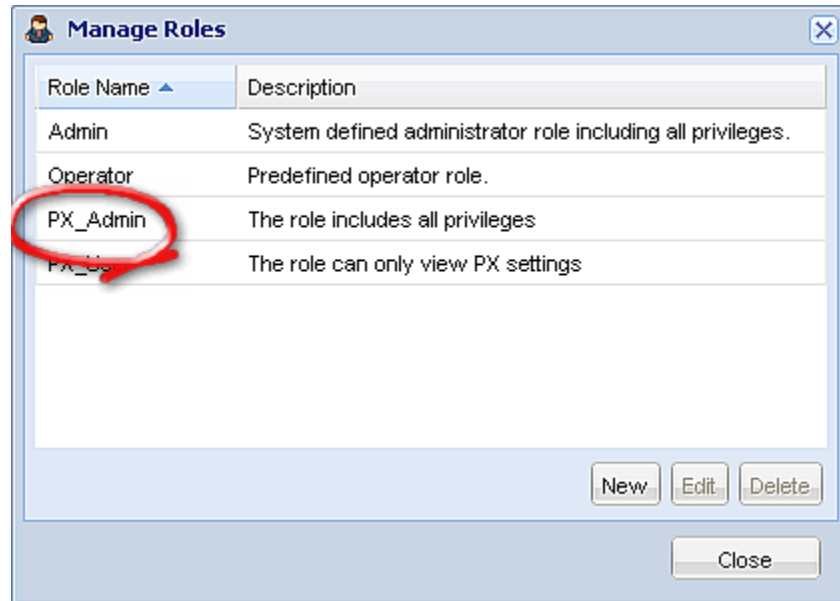
► **To create the PX\_Admin role with full permissions assigned:**

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 PXE 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 G Updating the LDAP Schema

## In This Chapter

Returning User Group Information .....	396
Setting the Registry to Permit Write Operations to the Schema .....	397
Creating a New Attribute .....	397
Adding Attributes to the Class .....	398
Updating the Schema Cache.....	400
Editing rcusergroup Attributes for User Members .....	400

---

## 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 PXE 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:

rcusergroup                      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.

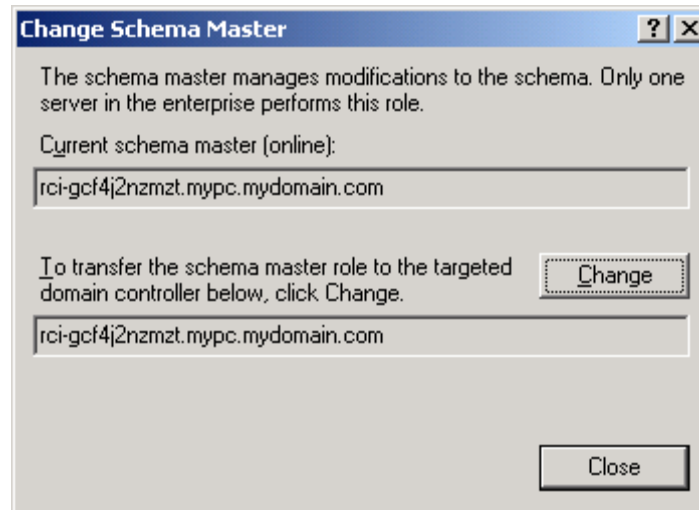
---

## 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.

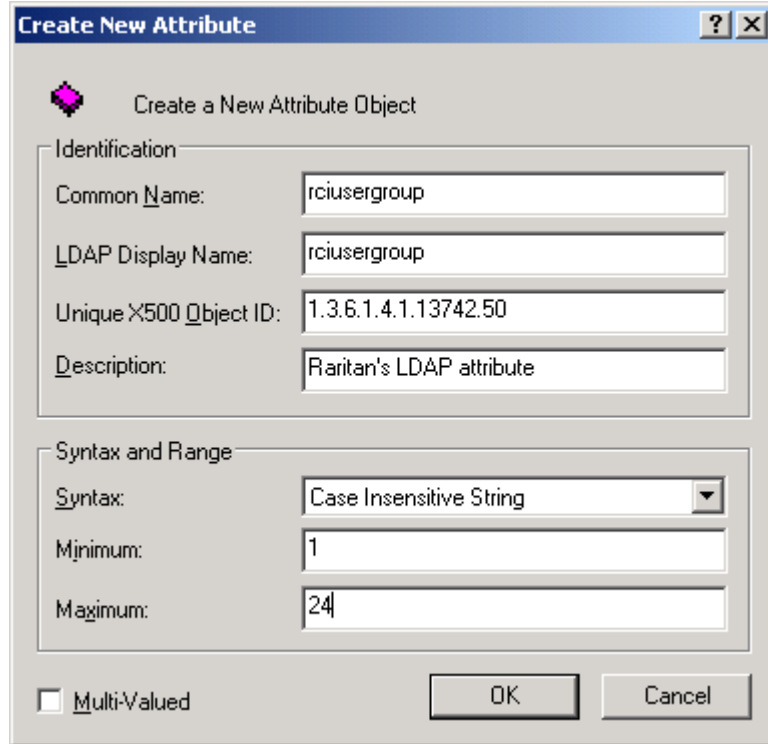
---

## Creating a New Attribute

► **To create new attributes for the rcigroup 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.

The image shows a Windows-style dialog box titled "Create New Attribute". It has a blue title bar with a question mark icon and a close button. The main area is light gray and contains two sections. The first section, "Identification", has four text input fields: "Common Name:" with the value "rciusergroup", "LDAP Display Name:" with the value "rciusergroup", "Unique X500 Object ID:" with the value "1.3.6.1.4.1.13742.50", and "Description:" with the value "Raritan's LDAP attribute". The second section, "Syntax and Range", has a "Syntax:" dropdown menu set to "Case Insensitive String", a "Minimum:" text input field with the value "1", and a "Maximum:" text input field with the value "24". At the bottom left is a checkbox labeled "Multi-Valued" which is currently unchecked. At the bottom right are two buttons: "OK" and "Cancel".

**Create New Attribute**

Create a New Attribute Object

Identification

Common Name: rciusergroup

LDAP Display Name: rciusergroup

Unique X500 Object ID: 1.3.6.1.4.1.13742.50

Description: Raritan's LDAP attribute

Syntax and Range

Syntax: Case Insensitive String

Minimum: 1

Maximum: 24

☐ Multi-Valued

OK Cancel

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.

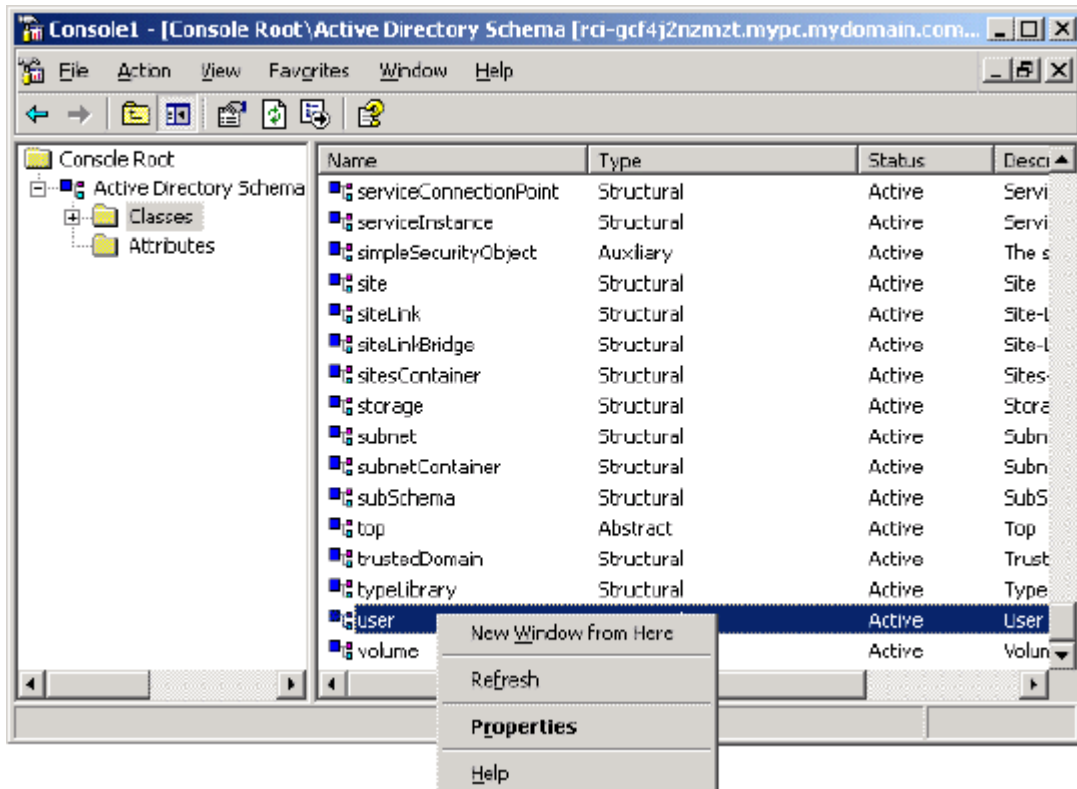
---

## Adding Attributes to the Class

► **To add attributes to the class:**

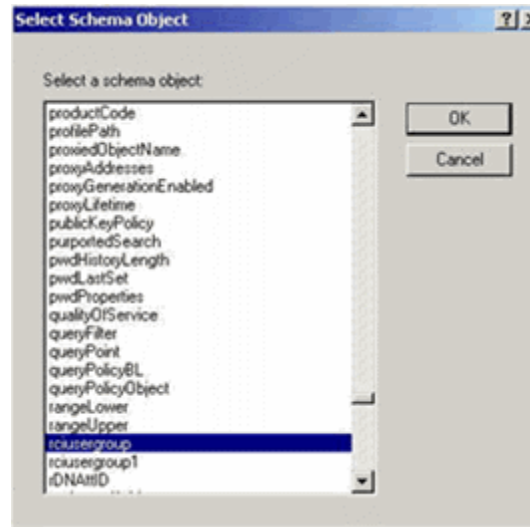
1. Click Classes in the left pane of the window.

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 rcusergroup 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 rcusergroup Attributes for User Members

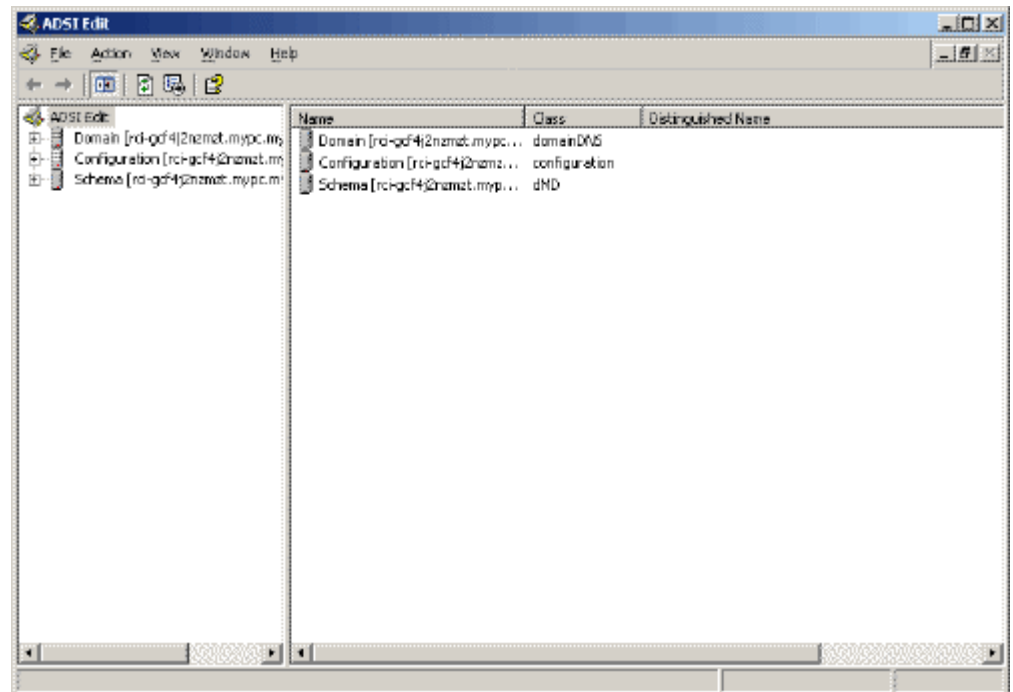
To run the Active Directory® script on a Windows 2003® server, use the script provided by Microsoft® (available on the Windows 2003 server installation CD). These scripts are loaded onto your system with a Microsoft® Windows 2003 installation. ADSI (Active Directory Service Interface) acts as a low-level 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 rcusergroup:**

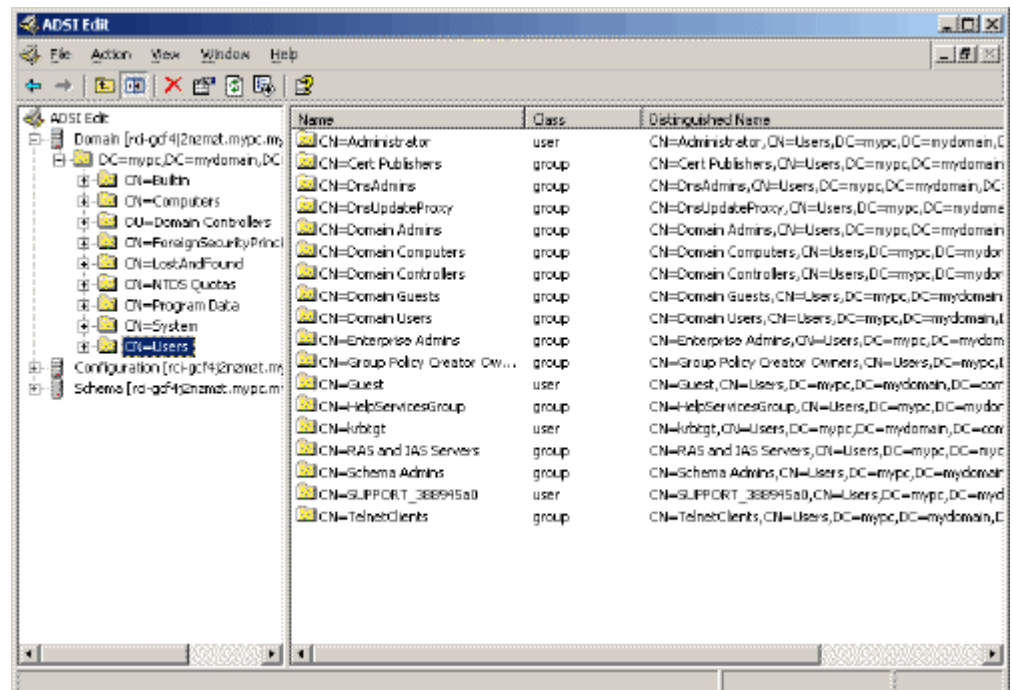
1. From the installation CD, choose Support > Tools.
2. Double-click SUPTOOLS.MSI to install the support tools.



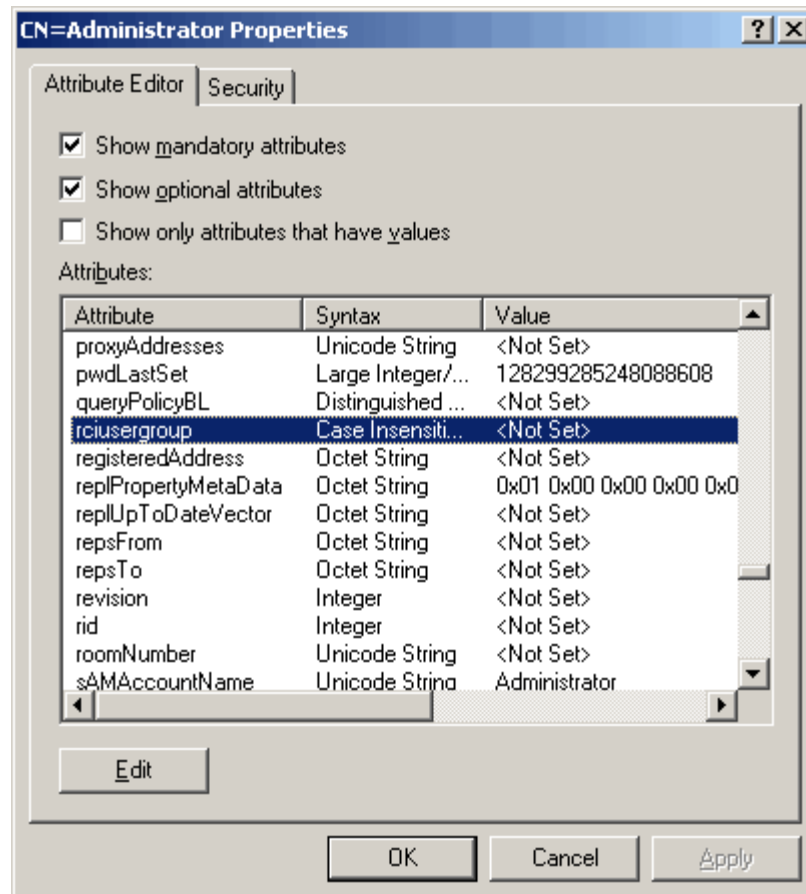
- Go to the directory where the support tools were installed. Run `adsiedit.msc`. The ADSI Edit window opens.



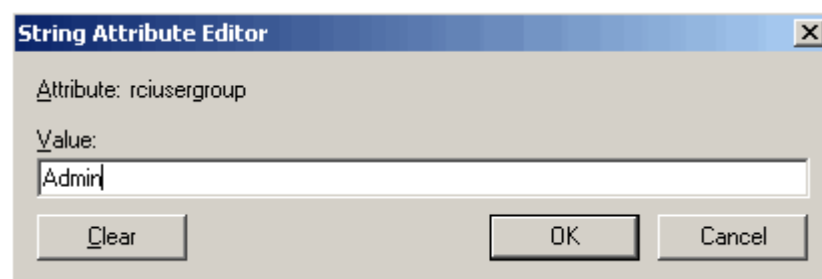
- Open the Domain.
- In the left pane of the window, select the CN=Users folder.



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 PXE) in the Edit Attribute field. Click OK.



# Appendix H RADIUS Configuration Illustration

This section provides illustrations for configuring RADIUS authentication. One illustration is based on the Microsoft® Network Policy Server (NPS), and the other is based on a non-Windows RADIUS server, such as FreeRADIUS.

The following steps are required for any RADIUS authentication:

- 1. Configure RADIUS authentication on the PXE device. See **Adding RADIUS Server Settings** (on page 125).
- 2. Configure roles on the PXE device. See **Creating a Role** (on page 97).
- 3. Configure your RADIUS server. See **Microsoft Network Policy Server** (on page 403) or **Non-Windows RADIUS Server** (on page 427).

## In This Chapter

Microsoft Network Policy Server .....	403
Non-Windows RADIUS Server .....	427

---

### 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 PXE 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 424).

---

### Step A: Add Your PXE as a RADIUS Client

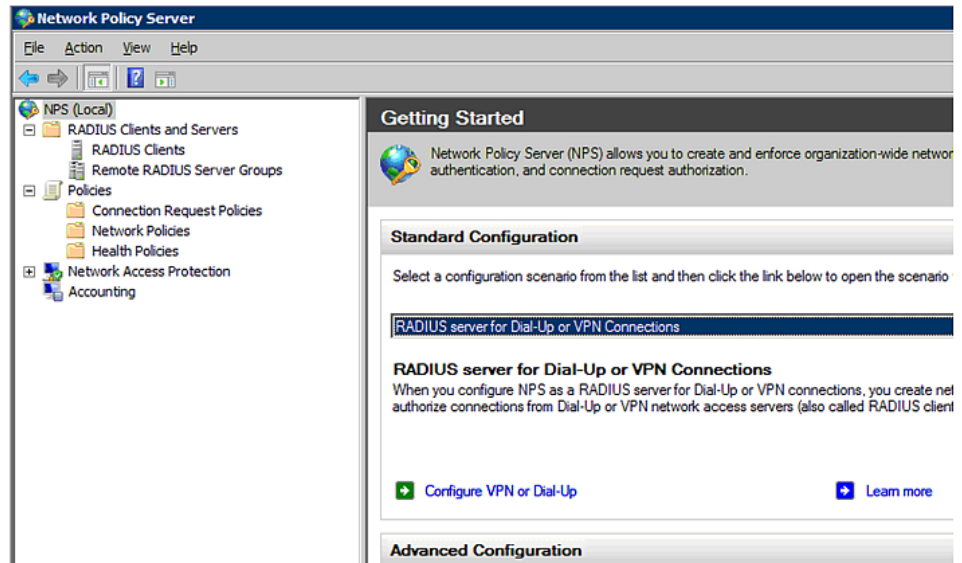
The RADIUS implementation on a PXE follows the standard RADIUS Internet Engineering Task Force (IETF) specification so you must select "RADIUS Standard" as its vendor name when configuring the NPS server.

In this illustration, we assume:

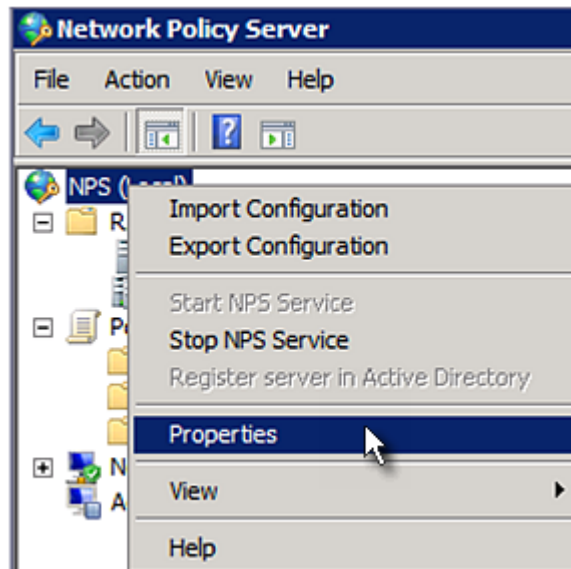
- IP address of your PXE: 192.168.56.29
- RADIUS authentication port specified for PXE: 1812
- RADIUS accounting port specified for PXE: 1813

► **To add your PXE to the RADIUS NPS:**

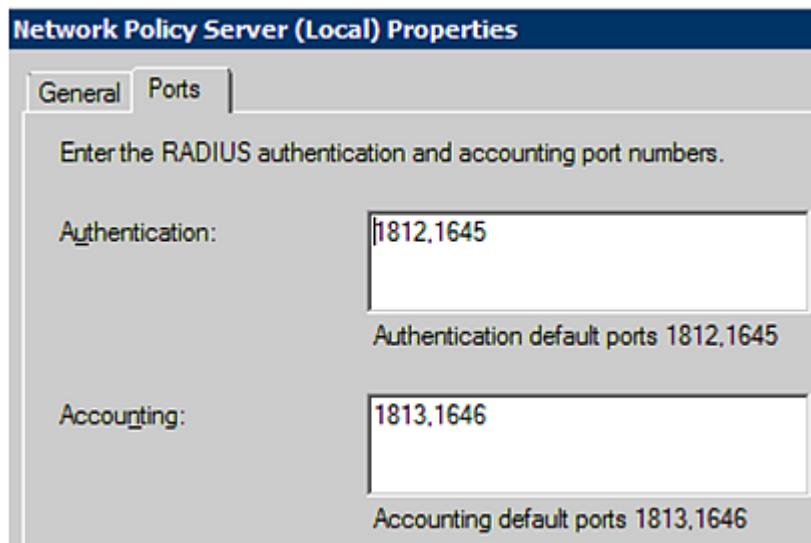
1. Choose Start > Administrative Tools > Network Policy Server. The Network Policy Server console window opens.



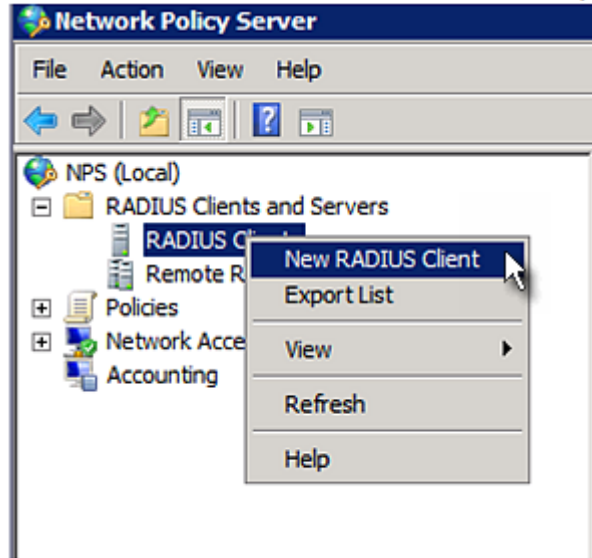
2. Right-click NPS (Local), and select Properties.



Verify the authentication and accounting port numbers shown in the properties dialog are the same as those specified on your PXE. 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 PXE to NPS:
  - a. Verify the "Enable this RADIUS client" checkbox is selected.
  - b. Type a name for identifying your PXE 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 PXE.

**New RADIUS Client**

☒ Enable this RADIUS client

**Name and Address**  
 Friendly name:  
  
 Address (IP or DNS):

**Vendor**  
 Specify RADIUS Standard for most RADIUS clients, or select the RADIUS client vendor from the list.  
 Vendor name:

**Shared Secret**  
 To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

☒ Manual ☐ Generate

Shared secret:  
  
 Confirm shared secret:

**Additional Options**  
☐ Access-Request messages must contain the Message-Authenticator attribute  
☐ RADIUS client is NAP-capable

5. Click OK.

### Step B: Configure Connection Request Policies

You need to configure the following for connection request policies:

- a. IP address or host name of the PXE

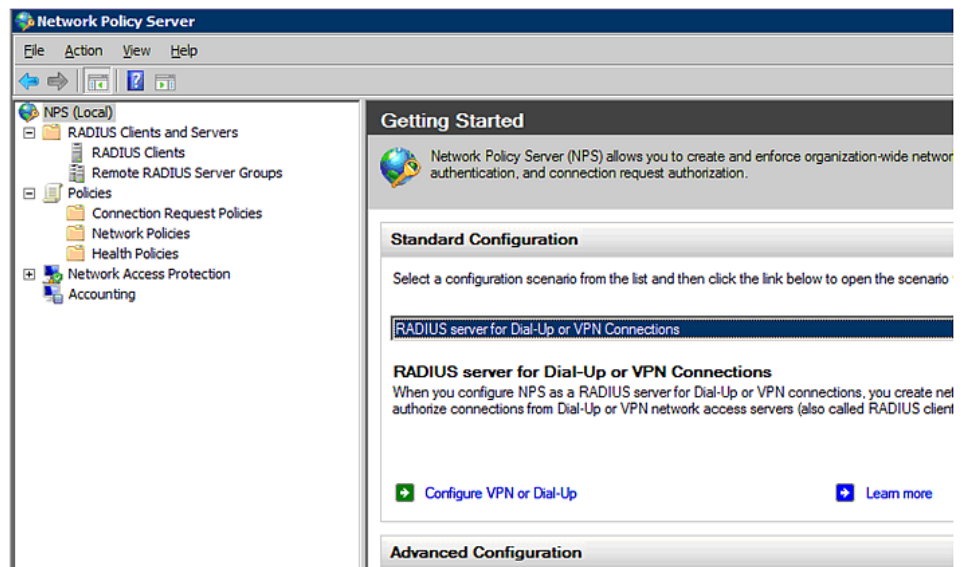
- b. Connection request forwarding method
- c. Authentication method(s)
- d. Standard RADIUS attributes

In the following illustration, we assume:

- *Local* NPS server is used
- IP address of your PXE: *192.168.56.29*
- RADIUS protocol selected on your PXE: *CHAP*
- Existing role of your PXE: *Admin*

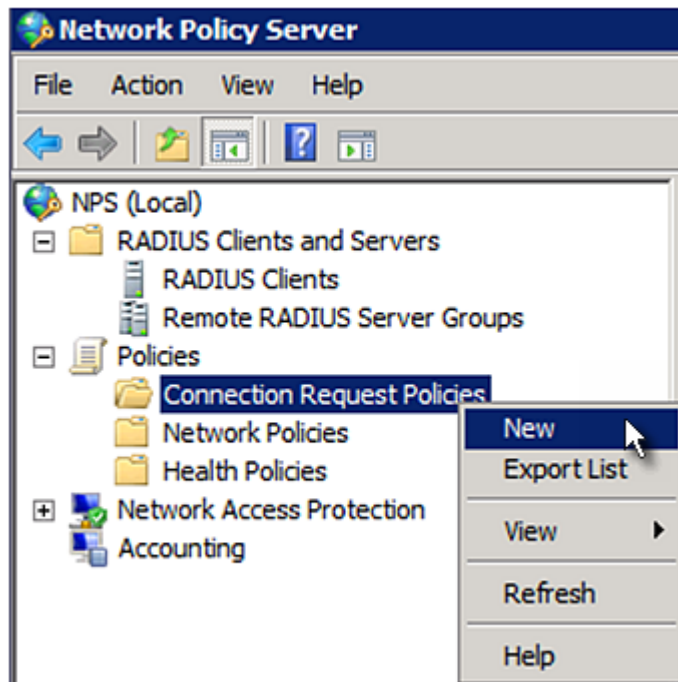
► **To configure connection request policies:**

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.

**New Connection Request Policy**



## Specify Connection Request Policy Name

You can specify a name for your connection request policy and it will be applied.

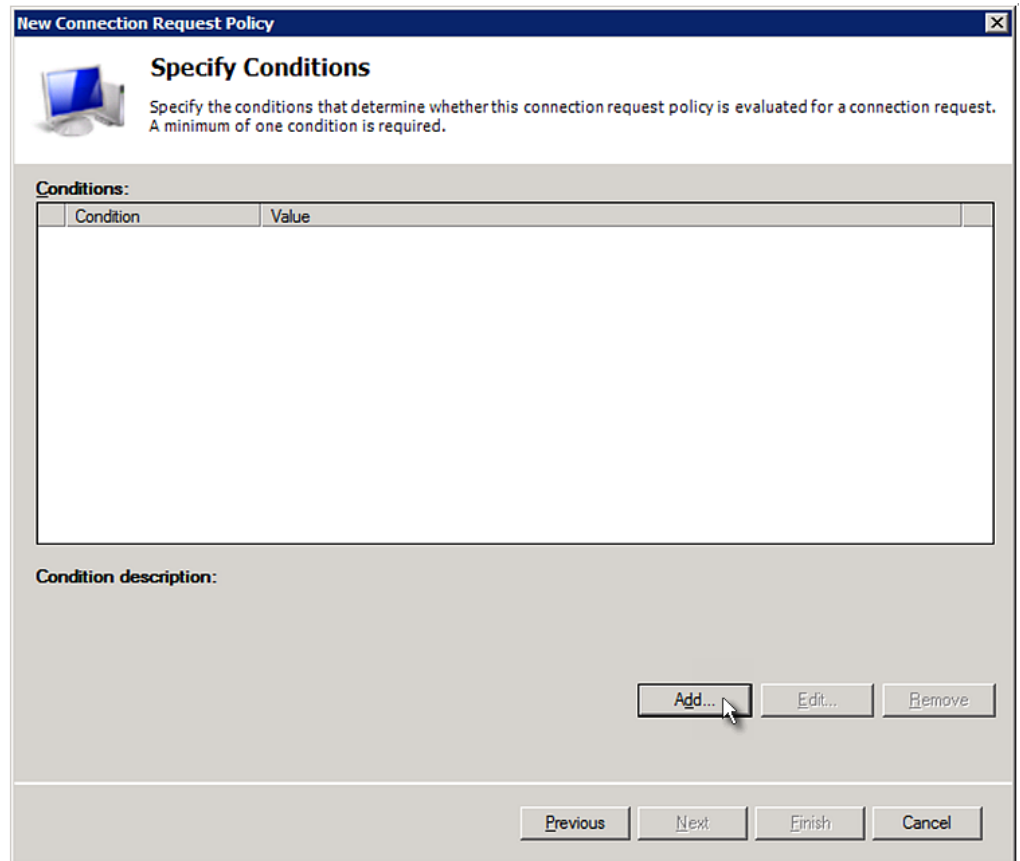
**Policy name:**

**Network connection method**  
Select the type of network access server that sends the connection request to NPS.  
Type or Vendor specific.

☒ **Type of network access server:**

☐ **Vendor specific:**

4. Click Next to show the "Specify Conditions" screen. Click Add.



**New Connection Request Policy**

**Specify Conditions**

Specify the conditions that determine whether this connection request policy is evaluated for a connection request. A minimum of one condition is required.

**Conditions:**

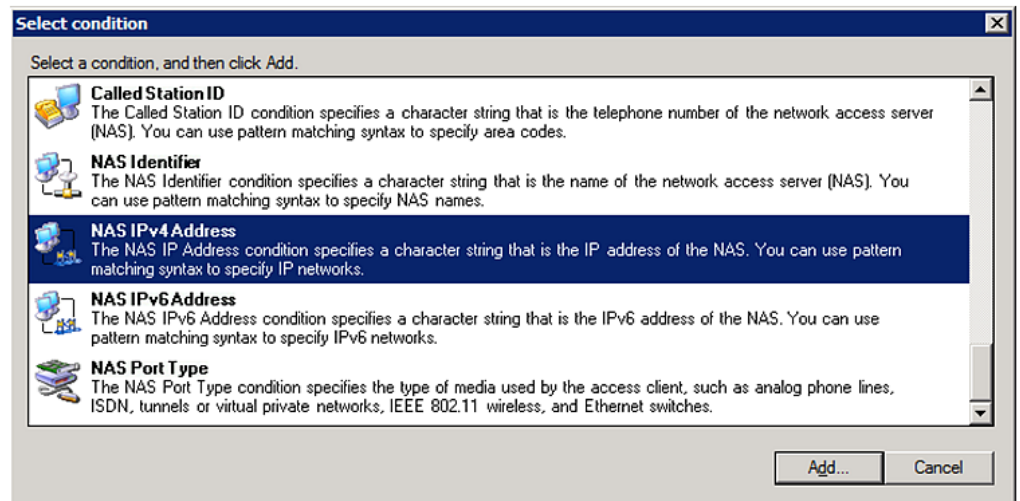
Condition	Value
-----------	-------

**Condition description:**

Buttons: Add..., Edit..., Remove

Buttons: Previous, Next, Finish, Cancel

5. The "Select condition" dialog appears. Click Add.



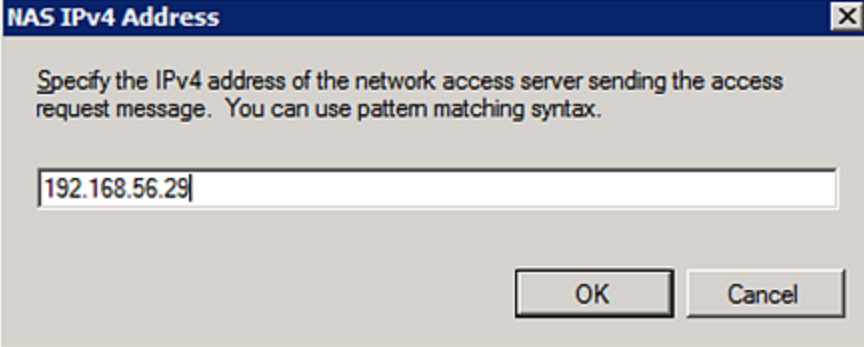
**Select condition**

Select a condition, and then click Add.

- Called Station ID**  
The Called Station ID condition specifies a character string that is the telephone number of the network access server (NAS). You can use pattern matching syntax to specify area codes.
- NAS Identifier**  
The NAS Identifier condition specifies a character string that is the name of the network access server (NAS). You can use pattern matching syntax to specify NAS names.
- NAS IPv4 Address**  
The NAS IP Address condition specifies a character string that is the IP address of the NAS. You can use pattern matching syntax to specify IP networks.
- NAS IPv6 Address**  
The NAS IPv6 Address condition specifies a character string that is the IPv6 address of the NAS. You can use pattern matching syntax to specify IPv6 networks.
- NAS Port Type**  
The NAS Port Type condition specifies the type of media used by the access client, such as analog phone lines, ISDN, tunnels or virtual private networks, IEEE 802.11 wireless, and Ethernet switches.

Buttons: Add..., Cancel

6. The NAS IPv4 Address dialog appears. Type the PXE IP address -- 192.168.56.29, and click OK.



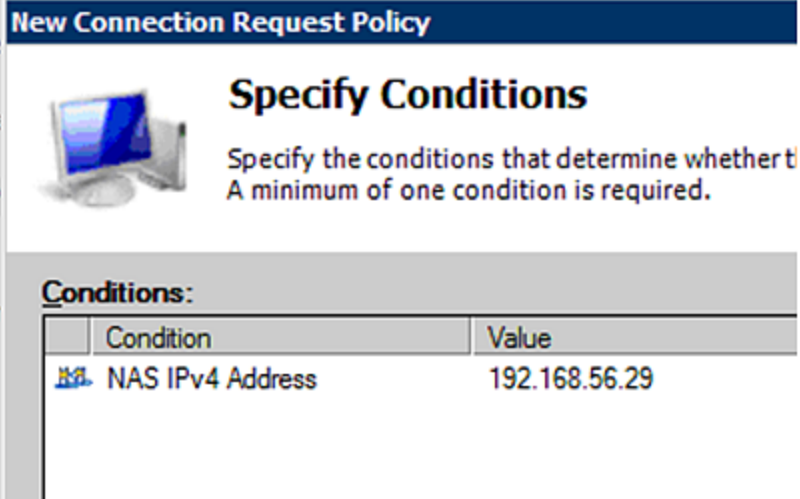
The dialog box is titled "NAS IPv4 Address" and contains a text field with the IP address "192.168.56.29". Below the text field are "OK" and "Cancel" buttons.

Specify the IPv4 address of the network access server sending the access request message. You can use pattern matching syntax.

192.168.56.29

OK Cancel

7. Click Next in the New Connection Request Policy dialog.



The dialog box is titled "New Connection Request Policy" and contains a section titled "Specify Conditions". Below this section is a table with two columns: "Condition" and "Value". The table contains one row with the condition "NAS IPv4 Address" and the value "192.168.56.29".

Specify Conditions

Specify the conditions that determine whether a minimum of one condition is required.

Conditions:

Condition	Value
NAS IPv4 Address	192.168.56.29

8. Select "Authenticate requests on this server" because a local NPS server is used in this example. Then click Next.

---

*Note: Connection Request Forwarding options must match your environment.*

---

The screenshot shows a Windows-style wizard window titled "New Connection Request Policy". The main heading is "Specify Connection Request Forwarding". Below the heading is a small icon of a computer and a text box stating: "The connection request can be authenticated by the local server or it can be forwarded to RADIUS servers in a remote RADIUS server group." Below this is a grey bar with the text: "If the policy conditions match the connection request, these settings are applied." Under the "Settings:" label, there is a left-hand pane titled "Forwarding Connection Request" and a right-hand pane. The right-hand pane contains the instruction: "Specify whether connection requests are processed locally, are forwarded to remote RADIUS servers for authentication, or are accepted without authentication." There are three radio button options: 1. "Authenticate requests on this server" (which is selected), 2. "Forward requests to the following remote RADIUS server group for authentication:" (which has a dropdown menu showing "<not configured>" and a "New..." button), and 3. "Accept users without validating credentials". At the bottom of the window are four buttons: "Previous", "Next", "Finish", and "Cancel".

9. When the system prompts you to select the authentication method, select the following two options:
  - Override network policy authentication settings
  - CHAP -- the PXE uses "CHAP" in this example

---

*Note: If your PXE uses PAP, then select "PAP."*

---

#### New Connection Request Policy



### Specify Authentication Methods

Configure one or more authentication methods required authentication, you must configure an EAP type. If you d Protected EAP.

☒ **Override network policy authentication settings**

These authentication settings are used rather than the constraints and authentication connections with NAP, you must configure PEAP authentication here.

EAP types are negotiated between NPS and the client in the order in which

**EAP Types:**

**Less secure authentication methods:**

- ☐ Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
  - ☐ User can change password after it has expired
- ☐ Microsoft Encrypted Authentication (MS-CHAP)
  - ☐ User can change password after it has expired
- ☒ Encrypted authentication (CHAP)
- ☐ Unencrypted authentication (PAP, SPAP)
- ☐ Allow clients to connect without negotiating an authentication method.

10. Select Standard to the left of the dialog and then click Add.

**New Connection Request Policy**

### Configure Settings

NPS applies settings to the connection request if all of the connection request policy conditions for the policy are matched.

Configure the settings for this network policy.  
If conditions match the connection request and the policy grants access, settings are applied.

**Settings:**

Specify a Realm Name

☐ Attribute

**RADIUS Attributes**

☒ Standard

☒ Vendor Specific

To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

**Attributes:**

Name	Value
------	-------

11. Select Filter-Id from the list of attributes and click Add.

**Add Standard RADIUS Attribute**

To add an attribute to the settings, select the attribute, and then click Add.

To add a custom or predefined Vendor Specific attribute, close this dialog and select Vendor Specific, and then click Add.

Access type:  
All

Attributes:

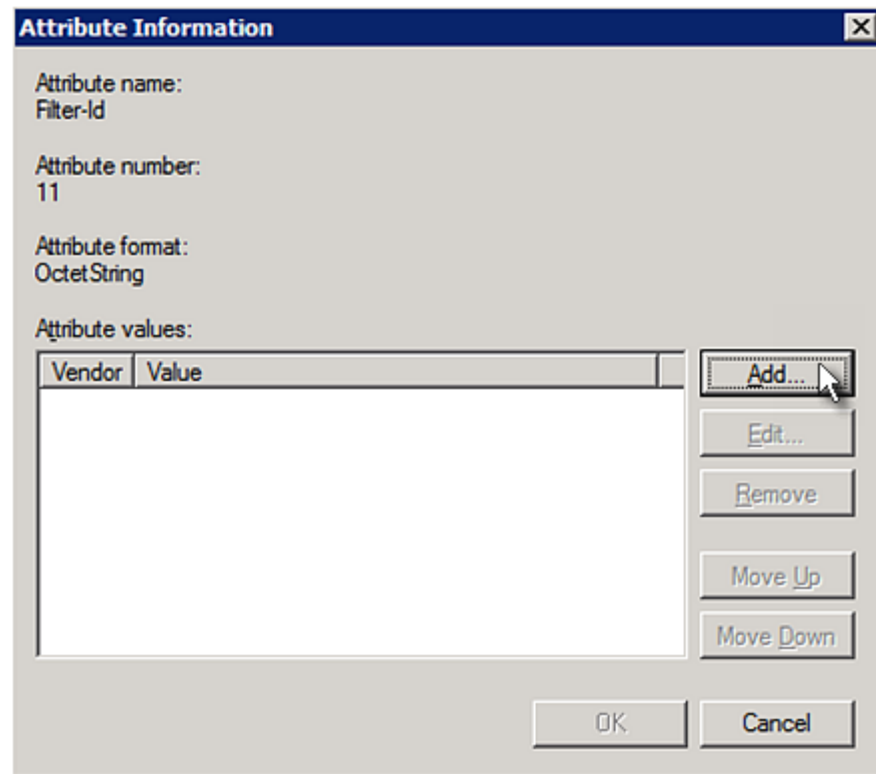
Name
Acct-Interim-Interval
Callback-Id
Callback-Number
Class
<b>Filter-Id</b>
Framed-AppleTalk-Link
Framed-AppleTalk-Network

Description:  
Specifies the name of filter list for the user requesting authentication.

Add... Close

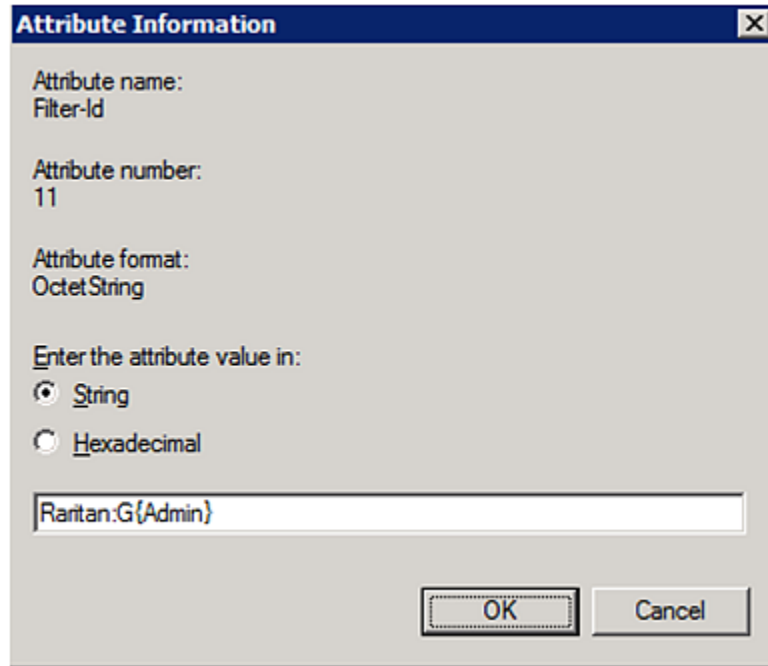


12. In the Attribute Information dialog, click Add.



13. Select String, type *Raritan:G{Admin}* in the text box, and then click OK.

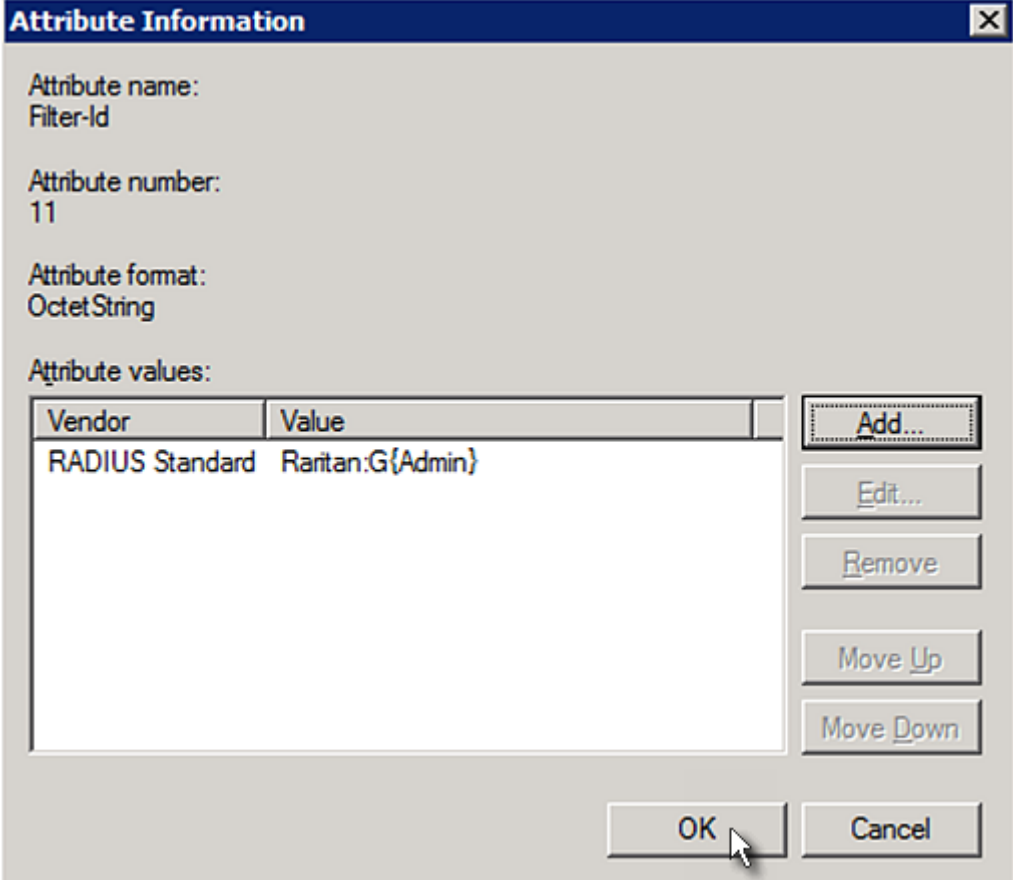
*Admin* inside the curved brackets {} is the existing role on the PXE. It is recommended to use the Admin role to test this configuration. The role name is case sensitive.



The image shows a Windows-style dialog box titled "Attribute Information". It contains the following fields and controls:

- Attribute name:** Filter-Id
- Attribute number:** 11
- Attribute format:** OctetString
- Enter the attribute value in:**
  - ☒ String
  - ☐ Hexadecimal
- Value field:** A text box containing "Raritan:G{Admin}"
- Buttons:** "OK" and "Cancel" at the bottom right.

14. The new attribute is added. Click OK.



The dialog box, titled "Attribute Information", contains the following fields and controls:


- Attribute name:** Filter-Id
- Attribute number:** 11
- Attribute format:** OctetString
- Attribute values:** A table with two columns: Vendor and Value.

Vendor	Value
RADIUS Standard	Raritan:G{Admin}

On the right side of the table, there are five buttons: Add..., Edit..., Remove, Move Up, and Move Down. At the bottom right of the dialog are OK and Cancel buttons. A mouse cursor is pointing at the OK button.

15. Click Next to continue.

### New Connection Request Policy




## Configure Settings

NPS applies settings to the connection request if all of the connect matched.


Configure the settings for this network policy.  
If conditions match the connection request and the policy grants access, settings are a

**Settings:**

#### Specify a Realm Name

 Attribute

#### RADIUS Attributes

 Standard

☒ Vendor Specific

To send additional attributes to RADIUS client then click Edit. If you do not configure an attr your RADIUS client documentation for require

Attributes:

Name	Value
Filter-Id	Raritan:G{Admin}

16. A summary showing connection request policy settings is displayed.  
Click Finish to close the dialog.

**New Connection Request Policy**

### Completing Connection Request Policy Wizard

You have successfully created the following connection request policy:

**KXII Policy**

**Policy conditions:**

Condition	Value
NAS IPv4 Address	192.168.56.29

**Policy settings:**

Condition	Value
Authentication Provider	Local Computer
Override Authentication	Enabled
Authentication Method	Encryption authentication (CHAP)
Filter-Id	Raritan:G{Admin}

To close this wizard, click Finish.

### Step C: Configure a Vendor-Specific Attribute

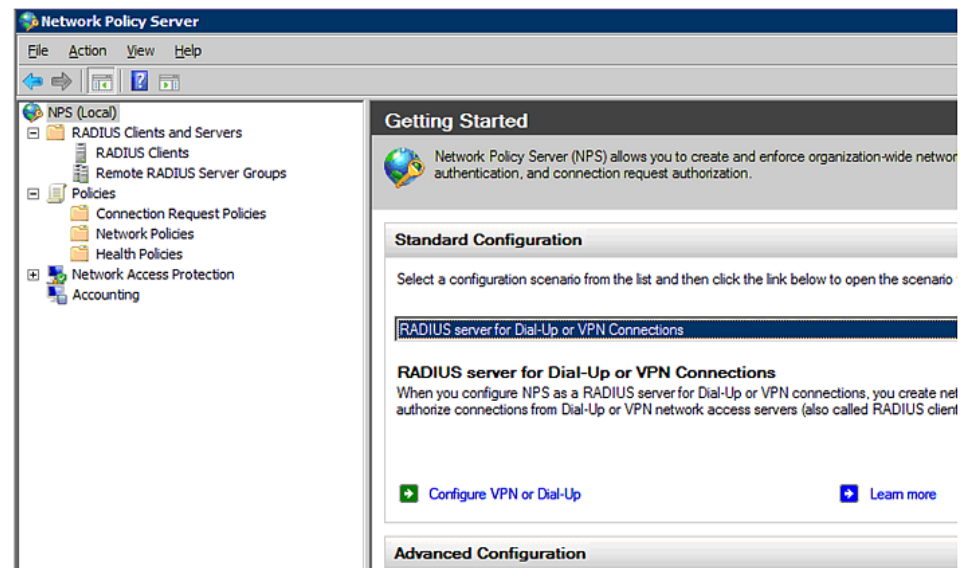
You must specify a vendor-specific attribute (VSA) for Raritan on Windows 2008 NPS. Raritan's vendor code is **13742**.

In the following illustration, we assume:

- There are three roles available on your PXE: *Admin*, *User*, and *SystemTester*.

#### ► To configure VSA:

1. Open the NPS console, and expand the Policies folder.

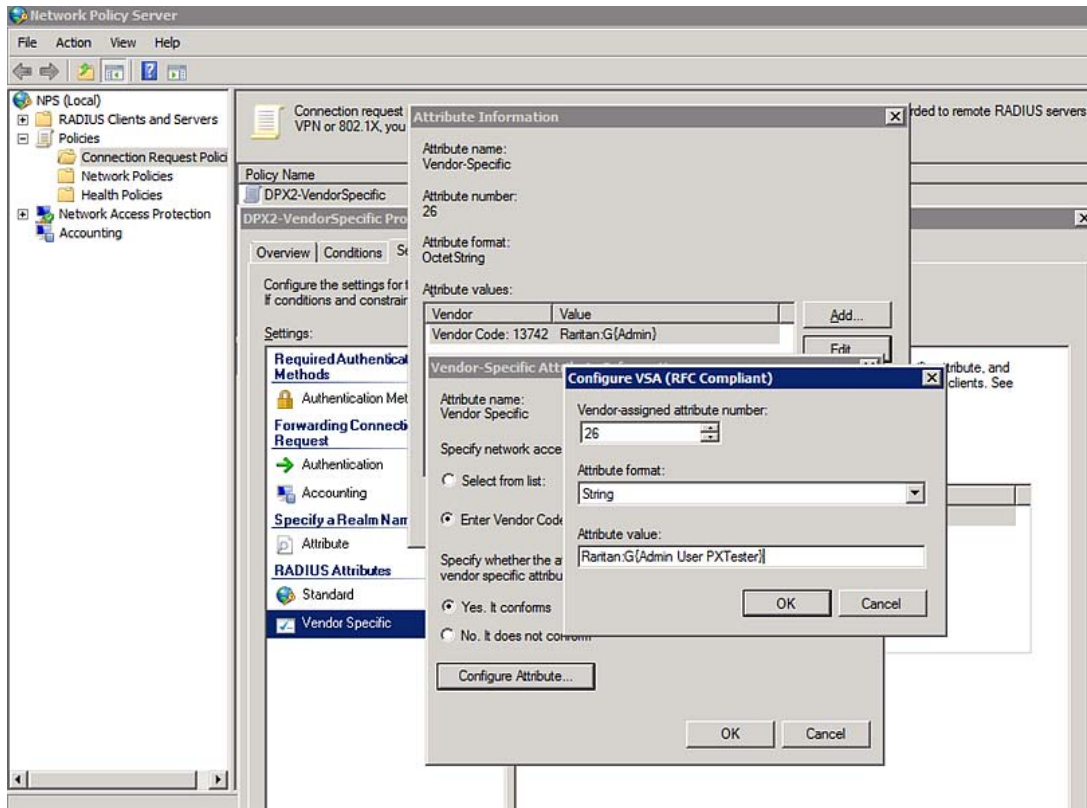


2. Select Connection Request Policies and double-click the policy where you want to add a custom VSA. The policy's properties dialog appears.
3. Click the Settings tab.
4. Select Vendor Specific, and click Add. The Add Vendor Specific Attribute dialog appears.
5. Select Custom in the Vendor field, and 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

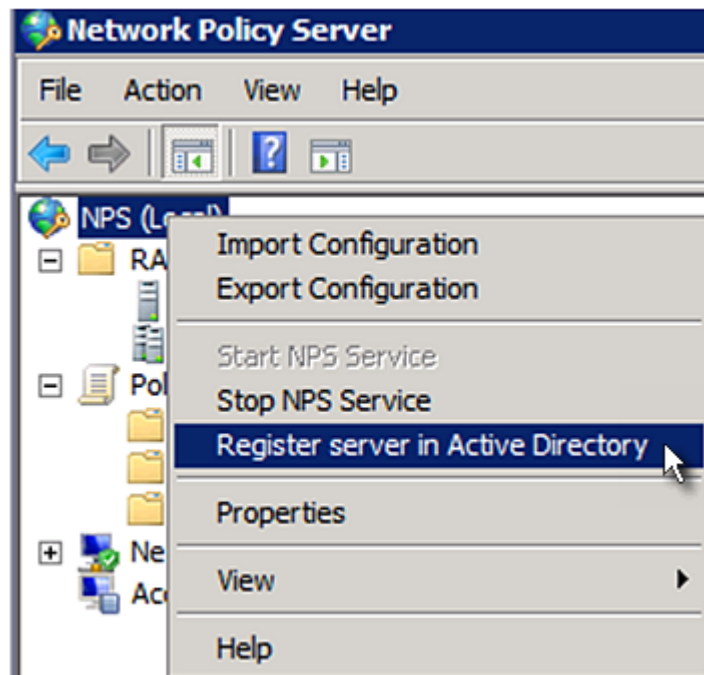
---

**Important: Reset the user password if the password is set before you enable the "Store password using reversible encryption" feature.**

---

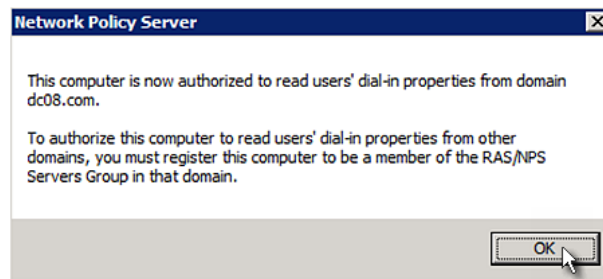
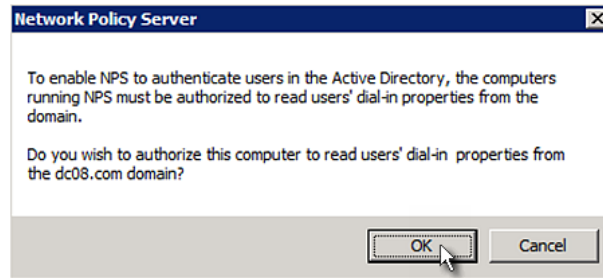
► **To register NPS:**

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 PXE 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.

The screenshot shows the 'Dial-in' tab of the 'Properties' dialog for a user. The 'Network Access Permission' section has three radio buttons: 'Allow access' (selected), 'Deny access', and 'Control access through NPS Network Policy'. Below this is a checkbox for 'Verify Caller-ID' with an empty text field. The 'Callback Options' section has three radio buttons: 'No Callback' (selected), 'Set by Caller (Routing and Remote Access Service only)', and 'Always Callback to:' with an empty text field. The 'Assign Static IP Addresses' section has a checkbox and a text field with a 'Static IP Addresses ...' button. The 'Apply Static Routes' section has a checkbox and a text field with a 'Static Routes ...' button. At the bottom are 'OK', 'Cancel', 'Apply', and 'Help' buttons.

► **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.

- Click the Account tab and select the "Store password using reversible encryption" checkbox.

The screenshot shows the 'Account' tab in the Windows NT User Manager console. The 'User logon name' is 'DC08\'. The 'User logon name (pre-Windows 2000)' is 'Administrator'. The 'Logon Hours...' and 'Log On To...' buttons are visible. The 'Unlock account' checkbox is unchecked. Under 'Account options', the 'Store password using reversible encryption' checkbox is checked. Under 'Account expires', the 'Never' radio button is selected.

## 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 428).

---

### Format of the "string"

The format of `string` in the dictionary file is:

```
Raritan:G{roles}
```

"roles" inside the curved brackets `{}` are role names, which comprise one or multiple roles to which the user belongs.

Multiple role names are separated with a space.

#### ► Example:

If the user has three roles -- *Admin*, *User* and *SystemTester*, then type:

```
Raritan:G{Admin User SystemTester}
```

Therefore, in Raritan's dictionary file, the attribute line is like the following:

```
ATTRIBUTE      Raritan-Vendor-Specific 26      Raritan:G{Admin User SystemTester}
```

# Appendix I Additional PXE Information

## In This Chapter

MAC Address .....	430
Locking Outlets and Cords .....	430
Unbalanced Current Calculation .....	433
PDView App for Viewing the PXE .....	434
Altitude Correction Factors .....	437
Raritan Training Website .....	437
Truncated Data in the Web Interface .....	438
Reserving IP Addresses in Windows DHCP Servers.....	438
Sensor Threshold Settings .....	440
Ways to Probe Existing User Profiles.....	447
Schroff LHX/SHX and USB Cascading Not Supported .....	448

---

## MAC Address

A label is affixed to the PXE, showing both the serial number and MAC address.



If necessary, you can find its IP address through the MAC address by using commonly-used network tools. Contact your LAN administrator for assistance.

---

## 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:

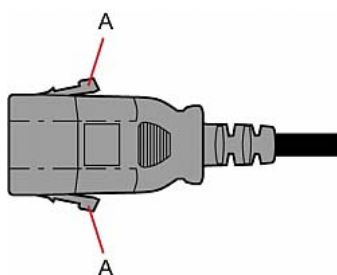
- SecureLock™ outlets and cords
- Button-type locking outlets

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.

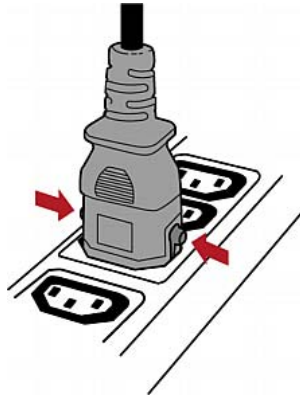
*Tip: The SecureLock™ outlets can accept regular power cords for power distribution but the SecureLock™ mechanism does not take effect.*

### ► 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.

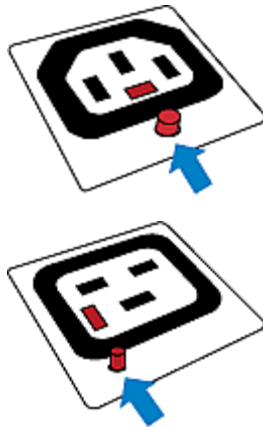
---

**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 PXE calculates the unbalanced current percentage.

### ► Calculation:

1. Calculate the average current of all 3 lines.

$$\text{Average current} = (L1 + L2 + L3) / 3$$

2. Calculate each line's current unbalance by having each line current subtracted and divided with the average current.

$$L1 \text{ current unbalance} = (L1 - \text{average current}) / \text{average current}$$

$$L2 \text{ current unbalance} = (L2 - \text{average current}) / \text{average current}$$

$$L3 \text{ current unbalance} = (L3 - \text{average current}) / \text{average current}$$

3. Determine the maximum absolute value among three lines' current unbalance values.

$$\text{Maximum} ( |L1 \text{ current unbalance}| , |L2 \text{ current unbalance}| , |L3 \text{ current unbalance}| )$$

4. Convert the maximum value to a percentage.

$$\text{Unbalanced load percent} = 100 * \text{maximum current unbalance}$$

### ► Example:

- Each line's current:

$$L1 = 5.5 \text{ amps}$$

$$L2 = 5.2 \text{ amps}$$

$$L3 = 4.0 \text{ amps}$$

- 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:  
 $100 * (0.1837) = 18\%$

---

## PDView App for Viewing the PXE

Raritan has developed an app that can turn your Android mobile device into a local display for the PXE.

This app is called PDView and it can be downloaded for free.

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

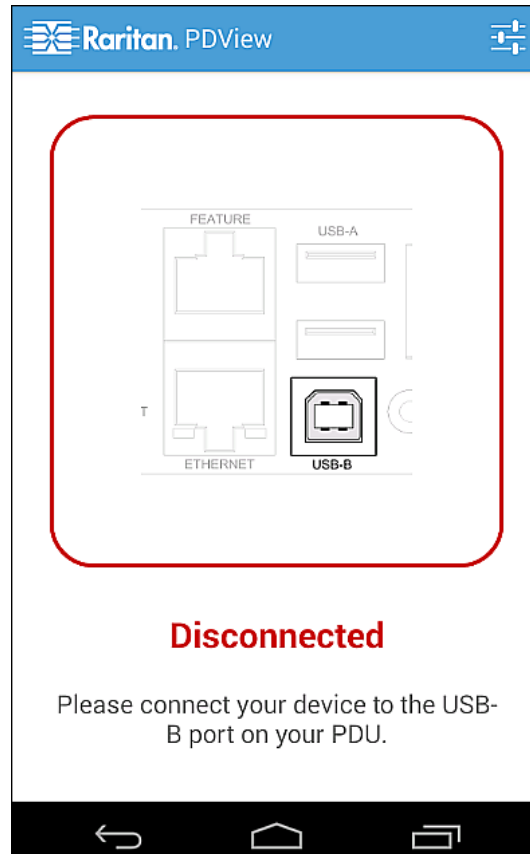
### ► Requirements for using PDView:

- The PXE is running firmware version 3.0.0 or later.
- The Android device must support USB "On-The-Go" (OTG).
- A USB OTG adapter cable is required.

### ► To install PDView:

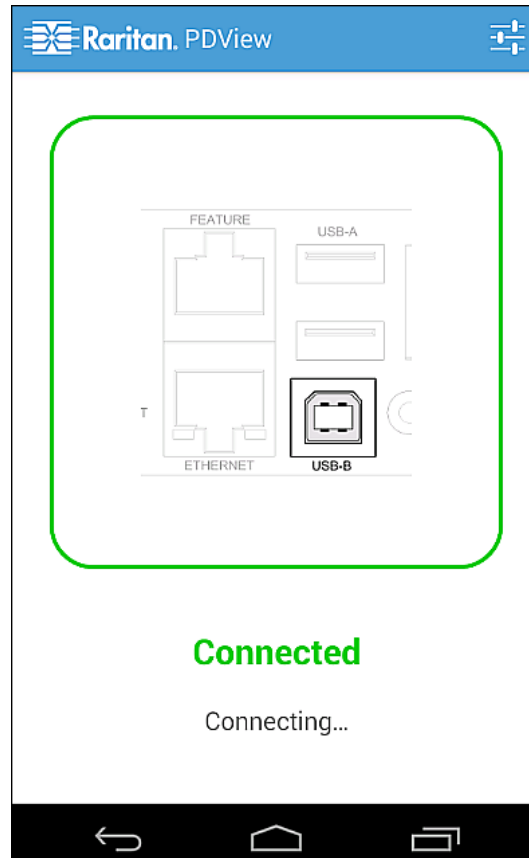
1. Use your mobile device to download the PDView app from the Google Play.

2. After installing the PDView, launch it. Below illustrates the PDView.



3. Connect your mobile device to the USB port of the PXE.

The PDView shows a "Connected" message when it detects the physical connection to the PXE.



4. Log in to the PDView app at the login prompt. Now you can view limited PXE 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 PXE.*

---

---

## 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

---

## 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.

---

## Truncated Data in the Web Interface

Some fields of the PXE 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

---

## Reserving IP Addresses in Windows DHCP Servers

The PXE uses its serial number as the client identifier in the DHCP request. Therefore, to successfully reserve an IP address for the PXE in a Windows® DHCP server, use the PXE device's serial number as the unique ID instead of the MAC address.

### ► IP address reservation procedure:

1. Convert the serial number of your PXE 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 PXE.

Field	Description
IP address	Enter the IP address you want to reserve.
MAC address	Enter the ASCII codes of the PXE serial number. Do NOT contain spaces in the ASCII codes. <ul style="list-style-type: none"><li>▪ In this example, enter 50454731413030303033</li></ul>
Other fields	Configure them according to your needs.

**New Reservation** ? X

Provide information for a reserved client.

Reservation name:

IP address:

MAC address:

Description:

Supported types

☒ Both

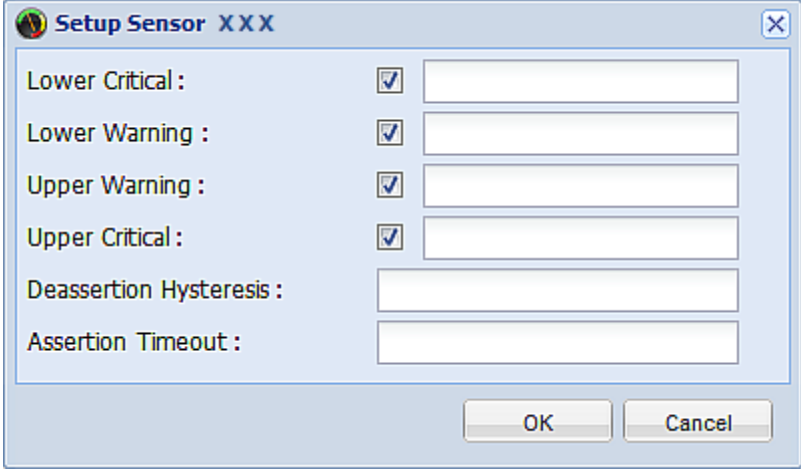
☐ DHCP only

☐ BOOTP only

---

## Sensor Threshold Settings

This section explains the thresholds settings in a threshold setup dialog for a numeric internal or external sensor.



The image shows a Windows-style dialog box titled "Setup Sensor XXX". It contains six rows of settings, each with a label, a checkbox, and a text input field. The first four rows have their checkboxes checked. The last two rows, "Deassertion Hysteresis" and "Assertion Timeout", do not have checkboxes. At the bottom right of the dialog are "OK" and "Cancel" buttons.

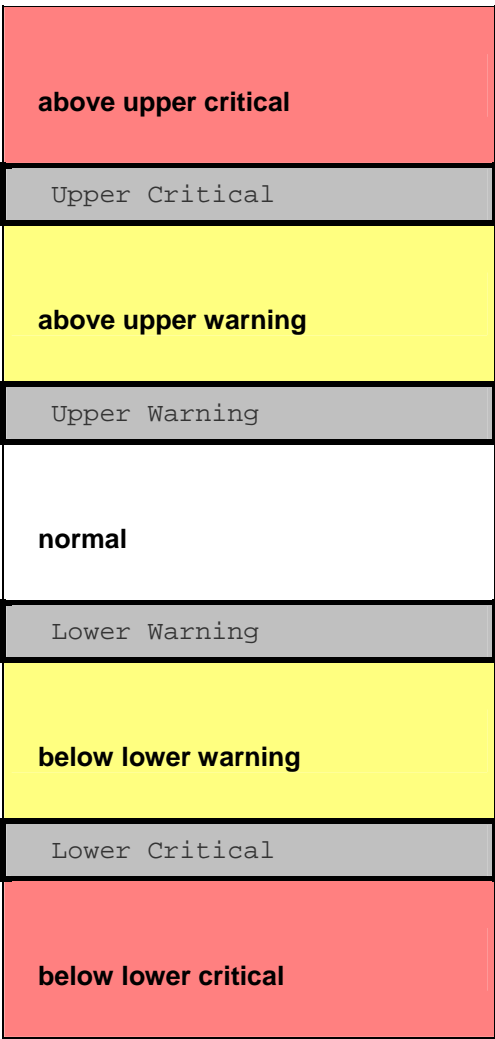
Setting	Checked	Value
Lower Critical :	<input checked="" type="checkbox"/>	
Lower Warning :	<input checked="" type="checkbox"/>	
Upper Warning :	<input checked="" type="checkbox"/>	
Upper Critical :	<input checked="" type="checkbox"/>	
Deassertion Hysteresis :		
Assertion Timeout :		



### Thresholds and Sensor States

A numeric sensor has four threshold settings: Lower Critical, Lower Warning, Upper Warning and Upper Critical.

The threshold settings determine how many sensor states are available for a certain sensor and the range of each sensor state. The diagram below shows how each threshold relates to each state.



#### ► Available sensor states:

The more thresholds are enabled for a sensor, the more sensor states are available for it. The "normal" state is always available regardless of whether any threshold is enabled.

For example:

- When a sensor only has the Upper Critical threshold enabled, it has two sensor states: normal and above upper critical.

- When a sensor has both the Upper Critical and Upper Warning thresholds enabled, it has three sensor states: normal, above upper warning, and above upper critical.

States of "above upper warning" and "below lower warning" are warning states to call for your attention.

States of "above upper critical" and "below lower critical" are critical states that require you to immediately handle.

► **Range of each available sensor state:**

The value of each enabled threshold determines the reading range of each available sensor state. For details, see:

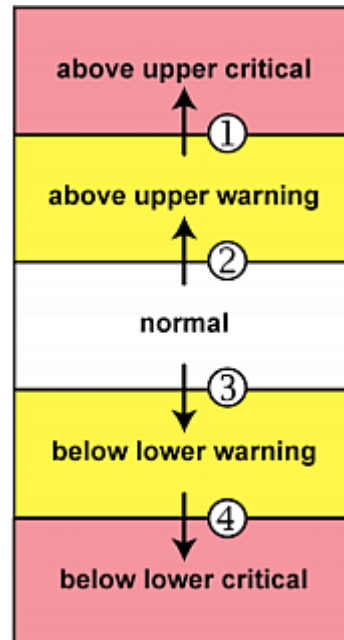
- **"above upper critical" State** (on page 193)
- **"above upper warning" State** (on page 192)
- **"below lower critical" State** (on page 192)
- **"below lower warning" State** (on page 192)

### "To Assert" and Assertion Timeout

If multiple sensor states are available for a specific sensor, the PXE 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 PXE 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 PXE turns on the "assertion" action. If that sensor changes its state again within the specified wait time, the PXE 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 PXE 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 PXE 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 PXE 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 PXE turns on the "assertion" action to announce the "above upper warning" state.
- If the temperature drops below 25 degrees Celsius within 5 seconds, the PXE does NOT turn on the "assertion" action.

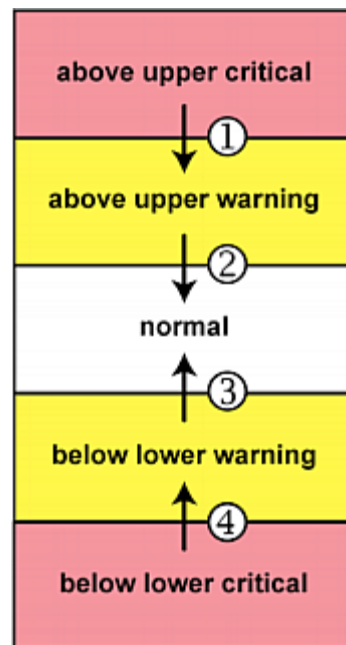
---

**"To De-assert" and Deassertion Hysteresis**

After the PXE 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 PXE to de-assert the previous state.



1. above upper critical --> above upper warning
2. above upper warning --> normal
3. below lower warning --> normal
4. below lower critical --> below lower warning

► **Deassertion Hysteresis:**

In the threshold settings dialog, the Deassertion Hysteresis field determines a new level to turn on the "deassertion" action.

Lower Critical :	<input checked="" type="checkbox"/>	
Lower Warning :	<input checked="" type="checkbox"/>	
Upper Warning :	<input checked="" type="checkbox"/>	
Upper Critical :	<input checked="" type="checkbox"/>	
Deassertion Hysteresis :		
Assertion Timeout :		

OK Cancel

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 PXE 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 PXE 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 PXE 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 PXE does NOT turn on the "deassertion" action.
- If the temperature drops to 17 degrees Celsius or lower, the PXE turns on the "deassertion" action to announce the end of the "above upper warning" state.

---

**Ways to Probe Existing User Profiles**

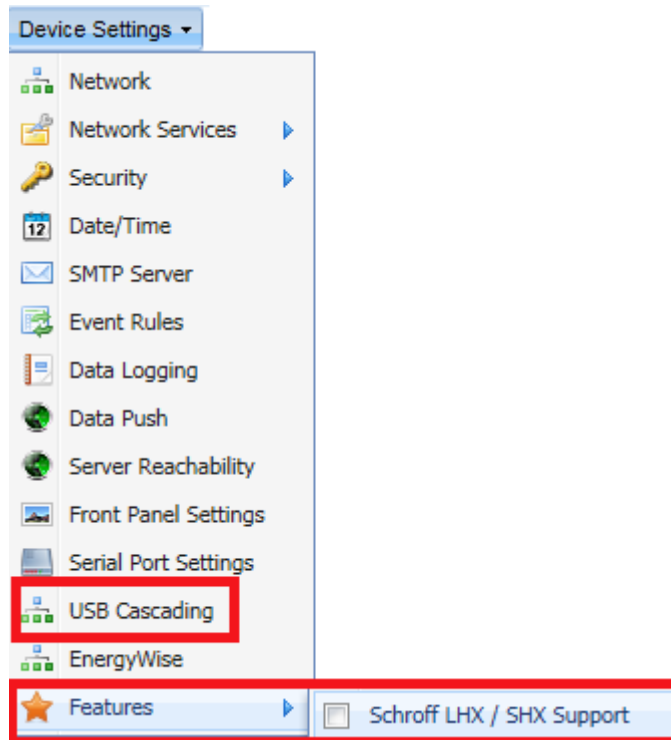
This section indicates available ways to query existing user accounts on the PXE.

- 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, which show a list of associated user names.

---

## Schroff LHX/SHX and USB Cascading Not Supported

Note that Schroff LHX/SHX and USB Cascading appear as supported options under the Device Settings menu, but they are not supported by the PXE.





## Appendix J Integration

The PXE device can work with certain Sunbird's products to provide diverse power solutions.

### In This Chapter

Power IQ Configuration .....	449
dcTrack.....	449

---

### 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.sunbirdcim.com>.

---

### dcTrack

Sunbird's dcTrack® is a product that allows you to manage the data center. The PXE is categorized as a power item in dcTrack. dcTrack offers an import wizard for conveniently adding the PXE 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.sunbirdcim.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.

# Index

## 1

1U Products • 1

## A

A Note about Enabling Thresholds • 218  
A Note about Firmware Upgrade Time • 203  
A Note about Infinite Loop • 168  
A Note about Untriggered Rules • 171  
About the Interface • 219  
Access Security Control • 98  
Accessing the Help • 204  
Action Group • 135, 137  
Actuator Configuration Commands • 316, 317, 330  
Actuator Control Operations • 338  
Actuator Information • 232  
Add Page Icon • 55, 58  
Adding a Firewall Rule • 277  
Adding a Monitored Device • 331  
Adding a Role-Based Access Control Rule • 290  
Adding Attributes to the Class • 400  
Adding Authentication Servers • 121  
Adding IT Devices for Ping Monitoring • 174  
Adding LDAP Server Settings • xv, 121  
Adding RADIUS Server Settings • 124, 405  
Additional PXE Information • 432  
AD-Related Configuration • 405, 426  
Alarm • 136, 138  
Alarms List • 64, 135, 138  
Alerted Sensors • 63  
All Privileges • xvi, 305, 311, 312, 315  
Altitude Correction Factors • 85, 250, 439  
APIPA and Link-Local Addressing • xv, 2, 12, 50, 80  
Assertion Timeout Example for Temperature Sensors • 446  
Automatic Mode • 44  
Automatically Completing a Command • 345  
Available SCP Commands • 386

## B

Backup and Restore of PXE Device Settings • 196, 199, 358  
Backup and Restore via SCP • 200, 388

Before You Begin • 10  
Browser-Defined Shortcut Menu • 62  
Browsing through the Online Help • 205  
Bulk Configuration • 20, 196, 199, 387  
Bulk Configuration Methods • xv, 12, 20  
Bulk Configuration or Firmware Upgrade via DHCP/TFTP • xvi, 20, 196, 203, 353  
Bulk Configuration via SCP • 197, 199, 387  
Bulk Configuration/Upgrade Procedure • 353, 363  
Button-Type Locking Outlets • 434

## C

Certificate Signing Request • 114  
Changing a User's Password • 299  
Changing Default Thresholds • 186, 187  
Changing HTTP(S) Settings • 75, 98  
Changing Measurement Units • 305, 308  
Changing Modbus/TCP Settings • 79  
Changing SSH Settings • 76, 93  
Changing Telnet Settings • 77  
Changing the Default Policy • 99, 109, 110  
Changing the Inlet Name • 296  
Changing the LAN Duplex Mode • 263  
Changing the LAN Interface Speed • 262  
Changing the Modbus Configuration • 269  
Changing the Modbus Port • 270  
Changing the Outlet Name • 295  
Changing the Overcurrent Protector Name • 297  
Changing the PDU Name • 249  
Changing the Role(s) • 305  
Changing the Sensor Description • 319  
Changing the Sensor Name • 317  
Changing the SSH Configuration • 266  
Changing the SSH Port • 266  
Changing the Telnet Configuration • 265  
Changing the Telnet Port • 266  
Changing the UDP Port • 336  
Changing Your Own Password • 307  
Changing Your Password • 52  
Checking Outlet-Specific Data • 128  
Checking Server Monitoring States • 177  
Checking the Accessibility of NTP Servers • 275  
Checking the Branch Circuit Rating • 11  
Circuit Breaker Orientation Limitation • 4, 6, 8  
Circuit Breakers • 46

- Clearing Event Entries • 172
  - Clearing Event Log • 247
  - Clearing Information • 247
  - Closing a Local Connection • 222
  - Collapsing the Tree • 57
  - Command History • 244
  - Commands for Environmental Sensors • 327
  - Commands for Inlet Pole Sensors • 325
  - Commands for Inlet Sensors • 323
  - Components of an Event Rule • 134
  - config.txt • 354, 357, 359
  - Configuration Files • 353, 354
  - Configuring Environmental Sensors' Default Thresholds • 321
  - Configuring Environmental Sensors or Actuators • 61, 178, 184, 187, 189
  - Configuring IP Protocol Settings • 253
  - Configuring IPv4 Parameters • 254
  - Configuring IPv6 Parameters • 258
  - Configuring SMTP Settings • 87, 140
  - Configuring SNMP Notifications • 167, 176, 210
  - Configuring SNMP Settings • 78, 91
  - Configuring the Firewall • 98
  - Configuring the PXE • xv, 11, 68
  - Configuring the PXE Device and Network • 248
  - Configuring Users for Encrypted SNMP v3 • 208, 209
  - Connecting a DPX2 Sensor Package to DPX3 • xv, 31, 40
  - Connecting a DPX2 Sensor Package to DX • 29, 34, 40
  - Connecting Environmental Sensor Packages • xv, 22, 178
  - Connecting the PDU to a Power Source • 11
  - Connecting the PXE to a Computer • xv, 2, 11, 14, 384
  - Connecting the PXE to Your Network • 12, 15
  - Connection Ports • 42
  - Controlling Actuators • 195
  - Copying the PXE Configuration • 198
  - Creating a Certificate Signing Request • 114
  - Creating a New Attribute • 399
  - Creating a Role • 93, 96, 311, 405
  - Creating a Self-Signed Certificate • 116
  - Creating a User Profile • 50, 77, 90, 94, 95, 96, 209, 298
  - Creating Actions • 64, 135, 153, 169
  - Creating an Event Rule • 135
  - Creating Configuration Files via Mass Deployment Utility • 355, 362
  - Creating Firewall Rules • 99, 100
  - Creating Role-Based Access Control Rules • 109, 110
  - Creating Rules • 147
  - Customizing the Date and Time • xvi, 274
- ## D
- Data Pane • 59
  - Date and Time Settings • 230
  - dcTrack • 451
  - dcTrack Overview • 452
  - Deassertion Hysteresis Example for Temperature Sensors • 448
  - Default Log Messages • xv, 108, 140, 157
  - Default Measurement Units • 230
  - Deleting a Firewall Rule • 281
  - Deleting a Monitored Device • 332
  - Deleting a Role • 98, 316
  - Deleting a Role-Based Access Control Rule • 293
  - Deleting a User Profile • 94, 307
  - Deleting an Event Rule or Action • 170
  - Deleting Authentication Server Settings • 126
  - Deleting Firewall Rules • 104
  - Deleting Ping Monitoring Settings • 177
  - Deleting Role-Based Access Control Rules • 113
  - Describing the Sensor's or Actuator's Location • 185, 187
  - Determining the SSH Authentication Method • xv, 267
  - Determining the Time Setup Method • 271, 274
  - Device Management • 65
  - devices.csv • 355, 357, 360, 361
  - DHCP IPv4 Configuration in Linux • 354, 380
  - DHCP IPv4 Configuration in Windows • 354, 363
  - DHCP IPv6 Configuration in Linux • 354, 382
  - DHCP IPv6 Configuration in Windows • 354, 373
  - Diagnostic Commands • 343
  - Dictionary File • 429
  - Different CLI Modes and Prompts • 221, 222, 224, 247, 248, 249, 275, 338, 343
  - Disabling an Inlet (for Multi-Inlet PDUs) • 131
  - Disabling External Authentication • 126

- Disabling the Automatic Management Function • 182, 194, 251
- Displaying PDU Information • 66, 128
- Downloading Diagnostic Information • xv, 201
- Downloading Key and Certificate Files • 118
- Downloading SNMP MIB • 78, 209, 210, 216
- DPX Sensor Packages • xv, 22
- DPX2 Sensor Packages • 22, 28
- DPX3 Sensor Packages • xv, 22, 30
- DX Sensor Packages • 22, 33, 146

## E

- Editing Authentication Server Settings • 126
- Editing Firewall Rules • 103
- Editing Ping Monitoring Settings • 176
- Editing rcusergroup Attributes for User Members • 402
- Editing Role-Based Access Control Rules • 112
- Email and SMS Message Placeholders • xv, 140, 141, 146, 164
- Enabling and Editing the Security Banner • 108
- Enabling Data Logging • 86
- Enabling External and Local Authentication Services • 127
- Enabling IPv4 or IPv6 • 253
- Enabling Login Limitations • 106
- Enabling or Disabling a User Profile • 301
- Enabling or Disabling an Inlet (for Multi-Inlet PDUs) • 296
- Enabling or Disabling Data Logging • 249
- Enabling or Disabling EnergyWise • 335
- Enabling or Disabling Modbus • 269
- Enabling or Disabling Peripheral Device Auto Management • xv, 251
- Enabling or Disabling SNMP v1/v2c • 267
- Enabling or Disabling SNMP v3 • 268
- Enabling or Disabling SSH • 266
- Enabling or Disabling Strong Passwords • 286
- Enabling or Disabling Telnet • 265
- Enabling or Disabling the Read-Only Mode • 270
- Enabling or Disabling the Restricted Service Agreement • 282
- Enabling or Disabling the Service Advertisement • 270
- Enabling Password Aging • 107
- Enabling Service Advertisement • 80, 270
- Enabling SNMP • 78, 86, 208
- Enabling Strong Passwords • 107
- Enabling the Feature • 109
- Enabling the Firewall • 98, 99
- Enabling User Blocking • 105
- EnergyWise Configuration Commands • 335
- EnergyWise Settings • 241
- Entering Configuration Mode • 222, 248, 299, 307, 308
- Entering Diagnostic Mode • 222, 342
- Environmental Sensor Configuration Commands • 316
- Environmental Sensor Default Thresholds • 238
- Environmental Sensor Information • 231
- Environmental Sensor Package Information • 233
- Environmental Sensor Threshold Information • 237
- Environmental Sensors and Actuators • 178
- Equipment Setup Worksheet • 11, 349
- Event Log • 242
- Event Rules and Actions • 78, 87, 132, 134, 174, 210
- Example • 273, 283, 299, 307, 308
  - Ping Monitoring and SNMP Notifications • 175
- Example - Actuator Naming • 331
- Example - Creating a Role • 316
- Example - Default Upper Thresholds for Temperature • 323
- Example - Inlet Naming • 297
- Example - OCP Naming • 297
- Example - Outlet Naming • 295
- Example - Ping Command • 345
- Example - Server Settings Changed • 334
- Example - Setting Up EnergyWise • 337
- Example - Turning On a Specific Actuator • 340
- Example 1 • 168
- Example 1 - Basic Security Information • 245
- Example 1 - Combination of IP, Subnet Mask and Gateway Parameters • 337
- Example 1 - Creating a User Profile • 310
- Example 1 - Environmental Sensor Naming • 321
- Example 1 - IPv4 Firewall Control Configuration • 293
- Example 1 - Networking Mode • 271
- Example 1 - PDU Naming • 252
- Example 1 - Time Setup Method • 275
- Example 1 - Upper Critical Threshold for a Temperature Sensor • 329
- Example 2 • 168

Example 2 - Adding an IPv4 Firewall Rule • 294  
 Example 2 - Combination of Upper Critical and Upper Warning Settings • 338  
 Example 2 - Data Logging Enabled • 252  
 Example 2 - Enabling Both IP Protocols • 271  
 Example 2 - In-Depth Security Information • 246  
 Example 2 - Modifying a User's Roles • 310  
 Example 2 - Primary NTP Server • 275  
 Example 2 - Sensor Threshold Selection • 321  
 Example 2 - Warning Thresholds for Inlet Sensors • 328  
 Example 3 - Basic PDU Information • 246  
 Example 3 - Default Measurement Units • 310  
 Example 3 - Static IPv4 Configuration • 271  
 Example 3 - User Blocking • 294  
 Example 4 - Adding an IPv4 Role-based Access Control Rule • 295  
 Example 4 - In-Depth PDU Information • 247  
 Examples • 245, 252, 271, 275, 293, 309, 320, 328  
 Existing Roles • 241  
 Existing User Profiles • 230, 240  
 Expanding the Tree • 55, 56, 128, 130

## F

Filling Out the Equipment Setup Worksheet • 11  
 Firewall Control • 276  
 Firmware Update via SCP • 203, 386  
 Firmware Update via Web Interface • 202, 386  
 Firmware Upgrade • 198, 202  
 Forcing a Password Change • 301  
 Forcing HTTPS Encryption • 98, 114  
 Format of the • 430  
 From LDAP/LDAPS • 398  
 From Microsoft Active Directory • 398  
 Full Disaster Recovery • 204  
 fwupdate.cfg • 354, 356, 359, 361

## G

Gathering the External Authentication Information • 119  
 Gathering the LDAP Information • 120  
 Gathering the RADIUS Information • 120

## H

Help Command • 223  
 History Buffer Length • 244  
 How to Use the Calendar • 82

## I

Identifying Environmental Sensors and Actuators • 178, 179, 183  
 Identifying Sensor or Actuator Channels • 182  
 Idle Timeout • 285  
 Initial Network Configuration via CLI • 3, 12, 15, 16, 57, 384  
 Inlet and Overcurrent Protector Management • 128  
 Inlet Configuration Commands • 295  
 Inlet Information • 228  
 Inlet Pole Sensor Threshold Information • 235  
 Inlet Sensor Threshold Information • 234  
 Installation and Configuration • 10  
 Installing a CA-Signed Certificate • 116  
 Installing Cable Retention Clips on Outlets (Optional) • 20  
 Installing Existing Key and Certificate Files • 118  
 Installing the USB-to-Serial Driver (Optional) • 13, 14  
 Integration • 451  
 Internal Beeper State • 89  
 Introduction • 1  
 Introduction to the Web Interface • 54  
 IP Configuration • 225

## L

LAN Interface Settings • 225  
 Layout • 217  
 LDAP Configuration Illustration • 125, 390  
 LED Display • 43  
 LEDs for Measurement Units • 44, 45  
 Listing TCP Connections • 201  
 Locking Outlets and Cords • 21, 432  
 Log an Event Message • 136, 139  
 Logging in to CLI • 220, 384  
 Logging in to the Web Interface • 50  
 Logging out of CLI • 222  
 Login • xv, 12, 15, 50, 91  
 Login Limitation • 283  
 Logout • 53



Lowercase Character Requirement • 287

## M

MAC Address • 12, 432  
 Managing Environmental Sensors or Actuators  
   • 33, 178, 182  
 Managing Event Logging • 171  
 Managing Firewall Rules • 277  
 Managing Role-Based Access Control Rules •  
   290  
 Manual Mode • 45  
 Matching the Position • xv, 179, 180  
 Matching the Serial Number • 179  
 Maximum Ambient Operating Temperature •  
   11, 347  
 Maximum Password History • 288  
 Maximum Password Length • 286  
 Menus • 55  
 Microsoft Network Policy Server • 405  
 Minimum Password Length • 286  
 Mixing Diverse Sensor Types • xv, 35, 37  
 Modifying a Firewall Rule • 279  
 Modifying a Monitored Device's Settings • 332  
 Modifying a Role • 93, 94, 96, 314  
 Modifying a Role-Based Access Control Rule •  
   291  
 Modifying a User Profile • 52, 94, 96, 298  
 Modifying a User's Personal Data • 300  
 Modifying an Action • 79, 170  
 Modifying an Event Rule • 168  
 Modifying Firewall Control Parameters • 276  
 Modifying IPv4 Settings • 69  
 Modifying IPv6 Settings • 71  
 Modifying Network Service Settings • 75, 219,  
   221  
 Modifying Network Settings • 57, 68, 80, 392  
 Modifying Role-Based Access Control  
   Parameters • 289  
 Modifying SNMPv3 Settings • 302  
 Modifying the Network Configuration • 16, 67  
 Modifying the Network Interface Settings • 68  
 Monitoring Server Accessibility • 173  
 Monitoring the Inlet • 129  
 More Information • 59  
 More Information about AD or RADIUS  
   Configuration • 125  
 Mounting 1U Models Using L-Brackets and  
   Buttons • 5  
 Mounting Zero U Models Using L-Brackets  
   and Buttons • 8

Mounting Zero U Models Using Two Rear  
 Buttons • 6  
 Multi-Command Syntax • 277, 283, 285, 286,  
   289, 298, 300, 302, 305, 308, 321, 323, 325,  
   327, 330, 332, 337

## N

Naming Outlets • 127  
 Naming Overcurrent Protectors • 130  
 Naming the Inlet • 129  
 Naming the PDU • 55, 57, 67, 85, 89, 186, 194  
 Network Configuration • 225  
 Network Configuration Commands • 252  
 Network Diagnostics • 200  
 Network Service Settings • 226  
 Network Troubleshooting • 200, 342  
 Networking Mode • 226  
 Non-Windows RADIUS Server • 405, 429  
 Numeric Character Requirement • 287

## O

Outlet Configuration Commands • 295  
 Outlet Information • 227  
 Outlet Management • 127  
 Outlets • 41  
 Overcurrent Protector Configuration  
   Commands • 297  
 Overcurrent Protector Information • 229  
 Overriding DHCP-Assigned NTP Servers •  
   272, 275  
 Overriding the IPv4 DHCP-Assigned DNS  
   Server • 256, 257  
 Overriding the IPv6 DHCP-Assigned DNS  
   Server • 260, 261

## P

Package Contents • 1, 10  
 Panel Components • 41  
 Password Aging • 284  
 Password Aging Interval • 284  
 PDU Configuration • 227  
 PDU Configuration Commands • 249  
 PDView App for Viewing the PXE • xvi, 436  
 Pinging a Host • 200  
 Power Cord • 41  
 Power IQ Configuration • 451  
 Preparing the Installation Site • 10  
 Product Models • 1  
 PX Explorer Pane • 55

## Q

Querying Available Parameters for a Command • 223, 224  
 Querying DNS Servers • 343  
 Quitting Configuration Mode • 248, 283  
 Quitting Diagnostic Mode • 342

## R

Rackmount Safety Guidelines • 4  
 Rack-Mounting the PDU • 4  
 RADIUS Configuration Illustration • 125, 405  
 Raritan Training Website • 439  
 Rebooting the PXE Device • 88  
 Reliability Data • 244  
 Reliability Error Log • 245  
 Remembering User Names and Passwords • 53  
 Reserving IP Addresses in Windows DHCP Servers • 440  
 Reset Button • 46  
 Resetting Active Energy Readings • 341  
 Resetting All Active Energy Readings • 89, 131  
 Resetting Inlet Active Energy Readings • 89, 130  
 Resetting the Button-Type Circuit Breaker • 46  
 Resetting the Handle-Type Circuit Breaker • 47  
 Resetting the PXE • 340  
 Resetting to Factory Defaults • 342, 384  
 Restarting the PDU • 341  
 Restricted Service Agreement • 281  
 Retrieving Previous Commands • 345  
 Retrieving Software Packages Information • 205  
 Returning User Group Information • 398  
 Role Configuration Commands • 311  
 Role of a DNS Server • 75, 392  
 Role-Based Access Control • 288  
 RS-485 Port Pinouts • 347

## S

Safety Guidelines • ii  
 Safety Instructions • iii, 11  
 Sample Event Rules • 166  
 Sample Inlet-Level Event Rule • 167  
 Sample PDU-Level Event Rule • 166

Saving the PXE Configuration • 197, 358  
 Scheduling an Action • 152, 157  
 Schroff LHX/SHX and USB Cascading Not Supported • xvi, 450  
 SecureLock™ Outlets and Cords • 433  
 Security Configuration Commands • 276  
 Security Settings • 239  
 Selecting IPv4 or IPv6 Addresses • 254  
 Selecting the Internet Protocol • 2, 69, 71  
 Send an SNMP Notification • 136, 141  
 Send EMail • 136, 140, 155, 157  
 Send Sensor Report • 136, 145, 156  
 Send Sensor Report Example • xv, 154  
 Sensor RJ-12 Port Pinouts • 347  
 Sensor Threshold Configuration Commands • 323  
 Sensor Threshold Settings • 132, 185, 442  
 Server Reachability Configuration Commands • 331  
 Server Reachability Information • 243  
 Server Reachability Information for a Specific Server • 243  
 Setting Data Logging • 86, 249, 250  
 Setting Data Logging Measurements Per Entry • 250  
 Setting Default Measurement Units • 85, 95, 305, 308  
 Setting Inlet Thresholds • 132  
 Setting IPv4 Static Routes • 257  
 Setting IPv6 Static Routes • 261  
 Setting LAN Interface Parameters • 262  
 Setting Network Service Parameters • 263  
 Setting NTP Parameters • 272, 275  
 Setting Power Thresholds • 61, 128, 132, 217  
 Setting the Alarmed to Normal Delay for DX-PIR • 320  
 Setting the Automatic Daylight Savings Time • 274  
 Setting the Date and Time • 81  
 Setting the EnergyWise Configuration • 89  
 Setting the History Buffer Length • 337  
 Setting the HTTP Port • 264  
 Setting the HTTPS Port • 265  
 Setting the IPv4 Address • 255  
 Setting the IPv4 Configuration Mode • 254  
 Setting the IPv4 Gateway • 256  
 Setting the IPv4 Preferred Host Name • 255  
 Setting the IPv4 Primary DNS Server • 256  
 Setting the IPv4 Secondary DNS Server • 256  
 Setting the IPv4 Subnet Mask • 255  
 Setting the IPv6 Address • 259



- Setting the IPv6 Configuration Mode • 258
  - Setting the IPv6 Gateway • 259
  - Setting the IPv6 Preferred Host Name • 259
  - Setting the IPv6 Primary DNS Server • 260
  - Setting the IPv6 Secondary DNS Server • 260
  - Setting the Networking Mode • 252
  - Setting the Polling Interval • 336
  - Setting the Registry to Permit Write
    - Operations to the Schema • 399
  - Setting the SNMP Configuration • 267
  - Setting the SNMP Read Community • 268
  - Setting the SNMP Write Community • 268
  - Setting the sysContact Value • 268
  - Setting the sysLocation Value • 269
  - Setting the sysName Value • 269
  - Setting the Time Zone • 273
  - Setting the X Coordinate • 318
  - Setting the Y Coordinate • 318
  - Setting the Z Coordinate • 251, 319
  - Setting the Z Coordinate Format • 185, 186
  - Setting the Z Coordinate Format for
    - Environmental Sensors • 251, 319, 331
  - Setting Thresholds for Multiple Sensors • 186, 188
  - Setting Up a TLS Certificate • 98, 113
  - Setting Up External Authentication • 75, 98, 119
  - Setting Up Role-Based Access Control Rules • 109
  - Setting Up Roles • 52, 90, 93, 95
  - Setting Up User Login Controls • 105
  - Setting Up Your Preferred Measurement Units
    - 85, 93, 95
  - Setup Button • 57
  - Showing Information • 224
  - Showing Network Connections • 343
  - Single Login Limitation • 284
  - SNMP Gets and Sets • 215
  - SNMP Sets and Thresholds • 217
  - SNMPv2c Notifications • 79, 211
  - SNMPv3 Notifications • 79, 213
  - Sorting Firewall Rules • 104
  - Sorting Role-Based Access Control Rules • 112
  - Sorting the Access Order • 125
  - Special Character Requirement • 288
  - Specifications • 4, 347
  - Specifying the Agreement Contents • 282
  - Specifying the CC Sensor Type • 317
  - Specifying the Device Altitude • 85, 250
  - Specifying the EnergyWise Domain • 335
  - Specifying the EnergyWise Secret • 336
  - Specifying the Primary NTP Server • 272
  - Specifying the Secondary NTP Server • 272
  - Specifying the SSH Public Key • 267, 306
  - States of Managed Actuators • 193
  - States of Managed Sensors • 190
  - States of Unmanaged Sensors or Actuators •
    - xv, 193, 194
  - Static Route Examples • 70, 71, 73
  - Status Bar • 57
  - Step A
    - Add Your PXE as a RADIUS Client • 406
  - Step A. Determine User Accounts and Roles • 390
  - Step B
    - Configure Connection Request Policies • 409
  - Step B. Configure User Groups on the AD Server • 391
  - Step C
    - Configure a Vendor-Specific Attribute • 424
  - Step C. Configure LDAP Authentication on the PXE Device • 392
  - Step D. Configure Roles on the PXE Device • 394
  - Strong Passwords • 286
  - Supported Maximum DPX Sensor Distances • 23, 27
  - Supported Web Browsers • xv, 49
  - Switch Peripheral Actuator • 136, 146
  - Switching Off an Actuator • 339
  - Switching On an Actuator • 339
  - Syslog Message • 136, 143
- ## T
- Testing the Network Connectivity • 344
  - Testing the Server Connection • 125
  - TFTP Requirements • 354, 363
  - The PXE MIB • 216
  - The Yellow- or Red-Highlighted Sensors • 60, 63, 64, 129, 132, 189
  - Three-Digit Row • 43
  - Thresholds and Sensor States • 443
  - Time Configuration Commands • 271
  - Tracing the Network Route • 201
  - Tracing the Route • 345
  - Truncated Data in the Web Interface • 440
  - Two-Digit Row • 44
- ## U
- Unbalanced Current Calculation • 435

## Index

- Unblocking a User • 105, 340
- Unmanaging Environmental Sensors or Actuators • xv, 33, 184, 193
- Unpacking the Product and Components • 10
- Updating the LDAP Schema • xvi, 398
- Updating the PXE Firmware • 202
- Updating the Schema Cache • 402
- Uppercase Character Requirement • 287
- User Blocking • 285
- User Configuration Commands • 297
- User Management • 90
- Using an Optional DPX3-ENVHUB4 Sensor Hub • xv, 35
- Using an Optional DPX-ENVHUB2 cable • 25
- Using an Optional DPX-ENVHUB4 Sensor Hub • 24
- Using Default Thresholds • 320
- Using SNMP • 203, 207
- Using the CLI Command • 342, 384
- Using the Command Line Interface • 75, 187, 219, 384
- Using the PDU • 41
- Using the Web Interface • 49

## V

- Viewing Connected Users • 172
- Viewing Firmware Update History • 204
- Viewing Sensor or Actuator Data • 189
- Viewing the Dashboard • 63
- Viewing the Local Event Log • 87, 121, 143, 171

## W

- Warning Icon • 59
- Ways to Probe Existing User Profiles • xvi, 449
- What's New in the PXE User Guide • xv
- Windows NTP Server Synchronization Solution • 82, 84
- With HyperTerminal • 220, 340
- With SSH or Telnet • 221

## Z

- Zero U Products • 1

## ► 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