Raritan PXE

User Guide

Xerus™ Firmware v3.3.10

Copyright © 2017 Raritan, Inc.
PXE-1A-v3.3.10-E
March 2017
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 2017 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.

1F61
I.T.E.

Warning

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

CAUTION:

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

SecureLock™

Contents

Safety Guidelines ii

Safety Instructions iii

What's New in the PXE User Guide xiv

Chapter 1 Introduction 1

Product Models 1
Package Contents 1
Zero U Products 1
1U Products 1
APIPA and Link-Local Addressing 2
Before You Begin 3
Unpacking the Product and Components 3
Preparing the Installation Site 3
Filling Out the Equipment Setup Worksheet 4
Checking the Branch Circuit Rating 4

Chapter 2 Rack-Mounting the PDU 5

Rackmount Safety Guidelines 5
Circuit Breaker Orientation Limitation 5
Mounting 1U Models Using L-Brackets and Buttons 6
Mounting Zero U Models Using Two Rear Buttons 7
Mounting Zero U Models Using L-Brackets and Buttons 9

Chapter 3 Initial Installation and Configuration 11

Connecting the PDU to a Power Source 11
Connecting the PXE to Your Network 11
Configuring the PXE 12
Installing the USB-to-Serial Driver (Optional) 13
Connecting the PXE to a Computer 14
Initial Network Configuration via CLI 15

Bulk Configuration Methods 18
Installing Cable Retention Clips on Outlets (Optional) 18

Chapter 4 Connecting Environmental Sensor Packages 20

DPX Sensor Packages 21
Using an Optional DPX-ENVHUB4 Sensor Hub 22
Using an Optional DPX-ENVHUB2 cable 24
Supported Maximum DPX Sensor Distances 26
DPX2 Sensor Packages 27
DPX3 Sensor Packages 29
Connecting a DPX2 Sensor Package to DPX3 30
DX Sensor Packages 31
Connecting a DPX2 Sensor Package to DX 33
Using an Optional DPX3-ENVHUB4 Sensor Hub 34
Mixing Diverse Sensor Types 36

Chapter 5 Using the PDU 40

Panel Components 40
Power Cord 40
Outlets 40
Connection Ports 41
LED Display 42
Reset Button 45
Circuit Breakers 45
Resetting the Button-Type Circuit Breaker 45
Resetting the Handle-Type Circuit Breaker 46

Chapter 6 Using the Web Interface 48

Supported Web Browsers 48
Login, Logout and Password Change 48
Login 49
Changing Your Password 50
Remembering User Names and Passwords 50
Logout 51
Web Interface Overview 51
Menu 53
Quick Access to a Specific Page 55
Sorting a List 55
Dashboard 56
Dashboard - Inlet I1 58
Dashboard - Alerted Sensors 60

Dashboard - Inlet History ... 62
Dashboard - Alarms ... 63
PDU ... 65
Internal Beeper State ... 66
Z Coordinate Format ... 67
How the Automatic Management Function Works ... 67
Inlet ... 68
Outlets ... 70
Available Data of the Outlets Overview Page ... 71
Individual Outlet Pages ... 71
OCPs ... 73
Individual OCP Pages ... 74
Peripherals ... 76
Yellow- or Red-Highlighted Sensors ... 81
Managed vs Unmanaged Sensors/Actuators ... 82
Sensor/Actuator States ... 83
Finding the Sensor's Serial Number ... 85
Identifying the Sensor Position and Channel ... 86
Managing One Sensor or Actuator ... 87
Individual Sensor/Actuator Pages ... 89
Sensor/Actuator Location Example ... 93
User Management ... 94
Creating Users ... 94
Editing or Deleting Users ... 98
Creating Roles ... 99
Editing or Deleting Roles ... 101
Setting Your Preferred Measurement Units ... 102
Setting Default Measurement Units ... 102
Device Settings ... 103
Configuring Network Settings ... 104
Configuring Network Services ... 114
Configuring Security Settings ... 121
Setting the Date and Time ... 143
Event Rules and Actions ... 146
Setting Data Logging ... 180
Configuring Data Push Settings ... 181
Monitoring Server Accessibility ... 183
Lua Scripts ... 187
Miscellaneous ... 192
Maintenance ... 193
Device Information ... 194
Viewing Connected Users ... 195
Viewing or Clearing the Local Event Log ... 196
Updating the PXE Firmware ... 197
Viewing Firmware Update History ... 199
Bulk Configuration ... 199

Backup and Restore of Device Settings ... 202
Network Diagnostics ... 203
Downloading Diagnostic Information ... 204
Rebooting the PXE Device ... 205
Resetting All Settings to Factory Defaults ... 205
Retrieving Software Packages Information ... 206

Chapter 7 Using SNMP 207

Enabling and Configuring SNMP ... 207
SNMPv2c Notifications ... 208
SNMPv3 Notifications ... 209
Downloading SNMP MIB ... 210
SNMP Gets and Sets ... 211
The PXE MIB ... 211
A Note about Enabling Thresholds ... 214

Chapter 8 Using the Command Line Interface 215

About the Interface ... 215
Logging in to CLI ... 216
With HyperTerminal ... 216
With SSH or Telnet ... 217
Different CLI Modes and Prompts ... 218
Closing a Local Connection ... 218
Logging out of CLI ... 218
Help Command ... 219
Querying Available Parameters for a Command ... 220
Showing Information ... 220
Network Configuration ... 221
PDU Configuration ... 225
Outlet Information ... 225
Inlet Information ... 226
Overcurrent Protector Information ... 227
Date and Time Settings ... 228
Default Measurement Units ... 228
Environmental Sensor Information ... 229
Actuator Information ... 230
Environmental Sensor Package Information ... 231
Inlet Sensor Threshold Information ... 232
Inlet Pole Sensor Threshold Information ... 233
Environmental Sensor Threshold Information ... 235
Environmental Sensor Default Thresholds ... 236
Security Settings ... 237
Existing User Profiles ... 238

Existing Roles ... 239
EnergyWise Settings ... 239
Event Log ... 240
Server Reachability Information ... 241
Command History ... 242
History Buffer Length ... 242
Reliability Data ... 242
Reliability Error Log ... 243
Examples ... 243
Clearing Information ... 245
Clearing Event Log ... 245
Configuring the PXE Device and Network ... 246
Entering Configuration Mode ... 246
Quitting Configuration Mode ... 246
PDU Configuration Commands ... 247
Network Configuration Commands ... 250
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 ... 313
Configuring Environmental Sensors' Default Thresholds ... 318
Sensor Threshold Configuration Commands ... 320
Actuator Configuration Commands ... 327
Server Reachability Configuration Commands ... 328
EnergyWise Configuration Commands ... 332
Setting the History Buffer Length ... 334
Multi-Command Syntax ... 334
Actuator Control Operations ... 335
Switching On an Actuator ... 336
Switching Off an Actuator ... 336
Example - Turning On a Specific Actuator ... 337
Unblocking a User ... 337
Resetting the PXE ... 337
Restarting the PDU ... 338
Resetting Active Energy Readings ... 338
Resetting to Factory Defaults ... 339
Network Troubleshooting ... 339
Entering Diagnostic Mode ... 339
Quitting Diagnostic Mode ... 339
Diagnostic Commands ... 340

Retrieving Previous Commands 342
Automatically Completing a Command 342

Chapter 9 Using SCP Commands 344

Firmware Update via SCP 344
Bulk Configuration via SCP 345
Backup and Restore via SCP 346
Downloading Diagnostic Data via SCP 347

Appendix A Specifications 349

Maximum Ambient Operating Temperature 349
Sensor RJ-12 Port Pinouts 349
RS-485 Port Pinouts 349

Appendix B Equipment Setup Worksheet 351

Appendix C Bulk Configuration or Firmware Upgrade via DHCP/TFTP 355

Bulk Configuration/Upgrade Procedure 355
Configuration Files 356
fwupdate.cfg 358
config.txt 362
devices.csv 364
Creating Configuration Files via Mass Deployment Utility 365
Data Encryption in 'config.txt' 366

TFTP Requirements 367
DHCP IPv4 Configuration in Windows 368
DHCP IPv6 Configuration in Windows 378
DHCP IPv4 Configuration in Linux 385
DHCP IPv6 Configuration in Linux 387

Appendix D Resetting to Factory Defaults 389

Using the CLI Command 389

Appendix E LDAP Configuration Illustration 391

Step A. Determine User Accounts and Roles 391
Step B. Configure User Groups on the AD Server 392
Step C. Configure LDAP Authentication on the PXE Device 393
Step D. Configure Roles on the PXE Device 394

Appendix F Updating the LDAP Schema 397

Returning User Group Information 397
From LDAP/LDAPS 397
From Microsoft Active Directory 397
Setting the Registry to Permit Write Operations to the Schema 398
Creating a New Attribute 398
Adding Attributes to the Class 399
Updating the Schema Cache 401
Editing rciusergroup Attributes for User Members 401

Appendix G RADIUS Configuration Illustration 404

Standard Attributes 404
NPS Standard Attribute Illustration 404
FreeRADIUS Standard Attribute Illustration 422
Vendor-Specific Attributes 423
NPS VSA Illustration 423
FreeRADIUS VSA Illustration 435
AD-Related Configuration 436

Appendix H Additional PXE Information 440

Locking Outlets and Cords 440
SecureLock™ Outlets and Cords 440
Button-Type Locking Outlets 442

MAC Address 442
Reserving IP Addresses in DHCP Servers 443
Reserving IP in Windows 443
Reserving IP in Linux 444
Sensor Threshold Settings 446
Thresholds and Sensor States 446
"To Assert" and Assertion Timeout 449
"To De-assert" and Deassertion Hysteresis 451
PDView App for Viewing the PXE 453
Altitude Correction Factors 455
Unbalanced Current Calculation 456
Ways to Probe Existing User Profiles 457
Raritan Training Website 458
Browsing through the Online Help 458

Appendix I Integration 460

Power IQ Configuration 460
dcTrack 460
dcTrack Overview 461

Index 463

What's New in the PXE User Guide

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.

Initial Network Configuration via CLI (on page 15)

The whole chapter of *Using the Web Interface* (on page 48)

Network Configuration (on page 221)

IP Configuration (on page 221)

IPv4-Only or IPv6-Only Configuration (on page 222)

Network Interface Settings (on page 223)

Configuring IPv4 Parameters (on page 250)

Setting the IPv4 Configuration Mode (on page 250)

Setting the IPv4 Preferred Host Name (on page 251)

Setting the IPv4 Address (on page 252)

Setting the IPv4 Gateway (on page 253)

Setting IPv4 Static Routes (on page 253)

Setting the IPv6 Configuration Mode (on page 254)

Setting the IPv6 Preferred Host Name (on page 255)

Setting the IPv6 Address (on page 256)

Setting the IPv6 Gateway (on page 257)

Setting IPv6 Static Routes (on page 257)

Configuring DNS Parameters (on page 259)

Setting LAN Interface Parameters (on page 259)

Enabling or Disabling the LAN Interface (on page 260)

Changing the LAN Interface Speed (on page 260)

Changing the LAN Duplex Mode (on page 261)

Deleting an NTP Server (on page 271)

Downloading Diagnostic Data via SCP (on page 347)

Step C. Configure LDAP Authentication on the PXE Device (on page 393)

Reserving IP Addresses in DHCP Servers (on page 443)

Reserving IP in Windows (on page 443)

Reserving IP in Linux (on page 444)

"To Assert" and Assertion Timeout (on page 449)

"To De-assert" and Deassertion Hysteresis (on page 451)

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
Before You Begin 3

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).

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 is available.

Link-local addressing:

- IPv4 address:

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

- IPv6 address:

  A link-local IPv6 address is available only after IPv6 is enabled on the PXE. See ***Configuring Network Settings*** (on page 104).

- 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 15).

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 349).*

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 351). 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.

Chapter 2 Rack-Mounting the PDU

This chapter describes how to rack mount a PXE device.

In This Chapter

Rackmount Safety Guidelines 5
Circuit Breaker Orientation Limitation 5
Mounting 1U Models Using L-Brackets and Buttons 6
Mounting Zero U Models Using Two Rear Buttons 7
Mounting Zero U Models Using L-Brackets and Buttons 9

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 349) 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%.

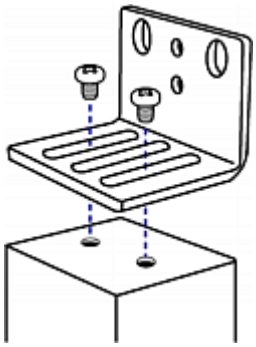
Note: If normally the line cord is down, upside down means the line cord is up.

Mounting 1U Models Using L-Brackets and Buttons

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

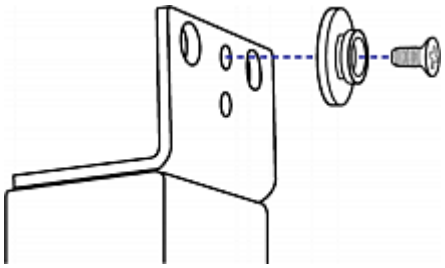
To mount 1U models using L-brackets and two buttons:

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).



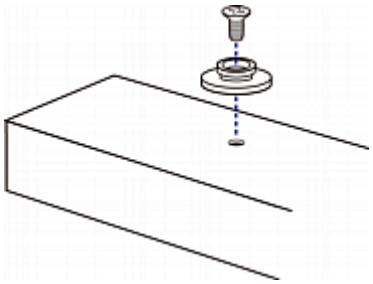
Mounting Zero U Models Using Two Rear Buttons

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 5) before mounting it.

To mount Zero U models using two buttons:

1. Turn to the rear of the PDU.

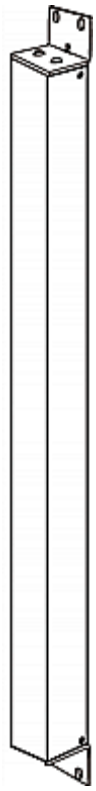
2. Locate two screw holes on the rear panel: one near the bottom and the other near the top (the side of cable gland).
3. Screw a button in the screw hole near the bottom. The recommended torque for the button is 1.96 N·m (20 kgf·cm).



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.

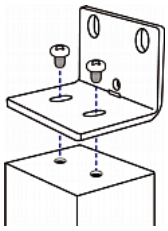
Mounting Zero U Models Using L-Brackets and Buttons

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 5) before mounting it.



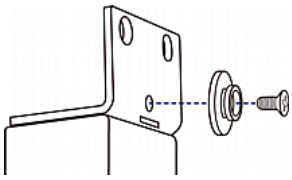
To mount Zero U models using L-brackets and two buttons:

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 Initial Installation and Configuration

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

In This Chapter

Connecting the PDU to a Power Source 11
Connecting the PXE to Your Network 11
Configuring the PXE 12
Bulk Configuration Methods 18
Installing Cable Retention Clips on Outlets (Optional) 18

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.

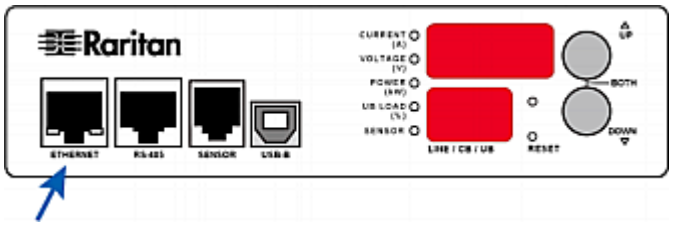
Connecting the PXE to Your Network

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.



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 15).
   - 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 49).

     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 IPv4 network. See *Connecting the PXE to Your Network* (on page 11).
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 15). 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 442).

3. Launch a web browser to configure the PXE. See ***Login*** (on page 49).

Tip: To configure a number of PXE devices quickly, see **Bulk Configuration Methods** *(on page 18).*

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 Windows driver for USB serial console from the Raritan website's ***Support page*** (***http://www.raritan.com/support/***). The downloaded driver's name is *dominion-serial-setup-<n>.exe*, where <n> represents the file's version number.

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

Automatic driver installation in Windows®:

1. Make sure the 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

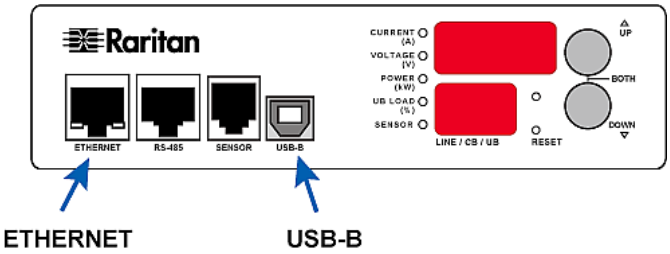
> connect

Connecting the PXE to a Computer

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

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

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 15).

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 49).

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 ***Configuring Network Settings*** (on page 104).

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. Refer to the following commands list. CLI commands are case sensitive.
9. After finishing the network settings, type `apply` to save changes. To abort, type `cancel`.

Commands for network settings:

The <ipvX> variable in all of the following commands is either *ipv4* or *ipv6*, depending on the type of IP protocol you are configuring. Replace the <ETH> variable with the word 'ethernet'.

- **General IP settings:**

To set or enable	Use this command
IPv4 or IPv6 protocol	`network <ipvX> interface <ETH> enabled <option>` <option> = *true*, or *false*
IPv4 configuration method	`network ipv4 interface <ETH> configMethod <mode>` <mode> = *dhcp* (default) or *static*
IPv6 configuration method	`network ipv6 interface <ETH> configMethod <mode>` <mode> = *automatic* (default) or *static*
Preferred host name (optional)	`network <ipvX> interface <ETH> preferredHostName <name>` <name> = preferred host name
IP address returned by the DNS server	`network dns resolverPreference <resolver>` <resolver> = *preferV4* or *preferV6*

- Static IP configuration:

To set	Use this command
Static IPv4 or IPv6 address	`network <ipvX> interface <ETH> address <ip address>` <ip address> = static IP address, with a syntax similar to the example below. ▪ Example: *192.168.7.9/24*
Static IPv4 or IPv6 gateway	`network <ipvX> gateway <ip address>` <ip address> = gateway's IP address
IPv4 or IPv6 primary DNS server	`network dns firstServer <ip address>` <ip address> = DNS server's IP address
IPv4 or IPv6 secondary DNS server	`network dns secondServer <ip address>` <ip address> = DNS server's IP address
IPv4 or IPv6 third DNS server	`network dns thirdServer <ip address>` <ip address> = DNS server's IP address

To verify network settings:

After exiting the above configuration mode and the # prompt re-appears, type this command to verify all network settings.

- `show network`

The IP address configured may take seconds to take effect.

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 199).

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 355).

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.

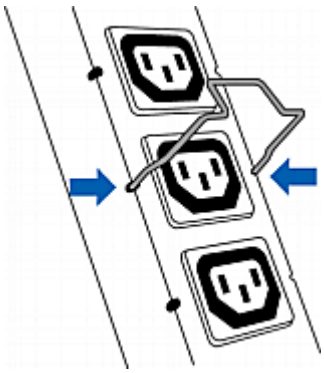
The use of cable retention clips is highly recommended for regions with high seismic activities, and environments where shocks and vibrations are expected.

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

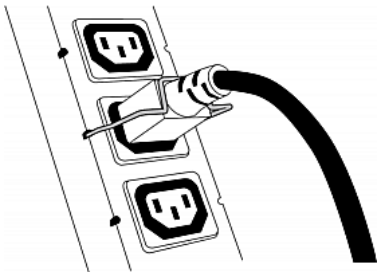
Note: Some NEMA sockets on PSE-certified PDUs for Japan have integral locking capability and do not need cable retention clips. See **Locking Outlets and Cords** *(on page 440).*

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:

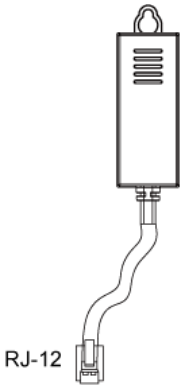
- *DPX Sensor Packages* (on page 21)
- *DPX2 Sensor Packages* (on page 27)
- *DPX3 Sensor Packages* (on page 29)
- *DX Sensor Packages* (on page 31)

In This Chapter

DPX Sensor Packages 21
DPX2 Sensor Packages 27
DPX3 Sensor Packages 29
DX Sensor Packages.....31
Using an Optional DPX3-ENVHUB4 Sensor Hub.....34
Mixing Diverse Sensor Types.....36

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 26).

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

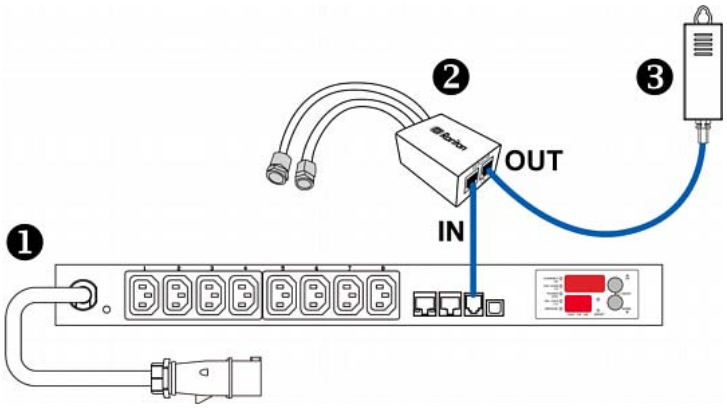
To connect a DPX sensor package with a factory-installed sensor cable:

- 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.



❶	The PXE device
❷	Raritan differential air pressure sensors
❸	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.

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

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

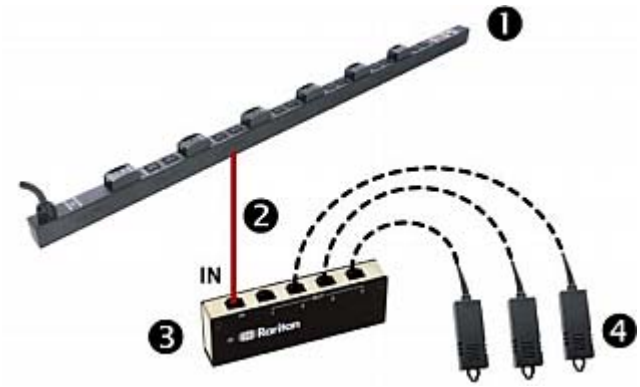
Tip: The Raritan sensor hub that supports ALL types of Raritan environmental sensor packages is DPX3-ENVHUB4*. See* **Using an Optional DPX3-ENVHUB4 Sensor Hub** *(on page 34).*

▶ 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.



❶	The PXE device
❷	Raritan-provided phone cable
❸	DPX-ENVHUB4 sensor hub
❹	DPX sensor packages

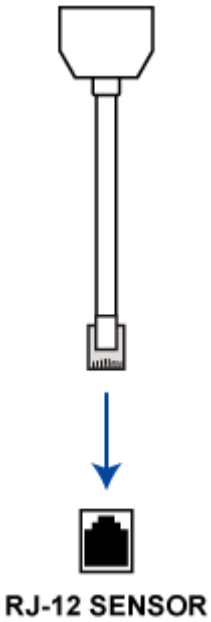
Using an Optional DPX-ENVHUB2 cable

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

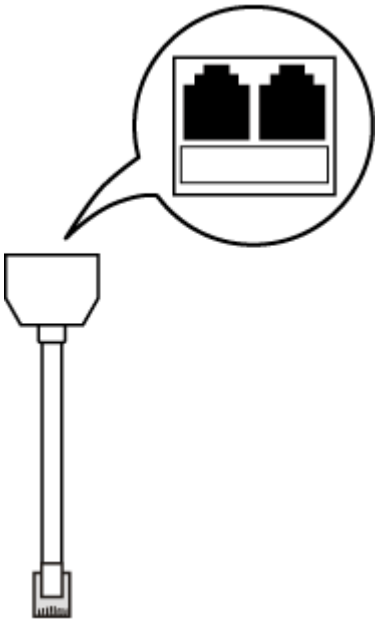
This cable supports DPX sensor packages only. Do NOT connect DPX2, DPX3 or DX sensor packages to it.

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

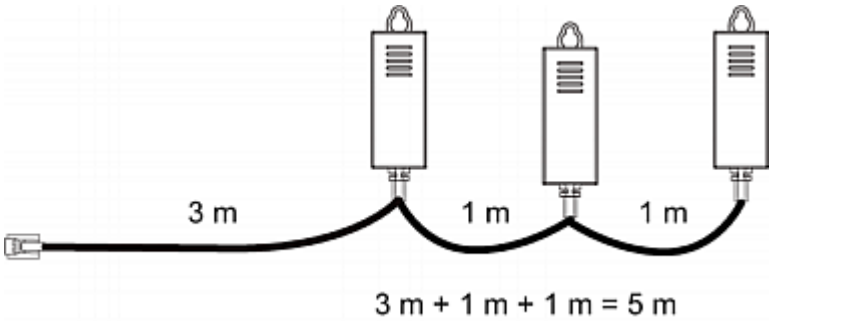
Sensor connection restrictions:

- 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.

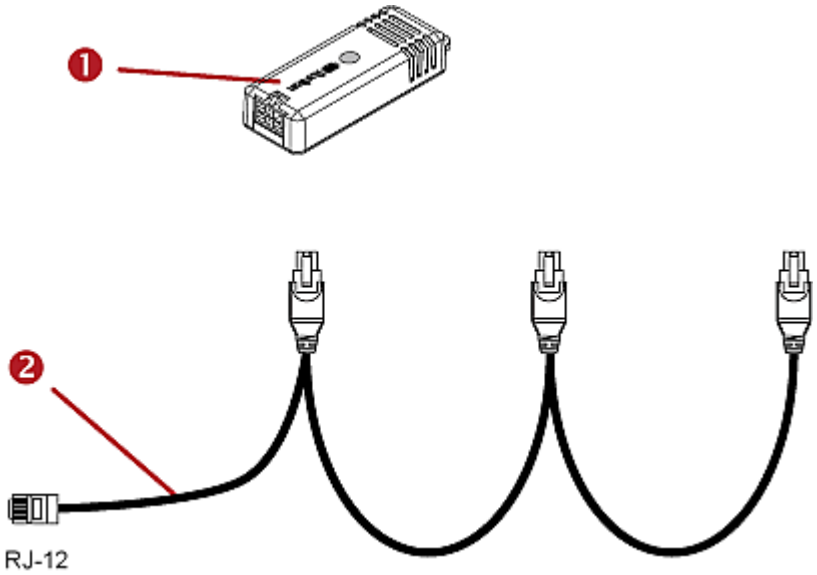
  Note that the length 16' (5 m) is the length of each DPX-T3H1 sensor cable, which is defined in the above diagram.

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/*).



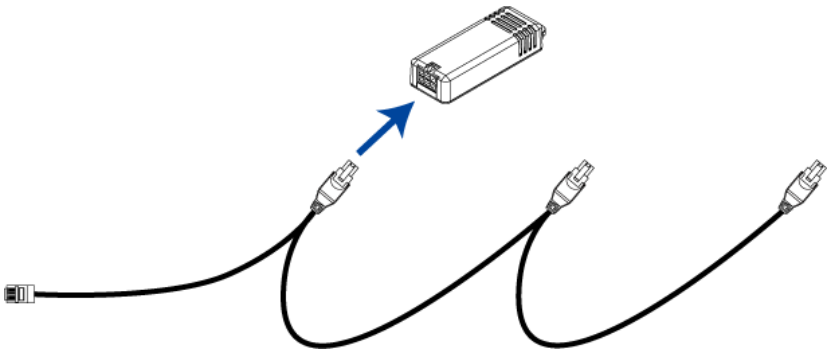
Item	
1	DPX2 sensor package
2	DPX2 sensor cable with one RJ-12 connector and three head connectors

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

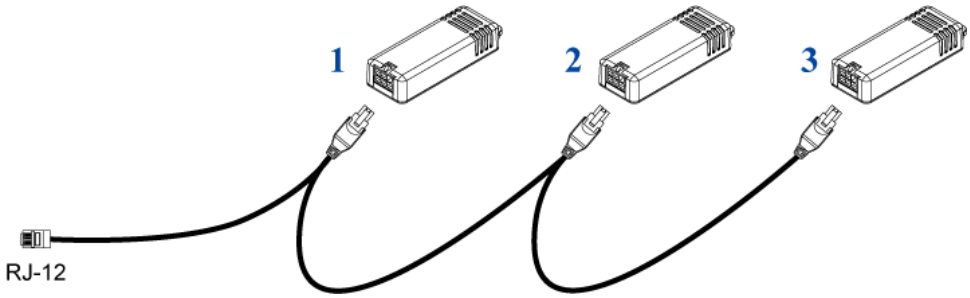
Warning: If there are free head connectors between a DPX2 sensor cable's RJ-12 connector and the final attached DPX2 sensor package, the sensor packages following the free head connector(s) on the same cable do NOT work properly. Therefore, always occupy all head connectors prior to the final sensor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

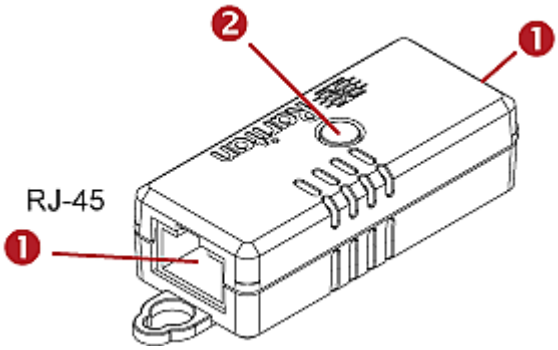
3. Plug the RJ-12 connector of the DPX2 sensor cable into the RJ-12 SENSOR port on the PXE.

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 33).

DPX3 Sensor Packages

A DPX3 sensor package features the following:

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

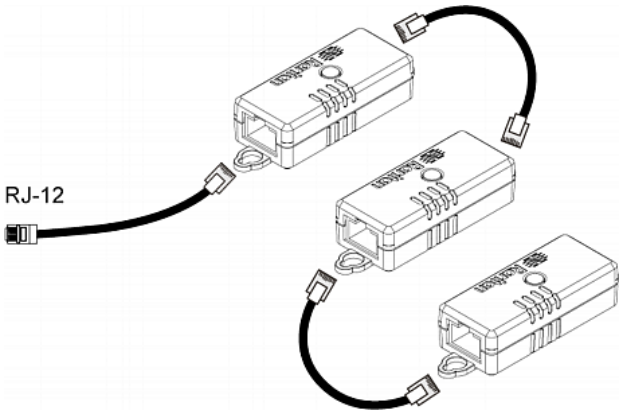


Numbers	Components
❶	RJ-45 ports, each of which is located on either end of a DPX3 sensor package.
❷	LED for indicating the sensor status.

To connect DPX3 sensor packages to the 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.

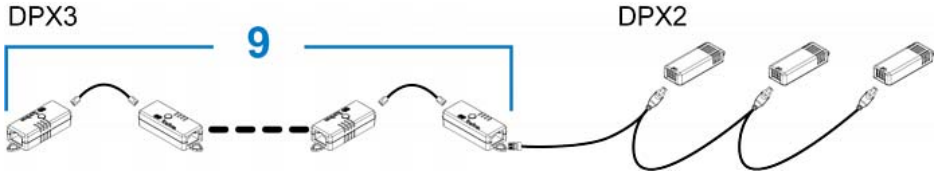
Connecting a DPX2 Sensor Package to DPX3

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.

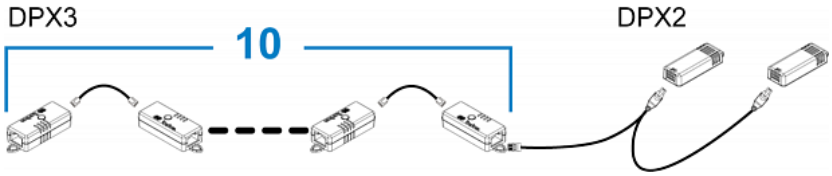
▶ **When connecting a DPX2 sensor package containing three DPX2 sensors:**

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



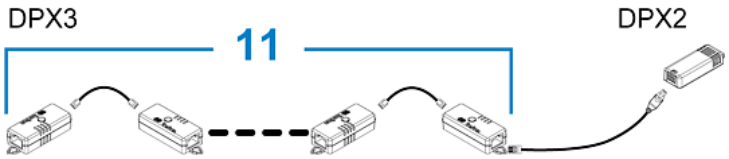
▶ **When connecting a DPX2 sensor package containing two DPX2 sensors:**

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/*).

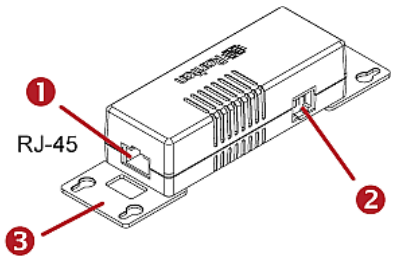
You can cascade up to 12 DX sensor packages.

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*3=36) exceeds 32 by 4.

Tip: To manage the last 4 functions, you can release 4 "managed" sensors or actuators, and then manually bring the last 4 functions into management. See **Peripherals** *(on page 76).*



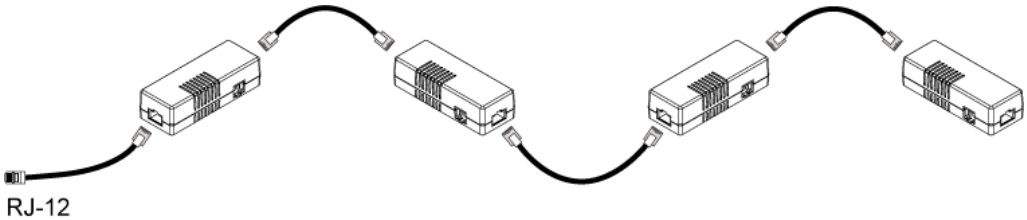
Numbers	Components
1	RJ-45 ports, each of which is located on either end of a DX sensor package.
2	RJ-12 port, which is reserved for future

Numbers	Components
	use and now blocked.
❸	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 33).

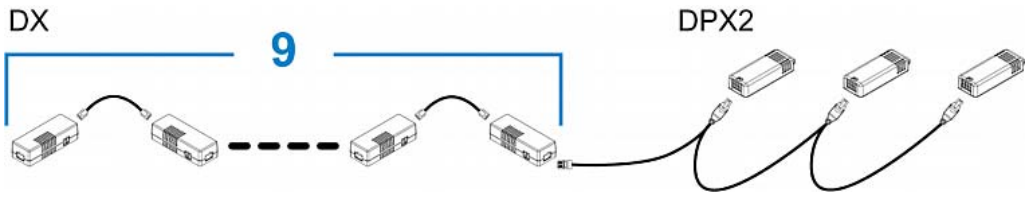
Connecting a DPX2 Sensor Package to DX

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.

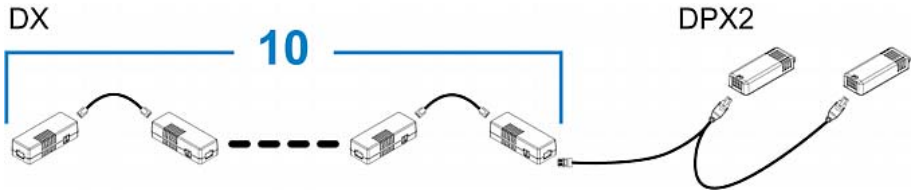
- **When connecting a DPX2 sensor package containing three DPX2 sensors:**

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



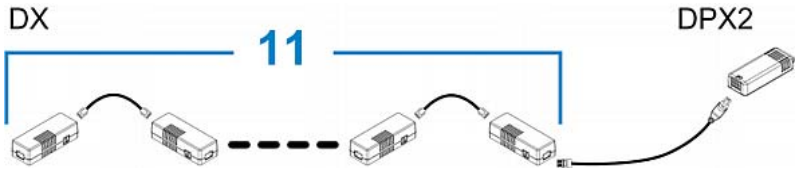
- **When connecting a DPX2 sensor package containing two DPX2 sensors:**

  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:

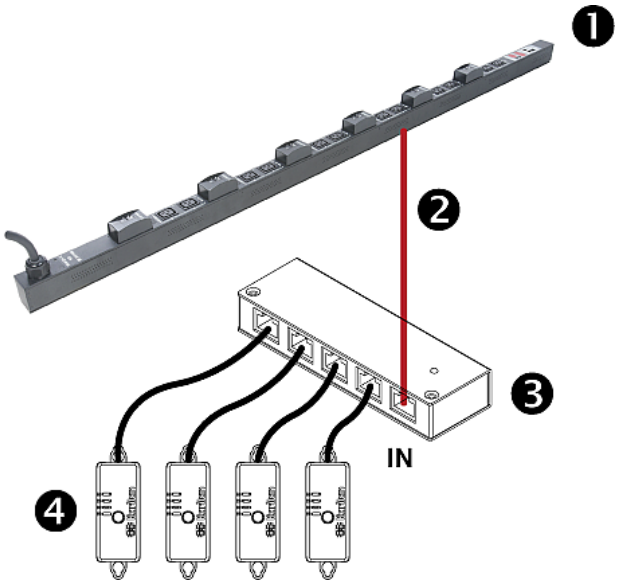
- All ports on the DPX3-ENVHUB4 sensor hub are RJ-45 instead of RJ-12 as the DPX-ENVHUB4 sensor hub.
- The DPX3-ENVHUB4 sensor hub supports all Raritan environmental sensor packages, including DPX, DPX2, DPX3 and DX sensor packages.

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 36).

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

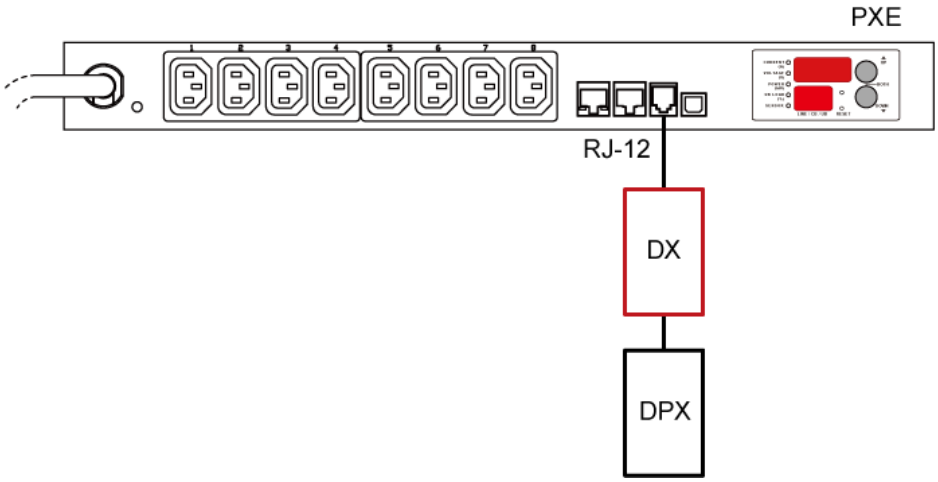
You can mix DPX, DPX2, DPX3 and DX sensor packages on one PXE according to the following sensor combinations. In some scenarios, the DPX3-ENVHUB4 sensor hub is required.

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.

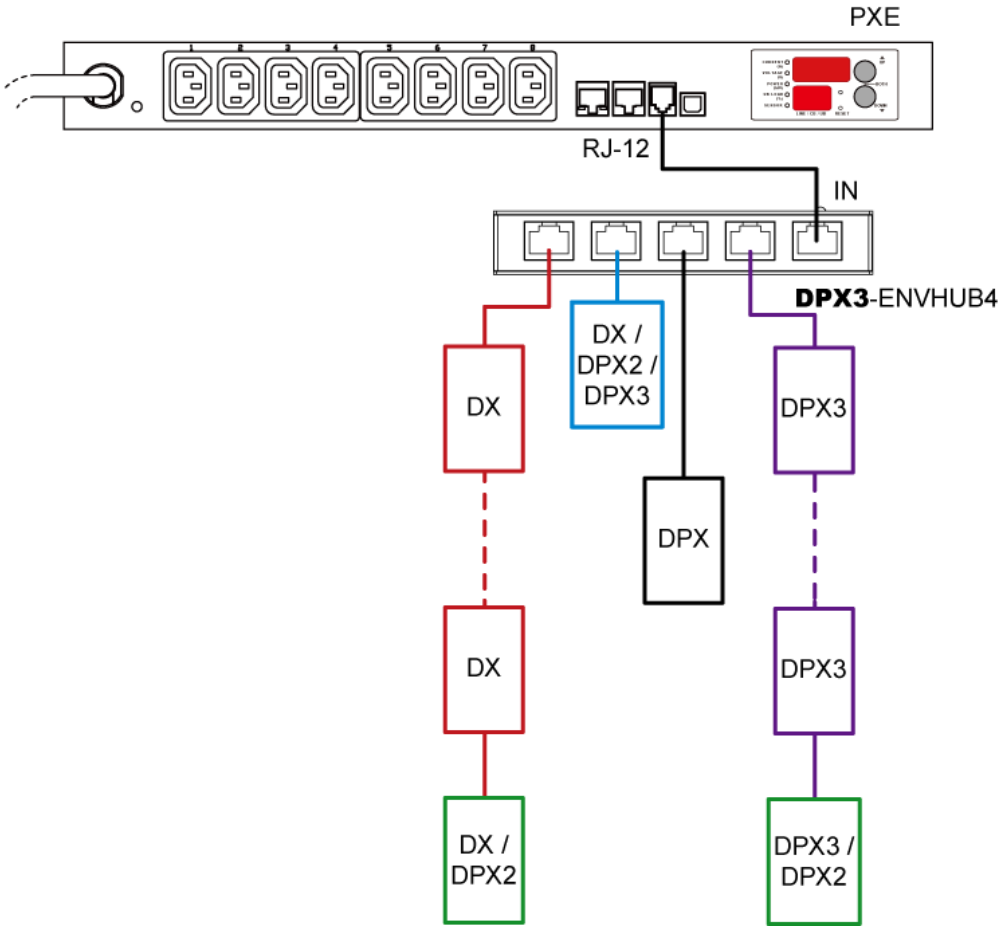


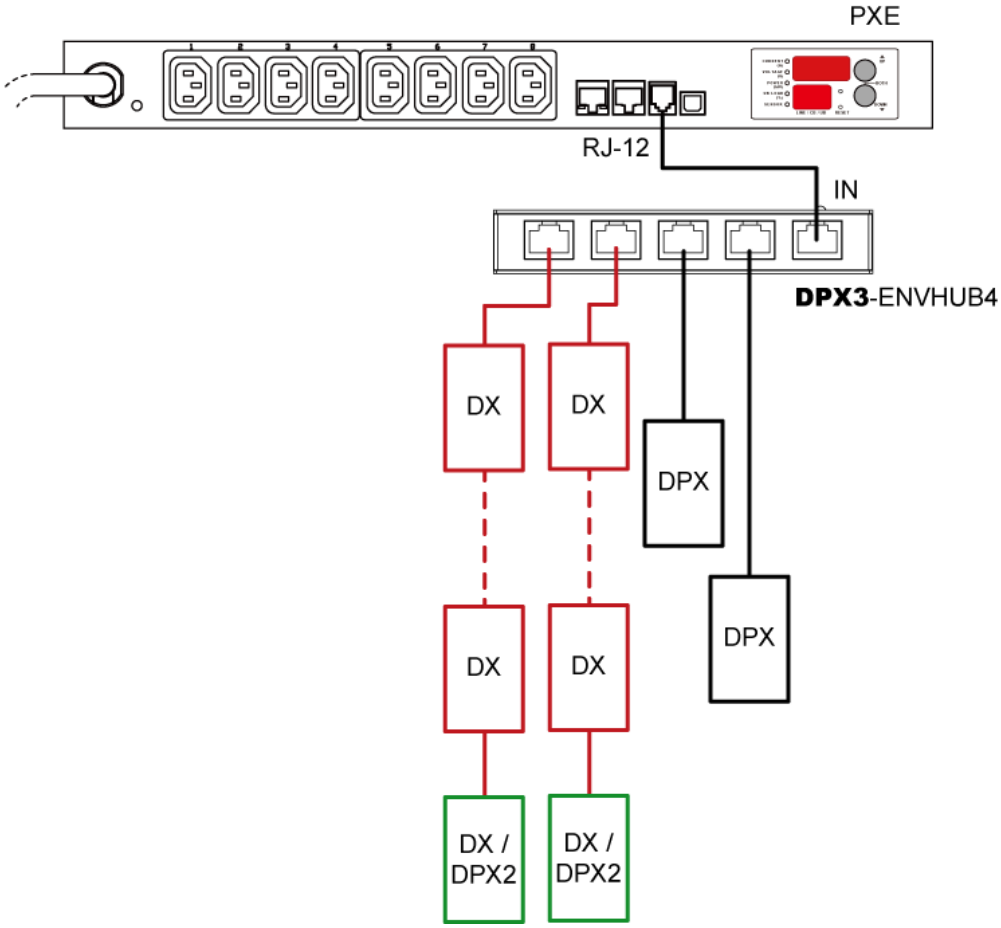
Diverse combinations via the DPX3-ENVHUB4 sensor hub:

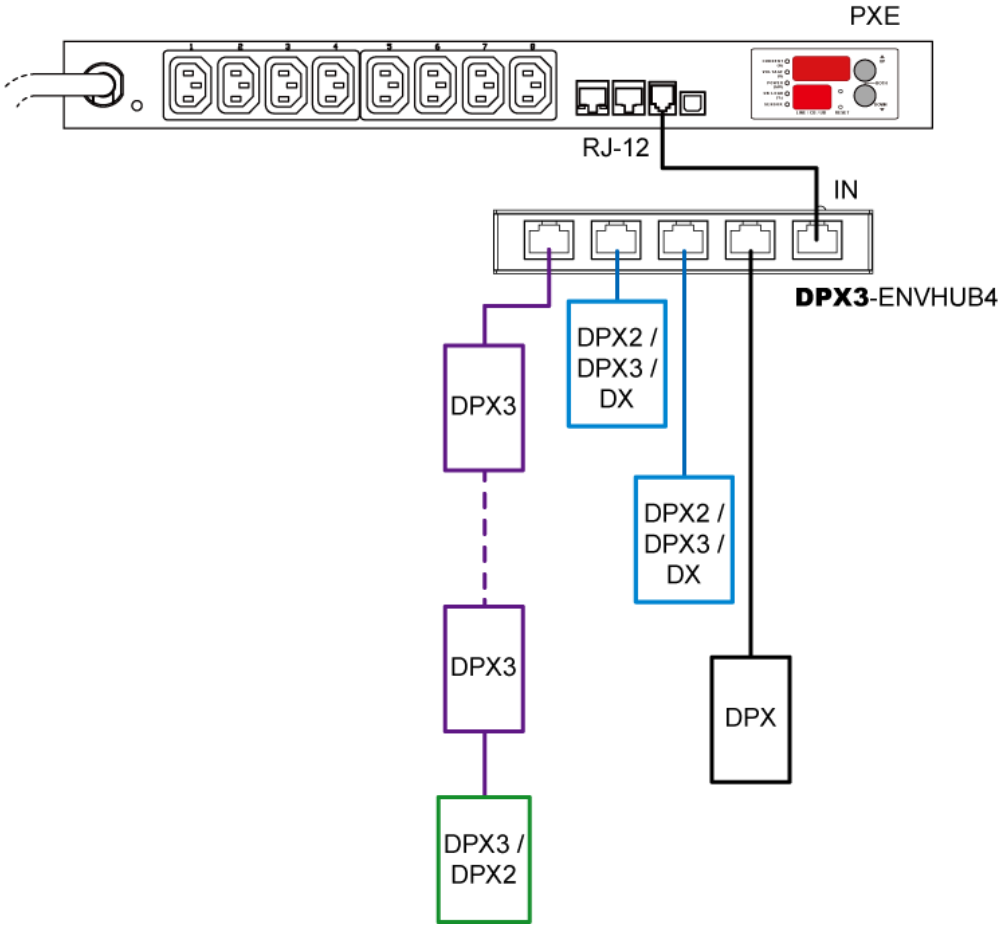
- You must use the **DPX3**-ENVHUB4 sensor hub instead of the old DPX-ENVHUB4 sensor hub. Each port on the hub supports any of the following:
  - A DX sensor package
  - A chain of DX sensor packages
  - A DPX3 sensor package
  - A chain of DPX3 sensor packages
  - A DPX2 sensor package
  - A DPX sensor 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 illustrations the following three combinations, but actually there are tens of different combinations by using the DPX3-ENVHUB4 sensor hub.



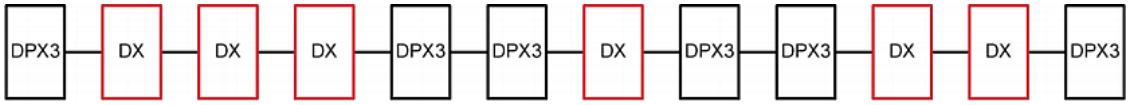

PXE
RJ-12
IN
DPX3-ENVHUB4
DX
DX
DPX
DX
DX
DPX
DX / DPX2
DX / DPX2



Mix DPX3 and DX in a sensor chain:

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

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



You can add a DPX2 sensor package to the end of such a sensor-mixing chain if intended. See *Connecting a DPX2 Sensor Package to DPX3* (on page 30) or *Connecting a DPX2 Sensor Package to DX* (on page 33).

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 40
Circuit Breakers 45

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 PXE 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

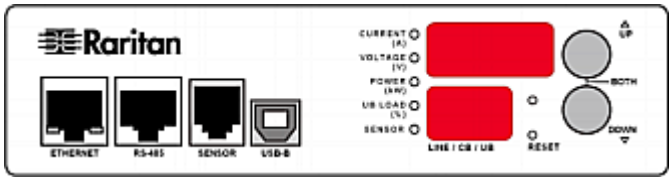
The total number of outlets varies from model to model.

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.



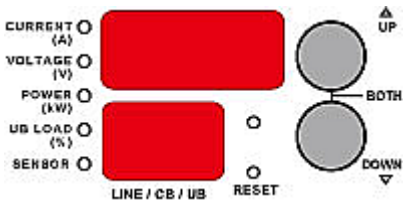
The table below explains the function of each port.

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)	Connection to one of the following devices: ▪ Raritan's environmental sensor package(s). ▪ Raritan's sensor hub, which expands the number of a sensor port to four ports.
ETHERNET	Connecting the PXE to your company's network via a standard network patch cable (Cat5e/6). This connection is necessary to administer or access the PXE remotely. There are two small LEDs adjacent to the port: ▪ Green indicates a physical link and activity. ▪ Yellow indicates communications at 10/100 BaseT speeds.

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 Firmware Upgrade is being performed

LEDs for Measurement Units

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

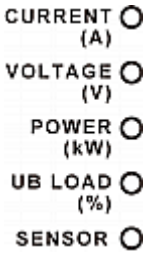
The measurement units vary according to the readings that appear in the three-digit row. They are:

- 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:

- Lx: 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 △ (UP) button moves up one selection.
   - Pressing the ▽ (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 43).
   - 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.

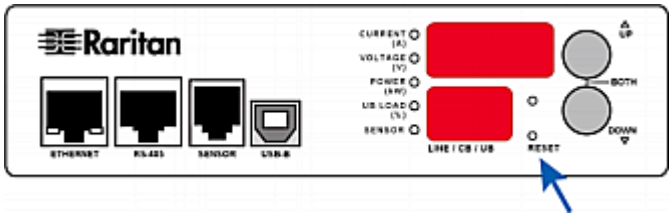
Note: The LED display returns to the Automatic Mode after 20 seconds elapse since the last time any button was pressed.

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.

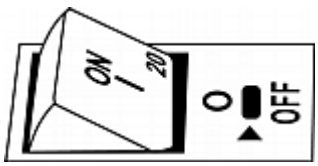
Depending on the model you purchased, the circuit breaker may use a button- or handle-reset mechanism.

Resetting the Button-Type Circuit Breaker

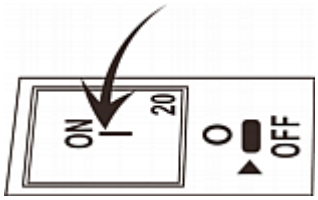
Your button-type circuit breakers may look slightly different from the images shown in this section, but the reset procedure remains the same.

▶ **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.

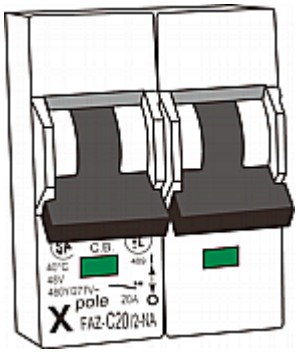


Resetting the Handle-Type Circuit Breaker

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

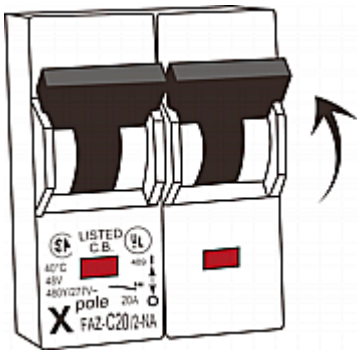
To reset the handle-type breakers:

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 48
Login, Logout and Password Change 48
Web Interface Overview 51
Dashboard 56
PDU 65
Inlet 68
Outlets 70
OCPs 73
Peripherals 76
User Management 94
Device Settings 103
Maintenance 193

Supported Web Browsers

- Internet Explorer® 11
- Windows Edge
- Firefox® 25 and later
- Safari® (Mac)
- Google® Chrome® 52 and later
- Android 4.2 and later
- iOS 7.0 and later

Note: Depending on the browser you use, spin controls similar to *may or may not appear in the numeric input fields. Clicking these adjusts numeric values by 1.*

Login, Logout and Password Change

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

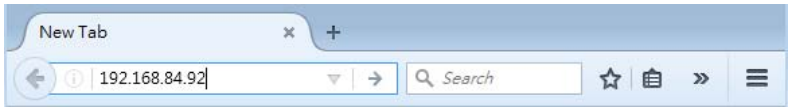
After login, you can create user accounts for other users. See *Creating Users* (on page 94).

Login

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

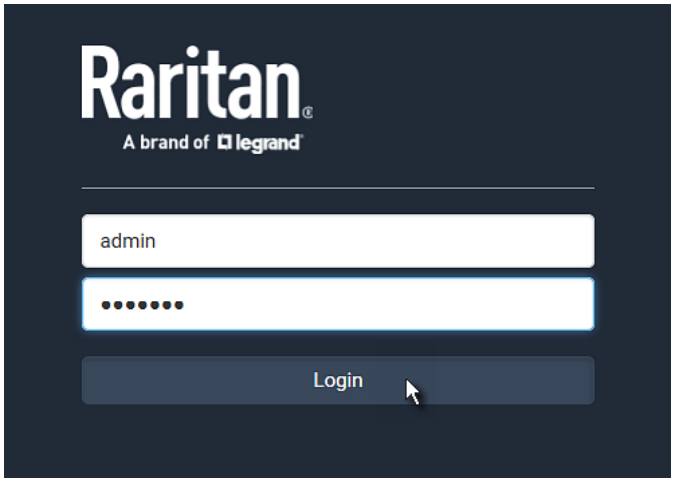
To log in to the web interface:

1. Open a browser and type the IP address of the PXE.
   - 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).



Tip: You can also enter the desired page's URL so that you can immediately go to that page after login. See **Quick Access to a Specific Page** *(on page 55).*

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



4. (Optional) If a security agreement is displayed, accept it. Otherwise, you cannot log in.
   - To select the agreement checkbox using the keyboard, first press Tab to go to the checkbox and then Enter.

Note: To configure the security agreement, see **Enabling the Restricted Service Agreement** *(on page 143).*

5. Click Login or press Enter. The PXE web interface opens.

Changing Your Password

You must have the Change Own Password permission to change your own password. See ***Creating Roles*** (on page 99).

You must have Administrator Privileges to change other users' passwords. See ***Editing or Deleting Users*** (on page 98).

Password change request on first login:

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

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

Users without permissions listed must change password.

Note: This password change request also appears if the 'force password change' is enabled in the user account setting. See Creating Users *(on page 94).*

To change your password via the Change Password command:

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

Remembering User Names and Passwords

The PXE supports the password manager of common web browsers, including:

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

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

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

The PXE does NOT support other browser password managers.

Logout

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

To log out without closing the web browser:

- Click "Logout" on the top-right corner.

  -- OR --

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

To log out by closing the web browser:

- Click on the top-right corner of the window.

  -- OR --

- Choose File > Close, or File > Exit.

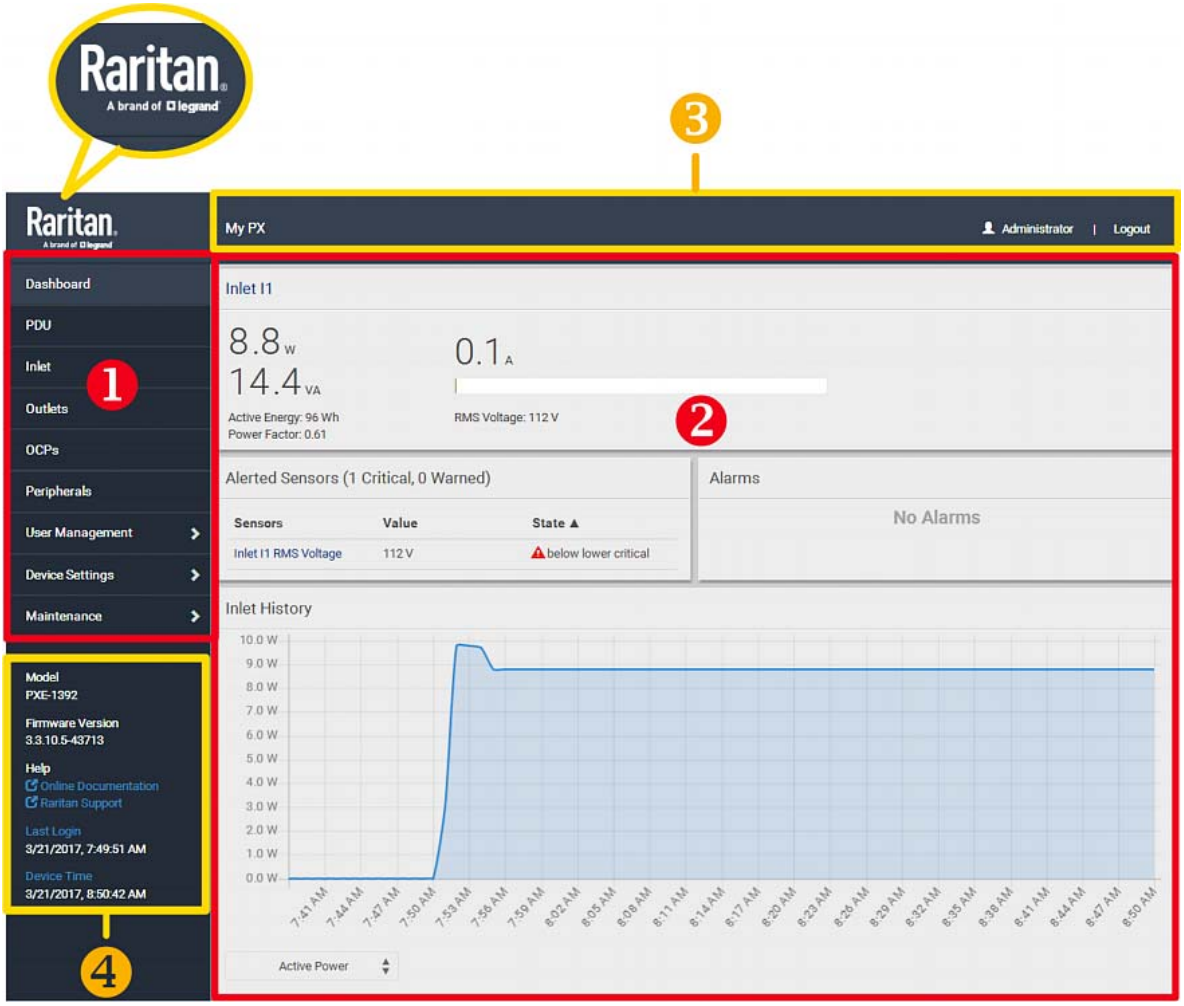
Web Interface Overview

The web interface consists of four areas as shown below.

Operation:

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

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

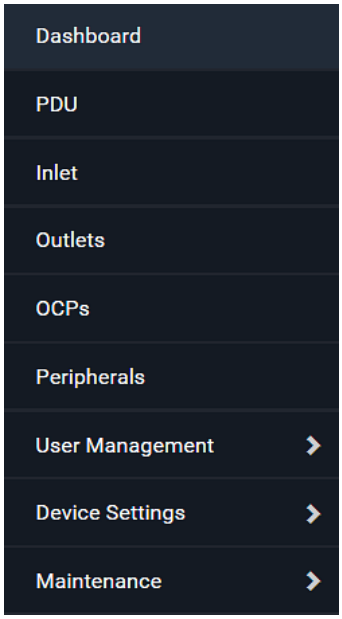


Number	Web interface element
1	*Menu* (on page 53)
2	Data/setup page of the selected menu item
3	▪ Left side: - PXE device name *Note: To customize the device name, see* PDU *(on page 65).* ▪ Right side:

Number	Web interface element
	- Your login name, which you can click to view your user account settings - Logout button
4	From top to bottom -- ▪ Your PXE model ▪ Current firmware version ▪ **Online Documentation**: link to the PXE online help. - See ***Browsing through the Online Help*** (on page 458). ▪ **Raritan Support**: link to the Raritan Technical Support webpage. ▪ Date and time of your user account's last login - Click **Last Login** to view your login history. ▪ PXE system time - Click **Device Time** to open the Date/Time setup page.

Menu

Depending on your model and hardware configuration, your PXE may show all or some menu items shown below.

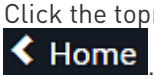


Menu	Information shown
Dashboard	Summary of the PXE status, including a list of alerted sensors and alarms, if

Menu	Information shown
	any. See *Dashboard* (on page 56).
PDU	Device data and settings, such as the device name and MAC address. See *PDU* (on page 65).
Inlet	Inlet status and settings, such as inlet thresholds. See *Inlet* (on page 68).
Outlets	Outlet data and settings, such as customizing each outlet's name. See *Outlets* (on page 70).
OCPs	The OCPs menu item appears only when there are overcurrent protectors implemented on your model. OCP data and settings, such as customizing each OCP's name. See *OCPs* (on page 73).
Peripherals	Status and settings of Raritan environmental sensor packages, if connected. See *Peripherals* (on page 76).
User Management	Data and settings of user accounts and groups, such as password change. See *User Management* (on page 94).
Device Settings	Device-related settings, including network, security, system time, event rules and more. See *Device Settings* (on page 103).
Maintenance	Device information and maintenance commands, such as firmware upgrade, device backup and reset. See *Maintenance* (on page 193).

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

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

- Click the topmost link with the symbol **>**. For example, click  .
- Press Backspace on the keyboard.
- OR click on the top-left corner to return to the main menu.

Quick Access to a Specific Page

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

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

URL examples:

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

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

Sorting a List

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

Example:

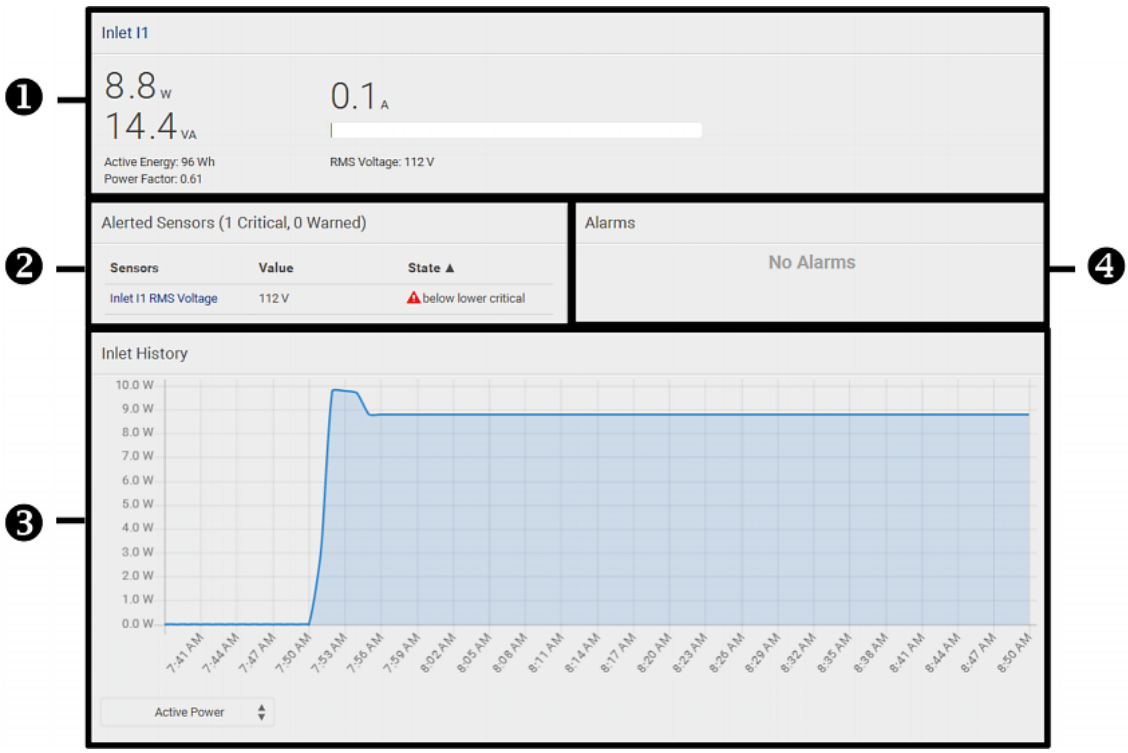
1. By default, the Firmware Update History is sorted in the ascending order based on the Timestamp column. Therefore, the arrow ▲ is displayed adjacent to the Timestamp header.
2. To have it resorted in the descending order based on the same column, click the Timestamp header.
3. The arrow turns to ▼, indicating the list is sorted in the "descending" order.

Timestamp ▼

4. To resort the list based on a different column, click a different column header.
5. The arrow ▲ now appears adjacent to the selected column header, indicating the list is sorted in the ascending order based on that column.

Dashboard

The Dashboard page contains four sections.



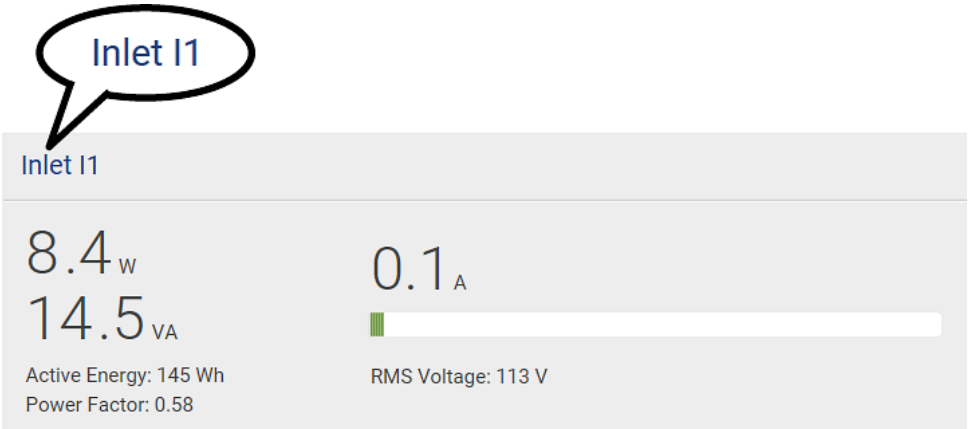
Number	Section	Information shown
❶	Inlet I1	▪ Overview of inlet power data ▪ A current bar per phase, which changes colors to indicate the RMS current state - green: normal - yellow: warning - red: critical See *Dashboard - Inlet I1* (on page 58).
❷	Alerted Sensors	▪ When no sensors enter the alarmed state, this section shows the message "No Alerted Sensors." ▪ When any sensor enters the alarmed state, this section lists all of them. See *Dashboard - Alerted Sensors* (on page 60).
❸	Inlet History	The waveform of the inlet's active power history is displayed by default. You can make it show a different data type. See *Dashboard - Inlet History* (on page 62).
❹	Alarms	This section can show data only after you have set event rules requiring users to take the acknowledgment action. ▪ When there are no unacknowledged events, this section shows the message "No Alarms." ▪ When there are unacknowledged events, this section lists all of them. See *Dashboard - Alarms* (on page 63).

Dashboard - Inlet I1

The number of phases shown in the Inlet section varies, depending on the model.

Link to the Inlet page:

To view more information or configure the inlet(s), click this section's title 'Inlet I1' to go to the Inlet page. See *Inlet* (on page 68).



Left side - generic inlet power data:

The left side lists all or some of the following data. Available data is model dependent.

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

Right side - inlet's current and voltage:

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

Inlet data from top to bottom includes:

- RMS current (A)
- A bar showing the RMS current level
- RMS voltage (V)

The RMS current bars automatically change colors to indicate the current status if the thresholds have been enabled. To configure thresholds, see ***Inlet*** (on page 68).

Status	Bar colors
normal	
above upper warning	
above upper critical	

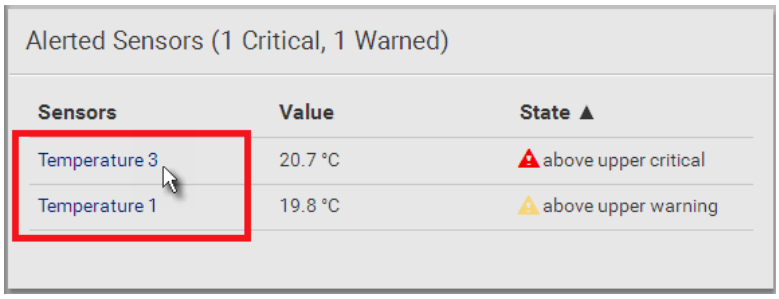
Note: The "below lower warning" and "below lower critical" states also show yellow and red colors respectively. However, it is not meaningful to enable these two thresholds for current levels.

Dashboard - Alerted Sensors

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

To view detailed information or configure each alerted sensor, you can click each sensor's name to go to individual sensor pages. See *Individual Sensor/Actuator Pages* (on page 89).

If wanted, you can resort the list by clicking the desired column header. See *Sorting a List* (on page 55).



Summary in the section title:

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

For example:

- 1 Critical: 1 sensor enters the critical or alarmed state.
  - Numeric sensors enter the critical state.
  - State sensors enter the alarmed state.

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

List of alerted sensors:

Two icons are used to indicate various sensor states.

Icons	Sensor states
	For numeric sensors: ▪ above upper warning ▪ below lower warning
	For numeric sensors: ▪ above upper critical ▪ below lower critical
	For state sensors: ▪ alarmed state

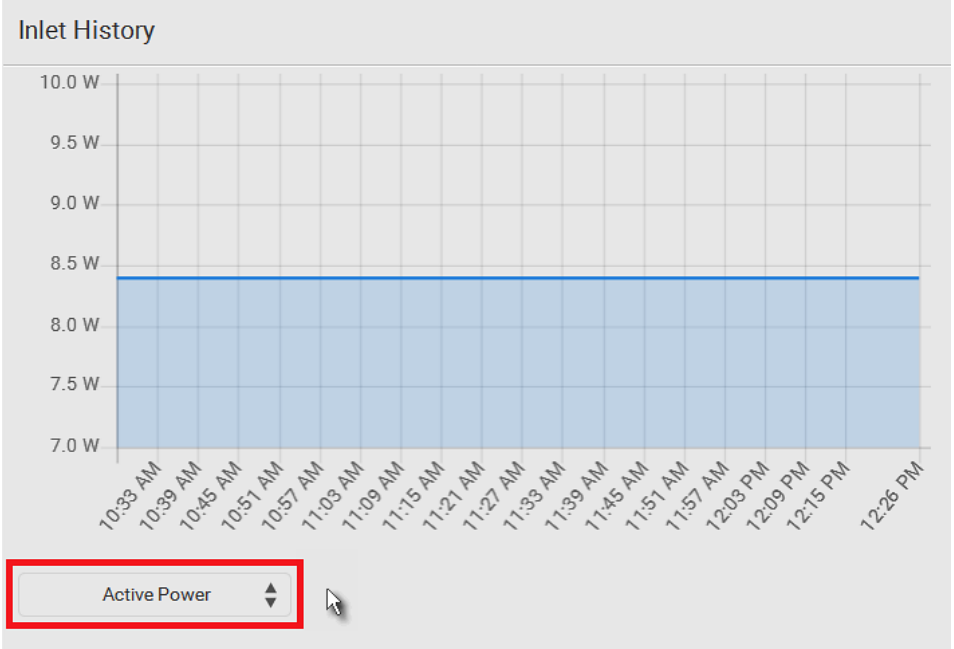
For details, see *Sensor/Actuator States* (on page 83).

Dashboard - Inlet History

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

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

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



Inlet selection on multi-inlet models:

If your PDU is a multi-inlet model, you can have one or multiple inlets show their power waveforms by selecting the checkbox(es) of the desired inlet(s).

- When multiple inlets are displayed, their waveform colors differ. You can identify each waveform according to the colors of the selected inlet checkboxes as illustrated below.

Dashboard - Alarms

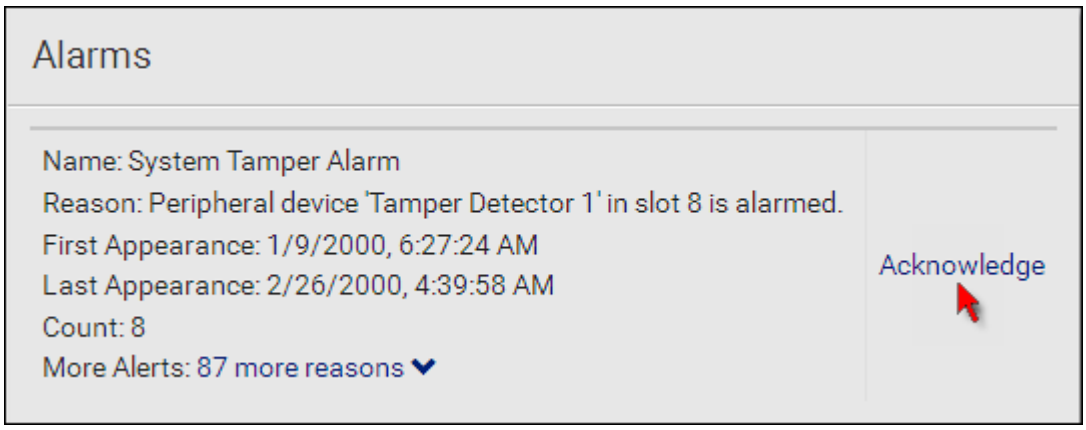
If configuring any event rules which require users to take the acknowledgment action, the Alarms section will list any event which no one acknowledges yet since event occurrence.

Note: For information on event rules, see **Event Rules and Actions** *(on page 146).*

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

To acknowledge an alarm:

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



This table explains each column of the alarms list.

Field	Description
Name	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	This field appears only when there are more than one type of events triggering this alert. If there are other types of events (that is, other reasons) triggering the same alert, the total number of additional reasons is displayed. You can click it to view a list of all events triggering this alert.

PDU

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

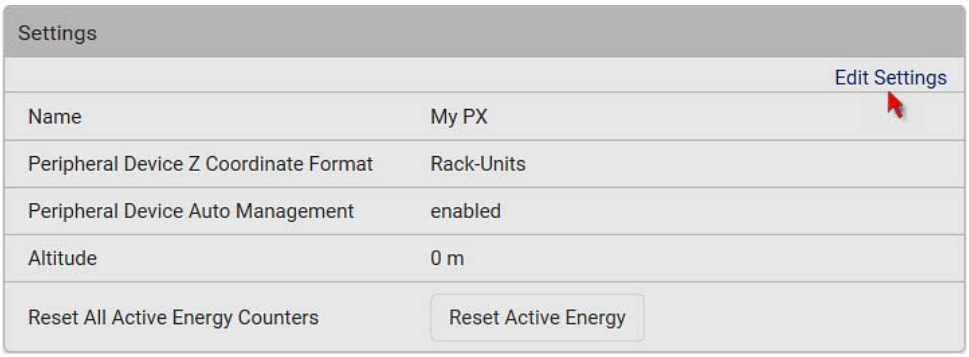
To open the PDU page, click 'PDU' in the ***Menu*** (on page 53).

Device information shown:

- Firmware version
- Serial number
- MAC address
- Rating

To configure global settings:

1. Click Edit Settings.



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

Field	Function	Note
Name	Customizes the device name.	
Peripheral Device Z Coordinate Format	Determines how to describe the vertical locations (Z coordinates) of Raritan environmental sensor packages. ▪ *Options: Rack-Units and Free-Form* See ***Z Coordinate Format*** (on page 67).	To specify the location of any sensor/actuators in the data center, see ***Individual Sensor/Actuator Pages*** (on page 89).

Field	Function	Note
Peripheral Device Auto Management	Enables or disables the automatic management feature for Raritan environmental sensor packages. ▪ *The default is to enable it.*	See ***How the Automatic Management Function Works*** (on page 67).
Altitude	Specifies the PXE device's altitude above sea level when a Raritan's DPX differential air pressure sensor is attached. ▪ *Range: 0 to 3000 meters (0 to 9842 feet)*	▪ The device's altitude is associated with the altitude correction factor. See ***Altitude Correction Factors*** (on page 455). ▪ The default altitude measurement unit is meter. See ***Setting Default Measurement Units*** (on page 102). ▪ You can have the measurement unit vary between meter and foot according to user credentials. See ***Setting Your Preferred Measurement Units*** (on page 102).

3. Click Save.

▶ To reset ALL active energy counters:

An active energy reading is a value of total accumulated energy, which is never reset, even if the power fails or the 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.

1. Click Reset Active Energy.
2. Click Reset on the confirmation message.
   - All active energy readings on this PXE are reset to zero.

Tip: You can choose to reset the active energy reading of an individual inlet only. See Inlet *(on page 68).*

Internal Beeper State

The PXE does NOT have an internal beeper so the internal beeper's state on the PDU page always shows Off.

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, which are configured on the *Individual Sensor/Actuator Pages* (on page 89).

The Z coordinate format is determined on *PDU* (on page 65). For a Z coordinate example, see *Sensor/Actuator Location Example* (on page 93).

Available Z coordinate formats:

- Rack Units: The height of the Z coordinate is measured in standard rack units. When this is selected, you can type a numeric value in the rack unit to describe the Z coordinate of any environmental sensors or actuators.
- Free-Form: Any alphanumeric string can be used for specifying the Z coordinate. The value can be 0 to 24 characters long.

How the Automatic Management Function Works

This setting is configured on *PDU* (on page 65).

After enabling the automatic management function:

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

A PXE can manage up to 32 sensors/actuators.

After disabling the automatic management function:

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

You must manually manage new sensors/actuators. See *Peripherals* (on page 76).

Inlet

You can view all inlet information, configure inlet-related settings, or reset the inlet active energy on the Inlet page. To open this page, click 'Inlet' in the *Menu* (on page 53).

Inlet thresholds, when enabled, help you identify whether the inlet enters the warning or critical level. In addition, you can have the PXE automatically generate alert notifications for any warning or critical status. See *Event Rules and Actions* (on page 146).

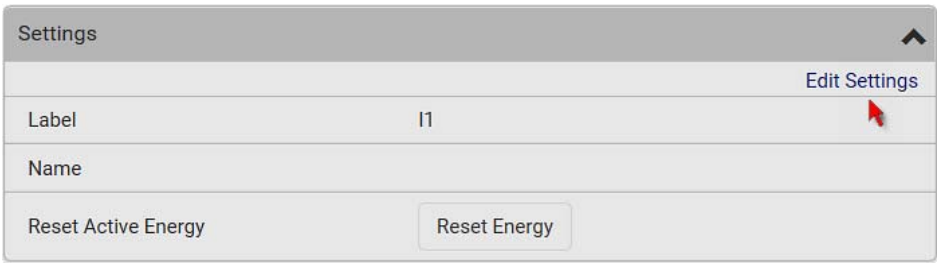
Generic inlet information shown:

- Inlet power overview, which is the same as *Dashboard - Inlet I1* (on page 58).
- A list of inlet sensors with more details. Number of available inlet sensors depends on the model.
  - Sensors show both readings and states.
  - Sensors in warning or critical states are highlighted in yellow or red.

  See *Yellow- or Red-Highlighted Sensors* (on page 81).
- Inlet's power waveform, which is the same as *Dashboard - Inlet History* (on page 62)

To customize the inlet's name:

1. Click Edit Settings.



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

To reset the inlet's active energy counter:

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

The energy reset feature per inlet is especially useful when your PXE has more than one inlet.

1. Click Reset Energy.
2. Click Reset on the confirmation message.

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

Tip: To reset ALL active energy counters on the PXE, see **PDU** *(on page 65).*

To configure inlet thresholds:

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

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

Thresholds

Edit Thresholds

Sensor ▲	Lower Critical	Lower Warning	Upper Warning	Upper Critical
Active Energy	---	---	---	---
Active Power	---	---	---	---
Apparent Power	---	---	---	---
Power Factor	---	---	---	---
RMS Current	---	---	20.8 A	25.6 A
RMS Voltage	188 V	194 V	247 V	254 V

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

   For concepts of thresholds, deassertion hysteresis and assertion timeout, see ***Sensor Threshold Settings*** (on page 446).
4. Click Save.

Outlets

The Outlets page shows a list of all outlets and their data, such as each outlet's associated lines. To open this page, click 'Outlets' in the *Menu* (on page 53).

Outlets

# ▲	Name	Receptacle Type	Lines
1	Outlet 1	IEC 60320 C13	L1–NEUTRAL
2	Outlet 2	IEC 60320 C13	L1–NEUTRAL
3	Outlet 3	IEC 60320 C13	L1–NEUTRAL
4	Outlet 4	IEC 60320 C13	L1–NEUTRAL
5	Outlet 5	IEC 60320 C13	L1–NEUTRAL

- **Go to an individual outlet's data/setup page by clicking an outlet's name.** See *Individual Outlet Pages* (on page 71).

Outlets

# ▲	Name
1	Outlet 1
2	Outlet 2
3	Outlet 3
4	Outlet 4

If wanted, you can resort the list by clicking the desired column header. See *Sorting a List* (on page 55).

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

1. Click to show a list of outlet data types.
2. Select those you want to show, and deselect those you want to hide. See *Available Data of the Outlets Overview Page* (on page 71).

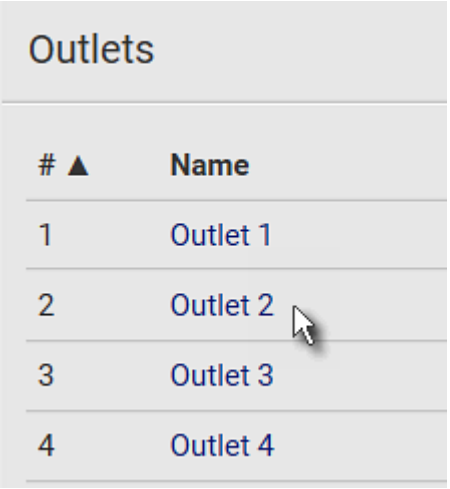
Available Data of the Outlets Overview Page

All of the following outlet data is displayed on the outlets overview page based on your selection. To show or hide specific data, click . See *Outlets* (on page 70).

- Receptacle type
- Lines associated with each outlet

Individual Outlet Pages

An outlet's data/setup page is opened after clicking the outlet's name on the Outlets overview page. See *Outlets* (on page 70).

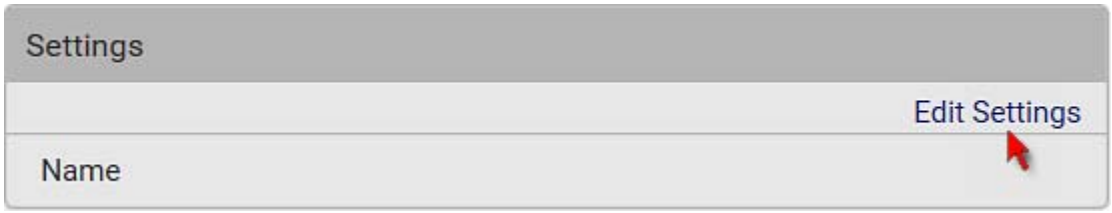


The individual outlet's page shows this outlet's detailed information. See *Detailed Information on Outlet Pages* (on page 72).

In addition, you can perform the following operations on this outlet page.

▶ **To configure this outlet:**

1. Click Edit Settings.

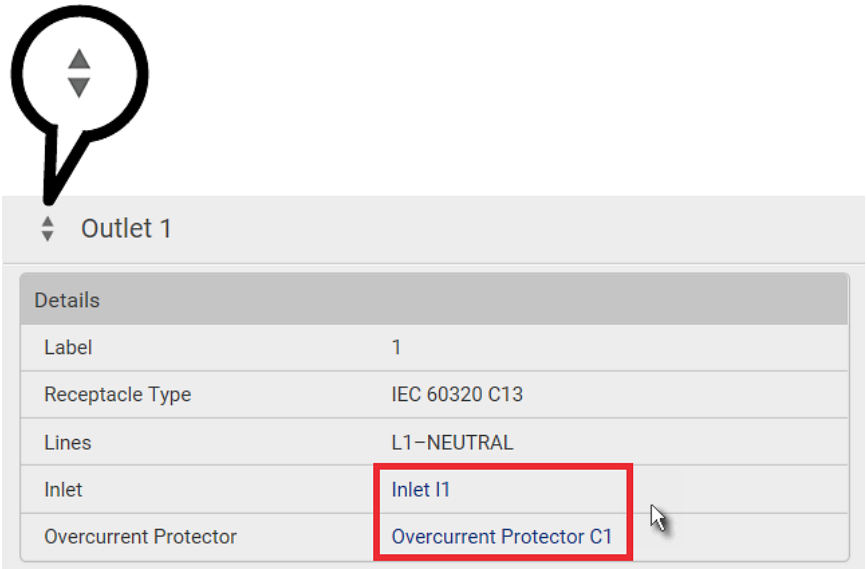


2. Specify the outlet name.
   - Type an outlet name up to 32 characters long.
3. Click Save.

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

Other operations:

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



Detailed Information on Outlet Pages

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

Details section:

Field	Description
Label	The physical outlet number
Receptacle Type	This outlet's receptacle type
Lines	Lines associated with this outlet
Inlet	Inlet associated with this outlet

Field	Description
Overcurrent Protector	This information is available only when your PXE has overcurrent protectors. Overcurrent protector associated with this outlet

OCPs

This page is available only when your PXE has overcurrent protectors, such as circuit breakers.

The OCPs page lists all overcurrent protectors as well as their data.

To open the OCPs page, click 'OCPs' in the *Menu* (on page 53).

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

If wanted, you can resort the list by clicking the desired column header. See *Sorting a List* (on page 55).

Individual OCP Pages

An OCP's data/setup page is opened after clicking any OCP's name on the OCPs page. See *OCPs* (on page 73).

General OCP information:

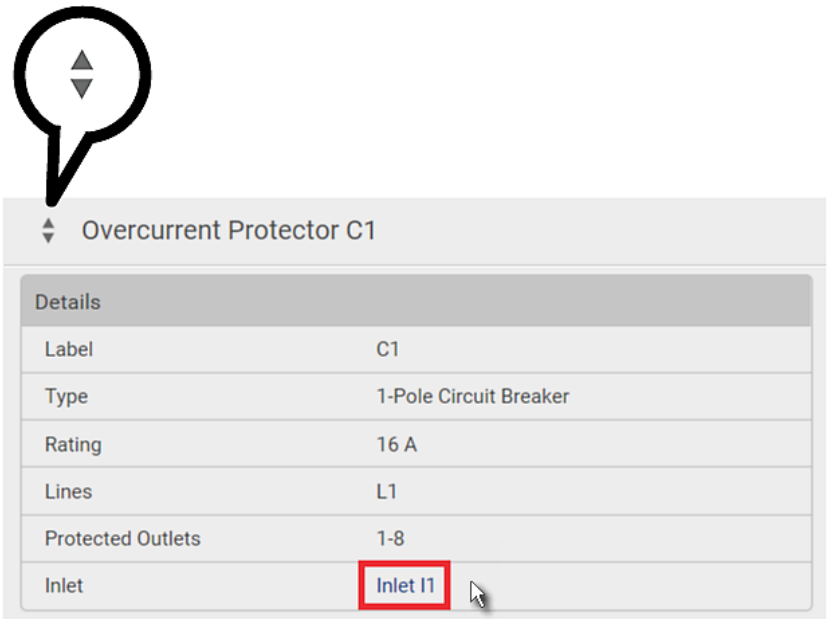
Field	Description
Label	This OCP's physical number
Type	This OCP's type
Rating	This OCP's rated current
Lines	Lines associated with this OCP
Protected Outlets	Outlets associated with this OCP
Inlet	Inlet associated with this OCP This information is useful only when your PDU has multiple inlets.

To customize this OCP's name:

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

Other operations:

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



Peripherals

If there are Raritan environmental sensor packages connected to the PXE, they are listed on the Peripherals page. See *Connecting Environmental Sensor Packages* (on page 20).

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

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

The PXE communicates with *managed* sensors/actuators only and retrieves their data. It does not communicate with unmanaged ones. See *Managed vs Unmanaged Sensors/Actuators* (on page 82).

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

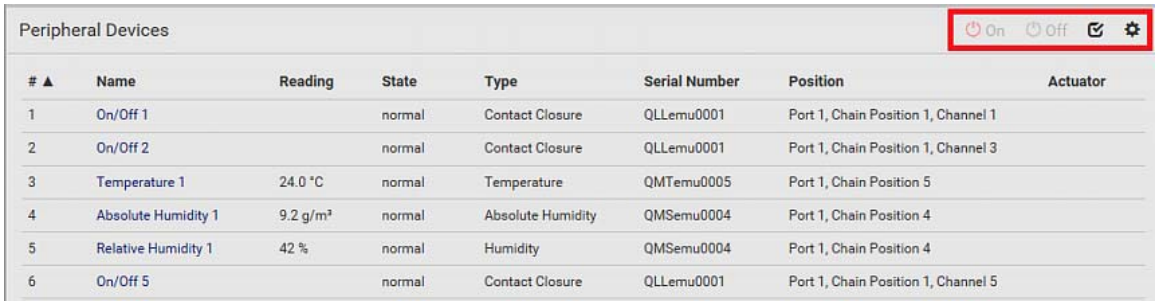
One PXE can manage a maximum of 32 sensors/actuators.

Note: To disable the automatic management function, go to PDU *(on page 65). You need to manually manage a sensor/actuator only when it is not under management.*

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

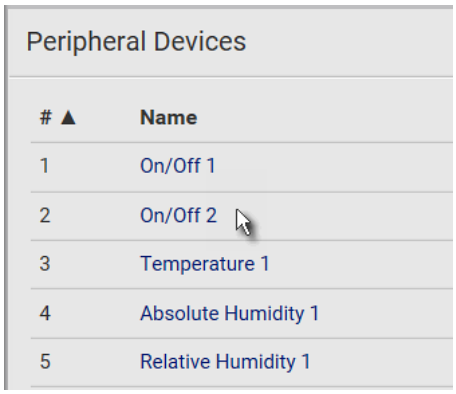
Open the Peripherals page by clicking Peripherals in the *Menu* (on page 53). Then you can:

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



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

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



If wanted, you can resort the list by clicking the desired column header. See *Sorting a List* (on page 55).

Sensor/actuator overview on this page:

If any sensor enters the alarmed state, it is highlighted in yellow or red. See *Yellow- or Red-Highlighted Sensors* (on page 81). An actuator is never highlighted.

Column	Description
Name	By default the PXE assigns a name comprising the following two elements to a newly-managed sensor/actuator. ▪ Sensor/actuator type, such as "Temperature" or "Dry Contact." ▪ Sequential number of the same sensor/actuator type, like 1, 2, 3 and so on. You can customize the name. See *Individual Sensor/Actuator Pages* (on page 89).
Reading	Only managed 'numeric' sensors show this data, such as temperature and humidity sensors.
State	The data is available for all sensors and actuators. See *Sensor/Actuator States* (on page 83).
Type	Sensor or actuator type.

Column	Description
Serial Number	This is the serial number printed on the sensor package's label. It helps to identify your Raritan sensors/actuators. See *Finding the Sensor's Serial Number* (on page 85).
Position	The data indicates where this sensor or actuator is located in the sensor chain. See *Identifying the Sensor Position and Channel* (on page 86).
Actuator	Indicates whether this sensor package is an actuator or not. If yes, the symbol ✔ is shown.

To release or manage sensors/actuators:

When the total of managed sensors/actuators reaches the maximum (32), you cannot manage additional ones. The only way to manage any sensor/actuator is to release or replace any managed ones. To replace a managed sensor/actuator, see *Managing One Sensor or Actuator* (on page 87). To release any one, follow this procedure.

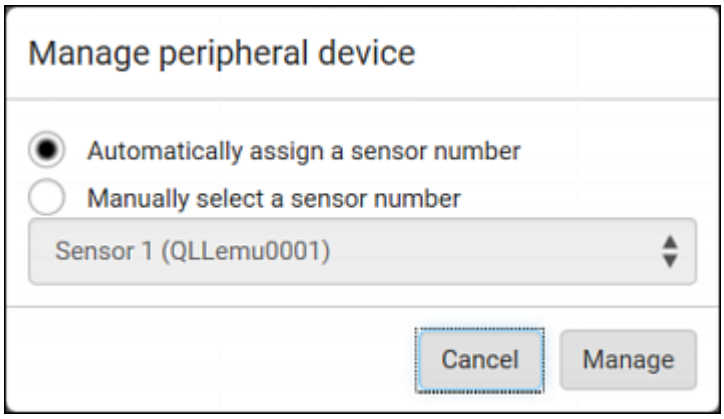
1. Click to make checkboxes appear in front of sensors/actuators.

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

2. Select multiple sensors/actuators.
   - To release sensors/actuators, you must only select "managed" ones. See *Sensor/Actuator States* (on page 83).
   - To manage sensors/actuators, you must only select "unmanaged" ones.
   - To select ALL sensors/actuators, select the topmost checkbox in the header row.
3. To release selected ones, click > Release.

   To manage them, click > Manage.

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



- If you are managing only *one* sensor/actuator, you can choose to assign an ID number by selecting "Manually select a sensor number." See ***Managing One Sensor or Actuator*** (on page 87).

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

   Managed ones show one of the managed states.

To configure default threshold settings:

Note that any changes made to default threshold settings not only re-determine the initial threshold values applying to newly-added sensors but also the threshold values of the already-managed sensors where default thresholds are being used. See ***Individual Sensor/Actuator Pages*** (on page 89).

1. Click ⚙ > Default Threshold Setup.

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

Peripherals Default Thresholds

Edit Thresholds

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

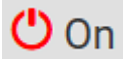
3. Make changes as needed.
   - To enable any threshold, select the corresponding checkbox.
   - Type a new value in the accompanying text box.

   For concepts of thresholds, deassertion hysteresis and assertion timeout, see ***Sensor Threshold Settings*** (on page 446).
4. Click Save.

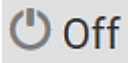
Tip: To customize the threshold settings on a per-sensor basis, go to **Individual Sensor/Actuator Pages** *(on page 89).*

To turn on or off any actuator(s):

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

: Turn ON.

: Turn OFF.
3. Confirm the operation when prompted.

Yellow- or Red-Highlighted Sensors

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

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

For concepts of thresholds, deassertion hysteresis and assertion timeout, see ***Sensor Threshold Settings*** (on page 446).

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

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

Sensor status	Color	States shown in the interface	Description
Unknown		unavailable	Sensor state or readings cannot be detected.
		unmanaged	Sensors are not being managed. See ***Managed vs Unmanaged Sensors/Actuators*** (on page 82).
Normal		normal	▪ Numeric or state sensors are within the normal range. -- OR -- ▪ No thresholds have been enabled for numeric sensors.
Warning		above upper warning	Upper Warning threshold < "R" <= Upper Critical threshold
		below lower warning	Lower Critical threshold <= "R" < Lower Warning threshold
Critical		above upper critical	Upper Critical threshold < "R"
		below lower critical	"R" < Lower Critical threshold

Sensor status	Color	States shown in the interface	Description
Alarmed		alarmed	State sensors enter the abnormal state.
OCP alarm		Open	▪ Circuit breaker trips. -- OR -- ▪ Fuse blown.

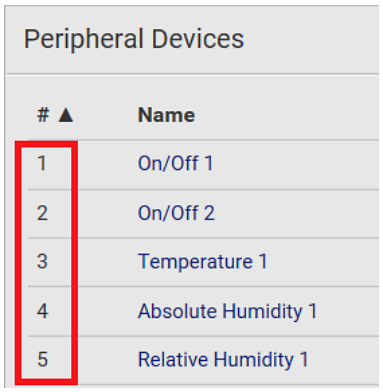
If you have connected a Schroff® LHX/SHX heat exchanger, when any sensor implemented on that device fails, it is also highlighted in red.

Managed vs Unmanaged Sensors/Actuators

To manually manage or unmanage/release a sensor or actuator, see *Peripherals* (on page 76).

Managed sensors/actuators:

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



- They show one of the managed states. See ***Sensor/Actuator States*** (on page 83).
- For managed 'numeric' sensors, their readings are retrieved and displayed. If any numeric sensor is disconnected or its reading cannot be retrieved, it shows "unavailable" for its reading.

Unmanaged sensors/actuators:

- The PXE neither communicates with unmanaged sensors/actuators nor retrieves their data.
- Unmanaged sensors/actuators are listed only when they are physically connected to the PXE. They disappear when they are no longer connected.
- They do *not* have an ID number.
- They show the "unmanaged" state.

Sensor/Actuator States

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

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

Sensors will be highlighted in yellow or red when they enter abnormal states. See ***Yellow- or Red-Highlighted Sensors*** (on page 81).

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

Managed sensor states:

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

State	Description
normal	▪ For numeric sensors, it means the readings are within the normal range. ▪ For state sensors, it means they enter the normal state.
below lower critical	"R" < Lower Critical threshold
below lower warning	Lower Critical threshold <= "R" < Lower Warning threshold
above upper warning	Upper Warning threshold < "R" <= Upper Critical threshold
above upper critical	Upper Critical threshold < "R"

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

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

▶ **Managed actuator states:**

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

▶ **Unmanaged sensor/actuator states:**

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

Note: Unmanaged sensors or actuators will disappear from the web interface after they are no longer physically connected to the PXE. To manage a sensor/actuator, go to **Peripherals** *(on page 76).*

Finding the Sensor's Serial Number

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

A DPX2, DPX3 or DX sensor package has a serial number tag attached to its rear side.

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

Peripheral Devices

On Off

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

Identifying the Sensor Position and Channel

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

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

Peripheral Devices

On Off

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

- DPX series only shows the sensor port number only.

  For example, *Port 1*.
- DPX2, DPX3 and DX series show both the sensor port number and its position in a sensor chain.

  For example, *Port 1, Chain Position 2*.
- If a Raritan DPX3-ENVHUB4 sensor hub is involved, the hub port information is also indicated for DPX2, DPX3 and DX series, but NOT indicated for DPX series.

  For example, *Hub Port 3*.
- If a sensor/actuator contains channels, such as a contact closure or dry contact sensor, the channel information is included in the position information.

  For example, *Channel 1*.

▶ **Sensor/actuator position examples:**

Example	Physical position
Port 1	Connected to the sensor port #1.
Port 1, Channel 2	▪ Connected to the sensor port #1. ▪ The sensor/actuator is the 2nd channel of the sensor package.
Port 1, Chain Position 4	▪ Connected to the sensor port #1. ▪ The sensor/actuator is located in the 4th sensor package of the sensor chain.
Port 1, Chain Position 3, Channel 2	▪ Connected to the sensor port #1. ▪ The sensor/actuator is located in the 3rd sensor package of the sensor chain. ▪ It is the 2nd channel of the sensor package.

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

Managing One Sensor or Actuator

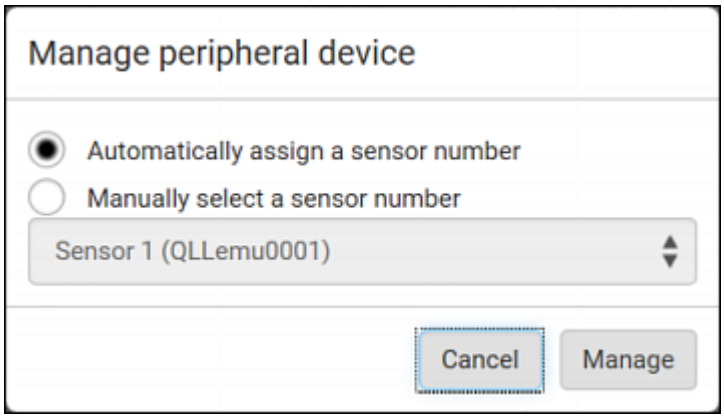
If you are managing only one sensor or actuator, you can assign the desired ID number to it. Note that you cannot assign ID numbers when you are managing multiple sensors/actuators at a time.

Tip: When the total of managed sensors/actuators reaches the maximum (32), you cannot manage additional ones. The only way to manage any sensor/actuator is to release or replace any managed ones. To replace a managed one, assign an ID number to it by following this procedure. To release any one, see Peripherals *(on page 76).*

To manage only one sensor/actuator:

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

2. The "Manage peripheral device" dialog appears.



   - To let the PXE randomly assign an ID number to it, select "Automatically assign a sensor number."

     This method does not release any managed sensor or actuator.
   - To assign the desired ID number to it, select "Manually select a sensor number." Then click ▲▼ to select an ID number.

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

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

3. Click Manage.

Special note for a Raritan humidity sensor:

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

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

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

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

Peripheral Devices

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

Individual Sensor/Actuator Pages

A sensor's or actuator's data/setup page is opened after clicking any sensor or actuator name on the Peripheral Devices page. See *Peripherals* (on page 76).

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

Threshold settings, if enabled, help you identify whether any numeric sensor enters the warning or critical level. See *Yellow- or Red-Highlighted Sensors* (on page 81). In addition, you can have the PXE automatically generate alert notifications for any warning or critical status. See *Event Rules and Actions* (on page 146).

To configure a numeric sensor's threshold settings:

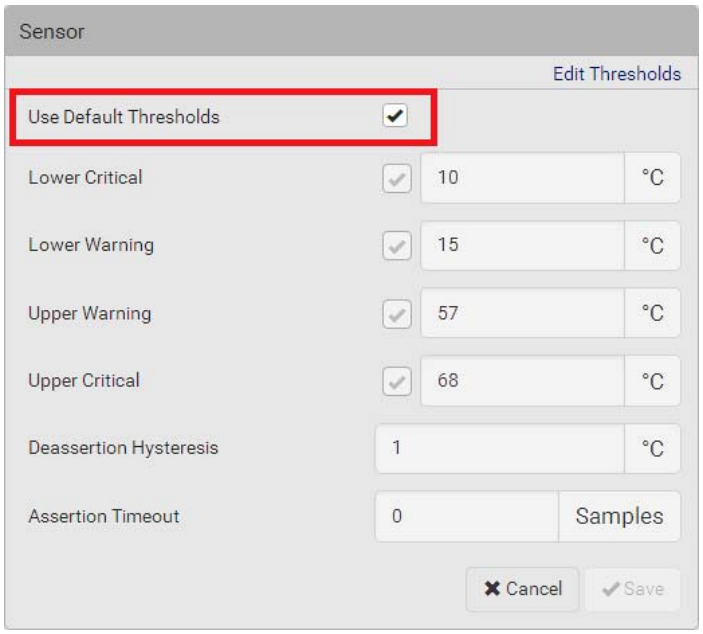
1. Click Edit Thresholds.

Sensor

Edit Thresholds

Reading	24.7 °C
State	normal
Last Time Changed	2/18/2017, 5:48:21 PM

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



- To have this sensor follow the default threshold settings configured for its sensor type, select the Use Default Thresholds checkbox.

  The default threshold settings are configured on the page of ***Peripherals*** (on page 76).
- To customize the threshold settings for this particular sensor, deselect the Use Default Thresholds checkbox, and then modify the threshold fields below it.

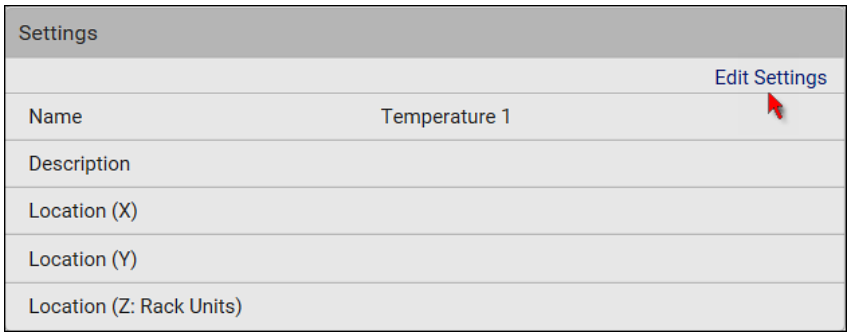
Note: For concepts of thresholds, deassertion hysteresis and assertion timeout, see **Sensor Threshold Settings** *(on page 446).*

---

3. Click Save.

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

1. Click Edit Settings.

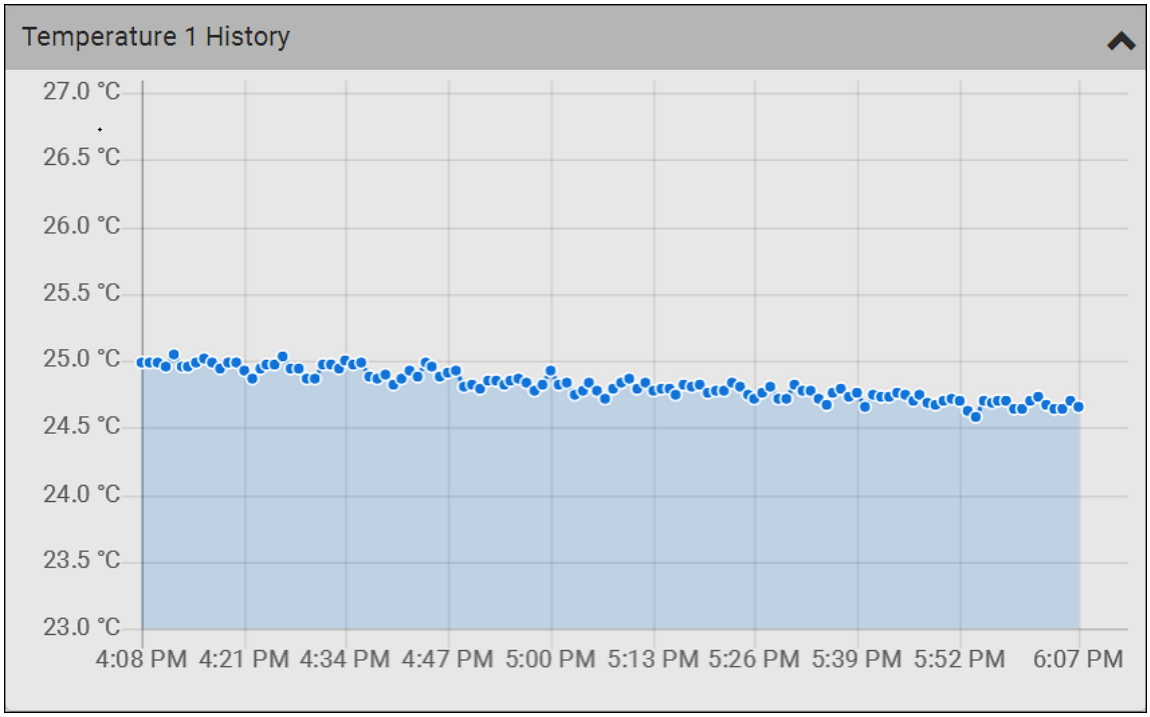


2. Make changes to available fields, and then click Save.

Fields	Description
Binary Sensor Subtype	This field is available for a contact closure sensor only. Determine the sensor type of your contact closure detector. ▪ *Contact Closure* detects the door lock or door open/closed status. ▪ *Smoke Detection* detects the appearance of smoke. ▪ *Water Detection* detects the appearance of water on the floor. ▪ *Vibration* detects the vibration of the floor.
Name	A name for the sensor or actuator.
Description	Any descriptive text you want.
Location (X, Y and Z)	Describe the sensor's or actuator's location in the data center by typing alphanumeric values for the X, Y and Z coordinates. See ***Sensor/Actuator Location Example*** (on page 93). If the term "Rack Units" appears in parentheses in the Z location, you must type an integer number. Note that the Z coordinate's format is determined on the page of ***PDU*** (on page 65).
Alarmed to Normal Delay	This field is available for the DX-PIR presence detector only. It determines the wait time before the PXE announces that the presence detector is back to normal after it actually returns to normal. Adjust the value in seconds.

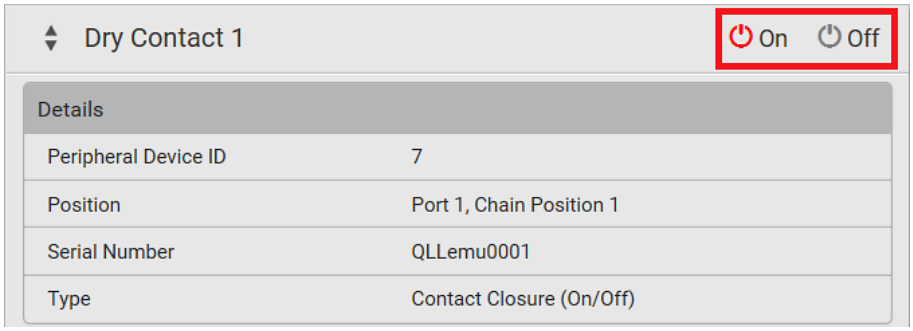
To view a numeric sensor's readings waveform:

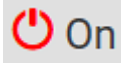
This sensor's data within the past tens of minutes is shown in the waveform diagram. Note that only a numeric sensor has this diagram. State sensors and actuators do not show such data.



To turn on or off an actuator:

1. Click the desired control button.





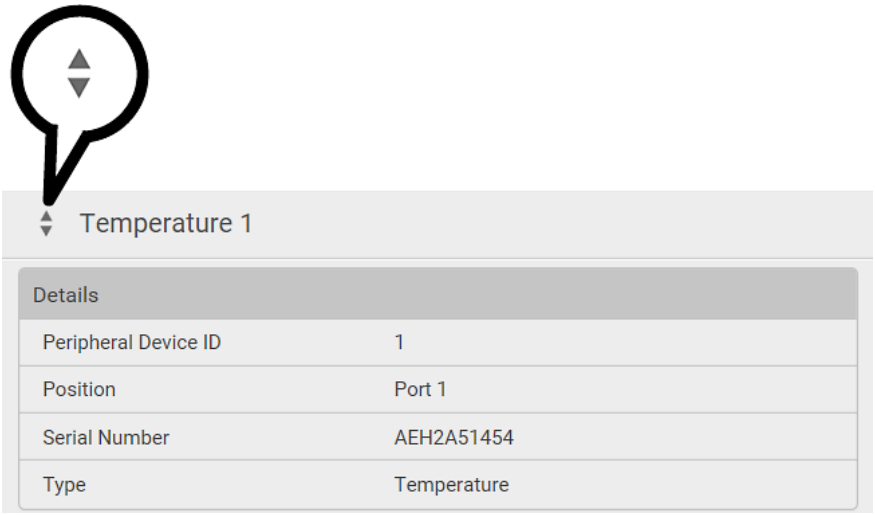
: Turn ON.

: Turn OFF.

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

Other operations:

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



Sensor/Actuator Location Example

Use the X, Y and Z coordinates to describe each sensor's or actuator's physical location in the data center. See *Individual Sensor/Actuator Pages* (on page 89).

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

Example:

X = `Brown Cabinet Row`

Y = `Third Rack`

Z = `Top of Cabinet`

Values of the X, Y and Z coordinates:

- X and Y: They can be any alphanumeric values comprising 0 to 24 characters.
- Z: When the Z coordinate format is set to *Rack Units*, it can be any number ranging from 0 to 60. When its format is set to *Free-Form*, it can be any alphanumeric value comprising 0 to 24 characters. See *PDU* (on page 65).

User Management

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

The PXE is shipped with one built-in administrator account: **admin**, which is ideal for initial login and system administrator. You can neither delete 'admin' nor change its permissions.

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

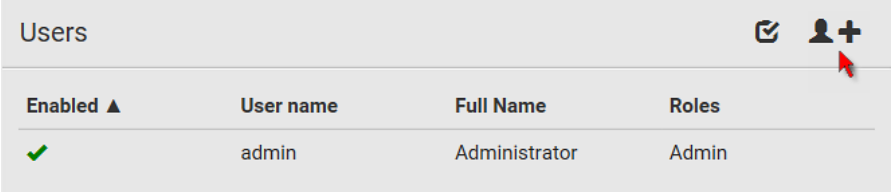
Click 'User Management' in the *Menu* (on page 53), and the following submenu displays.

Submenu command	Refer to...
Users	*Creating Users* (on page 94)
Roles	*Creating Roles* (on page 99)
Change Password	*Changing Your Password* (on page 50)
Preferences	*Setting Your Preferred Measurement Units* (on page 102)
Default Preferences	*Setting Default Measurement Units* (on page 102)

Creating Users

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

To add users, choose User Management > Users > .



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

User information:

Field/setting	Description
User Name	The name the user enters to log in to the PXE. ▪ 4 to 32 characters ▪ Case sensitive ▪ Spaces are NOT permitted.
Full Name	The user's first and last names.
Password, Confirm Password	▪ 4 to 64 characters ▪ Case sensitive ▪ Spaces are permitted.
Telephone Number	The user's telephone number
eMail Address	The user's email address ▪ Up to 64 characters ▪ Case sensitive
Enable	When selected, the user can log in to the PXE.
Force password change on next login	When selected, a password change request automatically appears when next time the user logs in. For details, see *Changing Your Password* (on page 50).

SSH:

You need to enter the SSH public key only if the public key authentication for SSH is enabled. See *Changing SSH Settings* (on page 118).

1. Open the SSH public key with a text editor.
2. Copy and paste all content in the text editor into the SSH Public Key field.

SNMPv3:

The SNMPv3 access permission is disabled by default.

Field/setting	Description
Enable SNMPv3	Select this checkbox when intending to permit the SNMPv3 access by this user. *Note: The SNMPv3 protocol must be enabled for SNMPv3 access. See* **Configuring SNMP Settings**

Field/setting	Description
	(on page 115).
Security Level	Click the field to select a preferred security level from the list: ▪ None: No authentication and no privacy. This is the default. ▪ Authentication: Authentication and no privacy. ▪ Authentication & Privacy: Authentication and privacy.

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

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

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

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

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

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

Preferences:

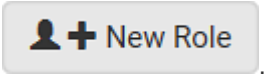
This section determines the measurement units displayed in the web interface and command line interface for this user.

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

Note: Users can change the measurement units at any time by setting their own preferences. See **Setting Your Preferred Measurement Units** *(on page 102).*

Roles:

Select one or multiple roles to determine the user's permissions. To select all roles, select the top-most checkbox in the header row.

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

. See ***Creating Roles*** (on page 99).

The Operator role is assigned to a newly-created user account by default.

Built-in role	Description
Admin	Provide full permissions.
Operator	Provide frequently-used permissions, including: • Acknowledge Alarms • Change Own Password • Change Pdu, Inlet, Outlet & Overcurrent Protector Configuration • View Event Settings • View Local Event Log

Note: With multiple roles selected, a user has the union of all roles' permissions.

Editing or Deleting Users

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

In the Enabled column:

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

If wanted, you can resort the list by clicking the desired column header. See ***Sorting a List*** (on page 55).

To edit or delete a user account:

1. On the Users page, click the desired user. The Edit User page for that user opens.
2. Make changes as needed.

- For information on each field, see *Creating Users* (on page 94).
- To change the password, type a new password in the Password and Confirm Password fields. If the password field is left blank, the password remains unchanged.
- To delete this user, click , and confirm the operation.

3. Click Save.

To delete multiple user accounts:

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

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

2. Select one or multiple users.
   - To select all roles, except for the admin role, select the top-most checkbox in the header row.
3. Click .
4. Click Delete on the confirmation message.

Creating Roles

A role is a combination of permissions. Each user must have at least one role.

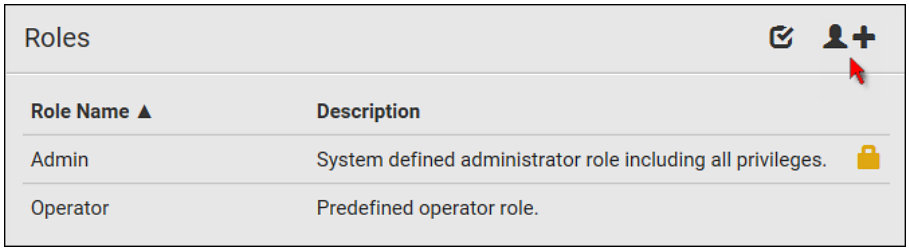
The PXE provides two built-in roles. The Operator role is assigned to a newly-created user account per default. See *Creating Users* (on page 94).

Built-in role	Description
Admin	Provide full permissions.
Operator	Provide frequently-used permissions, including: • Acknowledge Alarms • Change Own Password • Change Pdu, Inlet, Outlet & Overcurrent Protector Configuration • View Event Settings • View Local Event Log

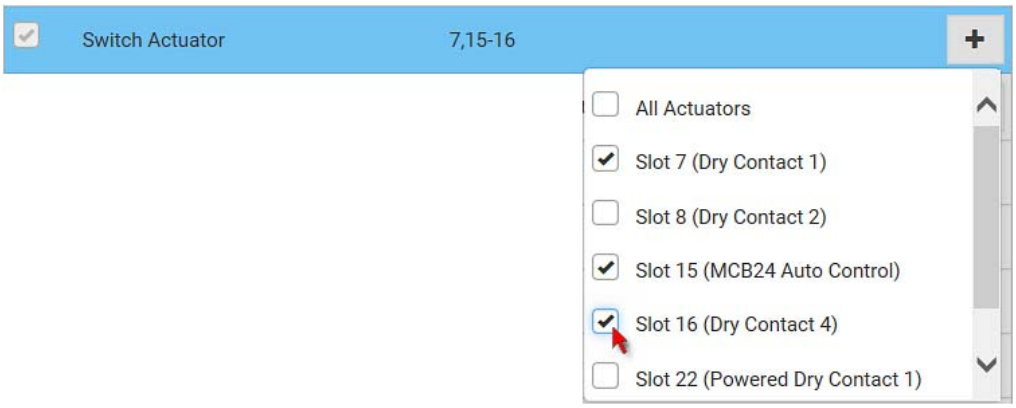
If the two do not satisfy your needs, add new roles.

To create a role:

1. Choose User Management > Roles > .



2. Assign a role name.
   - 1 to 32 characters long
   - Case sensitive
   - Spaces are permitted as of release 3.3.0
3. Type a description for the role in the Description field.
4. Select the desired privilege(s).
   - The 'Administrator Privileges' includes all privileges.
   - The 'Unrestricted View Privileges' includes all 'View' privileges.
5. To select any privilege requiring the argument setting, click to select the desired arguments.
   - For example, you can specify the actuators that are allowed to be switched on/off for the 'Switch Actuator' privilege as shown below.



6. Click Save.

Now you can assign the role to any user. See *Creating Users* (on page 94) or *Editing or Deleting Users* (on page 98).

Editing or Deleting Roles

Choose User Management > Roles to open the Roles page, which lists all roles.

If wanted, you can resort the list by clicking the desired column header. See *Sorting a List* (on page 55).

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

To edit a role:

1. On the Roles page, click the desired role. The Edit Role page opens.
2. Make changes as needed.
   - The role name cannot be changed.
   - To delete this role, click , and confirm the operation.
3. Click Save.

To delete any roles:

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

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

2. Select one or multiple roles.
   - To select all roles, except for the Admin role, select the top-most checkbox in the header row.
3. Click on the top-right corner.
4. Click Delete on the confirmation message.

Setting Your Preferred Measurement Units

You can change the measurement units shown in the PXE user interface according to your own preferences regardless of the permissions you have.

Tip: Preferences can also be changed by administrators for specific users on the Edit User page. See **Editing or Deleting Users** *(on page 98).*

Measurement unit changes only apply to the web interface and command line interface.

Setting your own preferences does not change the default measurement units. See ***Setting Default Measurement Units*** (on page 102).

To select the measurement units you prefer:

1. Choose User Management > Preferences.
2. Make changes as needed.

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

3. Click Save.

Setting Default Measurement Units

Default measurement units are applied to all PXE user interfaces across all users, including users accessing the PXE via external authentication servers. For a list of affected user interfaces, see ***User Interfaces Showing Default Units*** (on page 103).

Note: The preferred measurement units set by any individual user or by the administrator on a per-user basis will override the default units in the web interface and command line interface. See **Setting Your Preferred Measurement Units** *(on page 102) or* **Creating Users** *(on page 94).*

To set up default user preferences:

1. Click User Management > Default Preferences.

2. Make changes as needed.

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

3. Click Save.

User Interfaces Showing Default Units

Default measurement units will apply to the following user interfaces or information:

- Web interface for "newly-created" local users when they have not configured their own preferred measurement units. See ***Creating Users*** (on page 94).
- Web interface for users who are authenticated via LDAP/Radius servers.
- The sensor report sent because of the "Send Sensor Report" action. See ***Send Sensor Report*** (on page 164).

Device Settings

Click 'Device Settings' in the ***Menu*** (on page 53), and the following submenu displays.

Menu command	Submenu command	Refer to...
Network		***Configuring Network Settings*** (on page 104)
Network Services	HTTP	***Changing HTTP(S) Settings*** (on page 114)
	SNMP	***Configuring SNMP Settings*** (on page 115)
	SMTP Server	***Configuring SMTP Settings*** (on page 116)
	SSH	***Changing SSH Settings*** (on page 118)
	Telnet	***Changing Telnet Settings*** (on page 119)
	Modbus	***Changing Modbus Settings*** (on page 119)
	Server Advertising	***Enabling Service Advertising*** (on page 120)

Menu command	Submenu command	Refer to...
Security	IP Access Control	*Creating IP Access Control Rules* (on page 121)
	Role Access Control	*Creating Role Access Control Rules* (on page 124)
	SSL Certificate	*Setting Up an SSL/TLS Certificate* (on page 126)
	Authentication	*Setting Up External Authentication* (on page 131)
	Login Settings	*Configuring Login Settings* (on page 140)
	Password Policy	*Configuring Password Policy* (on page 142)
	Service Agreement	*Enabling the Restricted Service Agreement* (on page 143)
Date/Time		*Setting the Date and Time* (on page 143)
Event Rules		*Event Rules and Actions* (on page 146)
Data Logging		*Setting Data Logging* (on page 180)
Data Push		*Configuring Data Push Settings* (on page 181)
Server Reachability		*Monitoring Server Accessibility* (on page 183)
Serial Port		The PXE does NOT have the serial port. You can ignore this feature.
Lua Scripts		*Lua Scripts* (on page 187)
Miscellaneous		*Miscellaneous* (on page 192)

Configuring Network Settings

Configure wired networking and Internet protocol-related settings on the Network page after *Connecting the PXE to Your Network* (on page 11).

To set up the network settings:

1. Choose Device Settings > Network.
2. To use DHCP-assigned DNS servers and gateway instead of static ones, go to step 3. To manually specify DNS servers and default gateway, configure the Common Network Settings section. See *Common Network Settings* (on page 107).

   Static routes and cascading mode are also in this section.

- For the cascading mode, leave it to the default option 'None' because the PXE does NOT have the USB-A port to cascade another PXE. For information on the cascading feature other Raritan PDUs support, refer to the Cascading Guide on Raritan website's ***Support page*** (***http://www.raritan.com/support/***).
- For static routes, you need to configure them only when there are such local requirements. See ***Static Route Examples*** (on page 110).

3. To configure IPv4/IPv6 settings for a *wired* network, click the ETHERNET or BRIDGE section. See ***Wired Network Settings*** (on page 106).
   - If the device's cascading mode is set to 'Bridging', the BRIDGE section appears. Then you must click the BRIDGE section for IPv4/IPv6 settings. However, it is strongly recommended that you do NOT change the cascading mode since PXE PDUs cannot be cascaded due to absence of the USB-A port.
4. The PXE does NOT support any wireless networking so you can ignore the WIRELESS section.
5. To configure the ETHERNET interface settings, see ***Ethernet Interface Settings*** (on page 108).
6. Click Save.

▶ After enabling either or both Internet protocols:

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

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

Note: The PXE supports TLS 1.0, 1.1 *and* 1.2.

Wired Network Settings

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

If the device's cascading mode is set to 'Bridging', the BRIDGE section appears. Then you must click the BRIDGE section for IPv4/IPv6 settings. However, it is recommended that you do not change the cascading mode since PXE does NOT have the USB-A port to support the cascading feature.

Enable Interface:

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

Enable Interface ☑

IPv4 settings:

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

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

  Example: *192.168.84.99/24*

IPv6 settings:

Field/setting	Description
Enable IPv6	Enable or disable the IPv6 protocol.
IP Auto	Select the method to configure IPv6 settings.

Field/setting	Description
Configuration	▪ Automatic: Auto-configure IPv6 settings via DHCPv6. ▪ Static: Manually configure the IPv6 settings.

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

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

Common Network Settings

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

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

Field	Description
IPv4/IPv6 Routes	You need to configure these settings only when your local network contains two subnets, and you want PXE to communicate with the other subnet. If so, make sure IP forwarding has been enabled in your network, and then you can click 'Add Route' to add static routes. See *Static Route Examples* (on page 110).

Ethernet Interface Settings

By default the Ethernet interface is enabled.

Enable Interface:

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

Enable Interface ☑

Other Ethernet settings:

Field	Description
Speed	Select a LAN speed. • Auto: System determines the optimum LAN speed through auto-negotiation. • 10 MBit/s: Speed is always 10 Mbps. • 100 MBit/s: Speed is always 100 Mbps.
Duplex	Select a duplex mode. • Auto: The 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.

Field	Description
Current State	Show the LAN's current status, including the current speed and duplex mode.

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

Static Route Examples

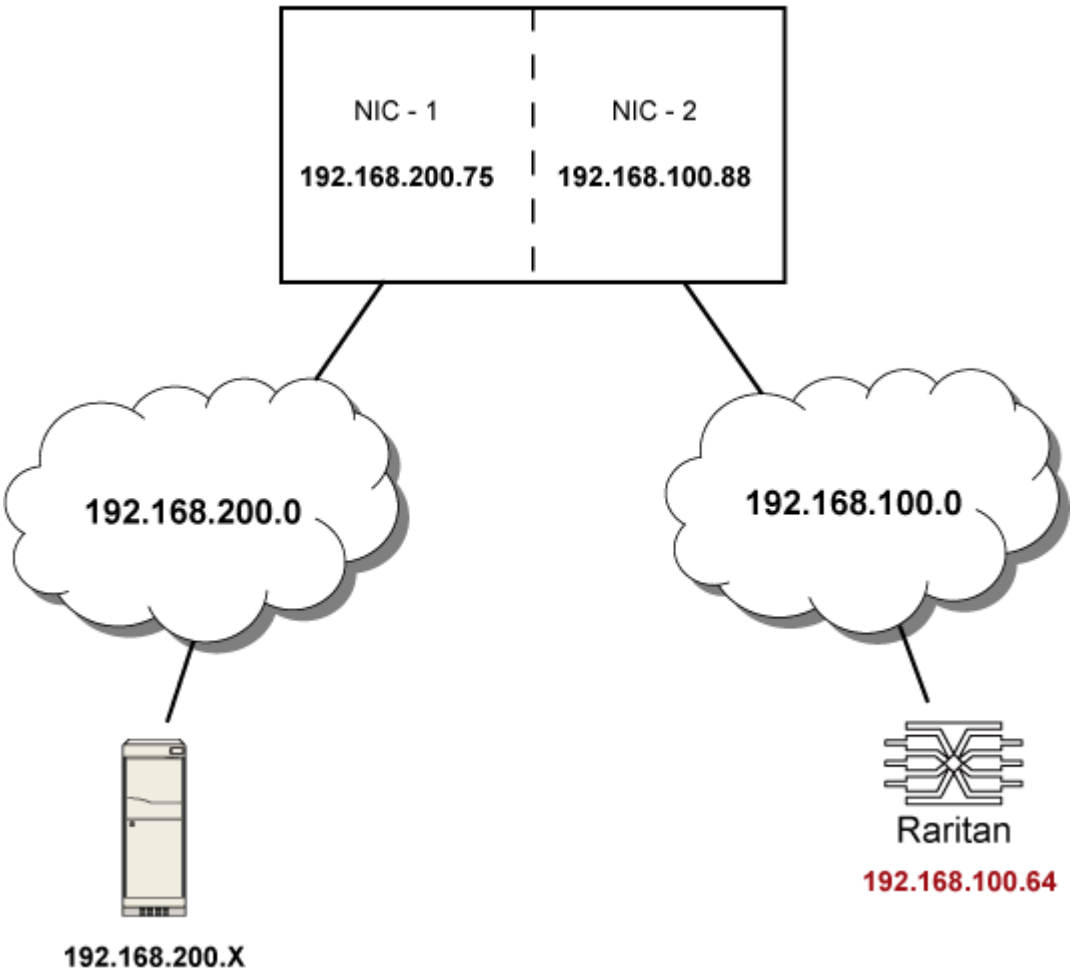
This section describes two static route examples: IPv4 and IPv6. Both examples assume that two network interface controllers (NIC) have been installed in one network server, leading to two available subnets, and IP forwarding has been enabled. All of the NICs and PXE devices in the examples use static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

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

Note: If Interface is selected, you should select an interface name instead of entering an IP address. See Interface Names *(on page 113).*

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*

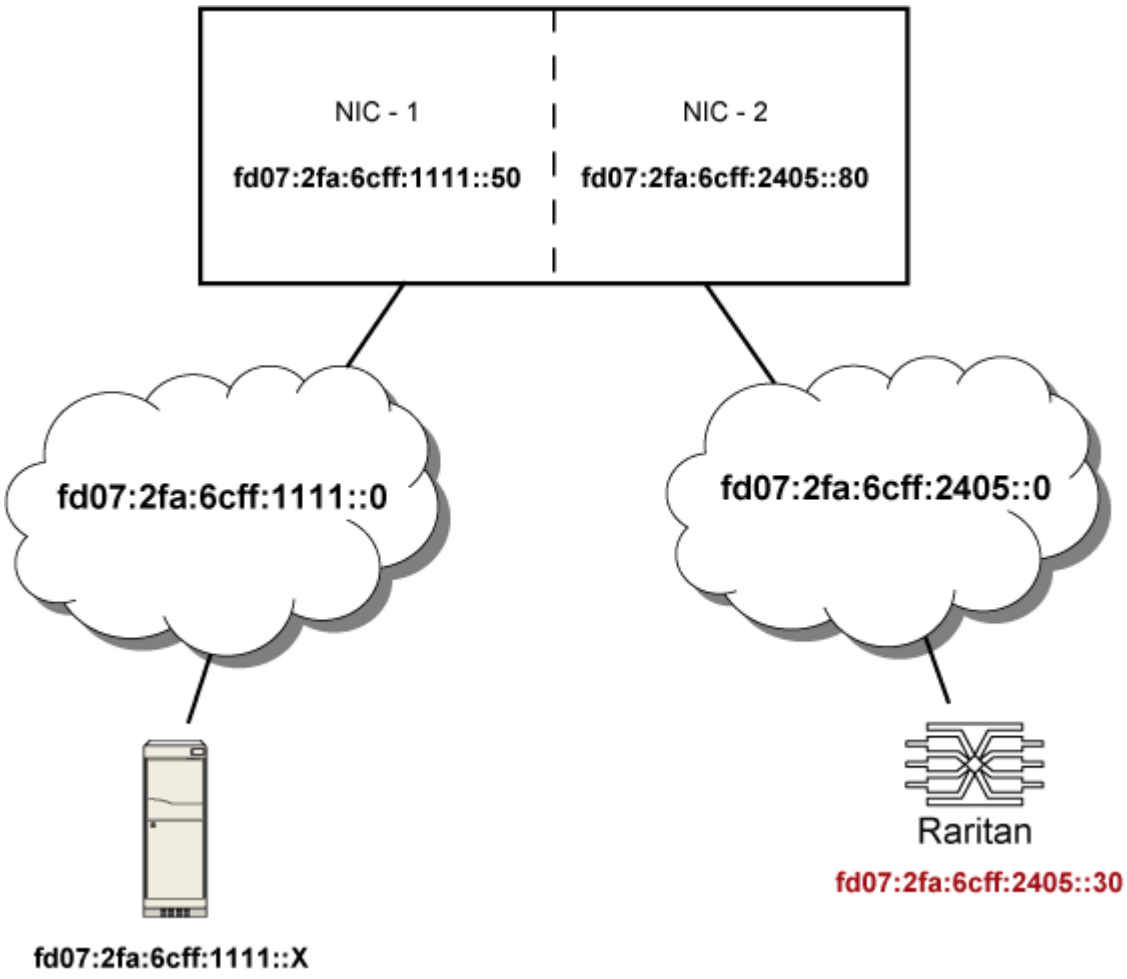


In this example, NIC-2 (192.168.100.88) is the next hop router for your PXE to communicate with any device in the other subnet 192.168.200.0. In the IPv4 "Static Routes" section, you should specify:

Tip: If you have configured multiple static routes, you can click on any route and then make changes, use ↑ or ↓ to re-sort the priority, or click 🗑 to delete it.

▶ IPv6 example:

- Your 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*

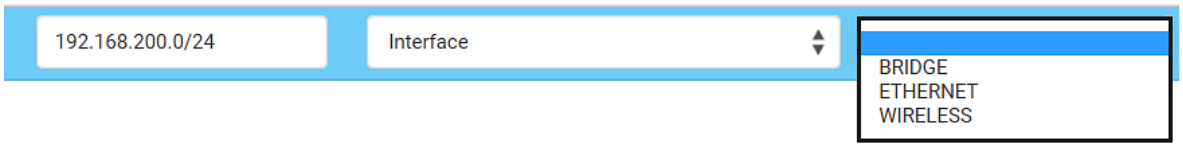


In this example, NIC-2 (fd07:2fa:6cff:2405::80) is the next hop router for your PXE to communicate with any device in the other subnet fd07:2fa:6cff:1111::0. In the IPv6 "Static Routes" section, you should specify:

Tip: If you have configured multiple static routes, you can click on any route and then make changes, use ↑ *or* ↓ *to re-sort the priority, or click* 🗑 *to delete it.*

Interface Names

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



Interface name	Description
BRIDGE	When another wired network is connected to the Ethernet port of your PXE, and your PXE has been set to the bridging mode, select this interface name instead of the Ethernet interface.
ETHERNET	When another wired network is connected to the Ethernet port of your PXE, select this interface name.
WIRELESS	PXE does not support this option because it does not support the wireless networking.

Configuring Network Services

The PXE supports the following network communication services.

HTTPS and HTTP enable the access to the web interface. Telnet and SSH enable the access to the command line interface. See *Using the Command Line Interface* (on page 215).

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

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

Submenu command	Refer to
HTTP	*Changing HTTP(S) Settings* (on page 114)
SNMP	*Configuring SNMP Settings* (on page 115)
SMTP Server	*Configuring SMTP Settings* (on page 116)
SSH	*Changing SSH Settings* (on page 118)
Telnet	*Changing Telnet Settings* (on page 119)
Modbus	*Changing Modbus Settings* (on page 119)
Service Advertising	*Enabling Service Advertising* (on page 120)

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

Changing HTTP(S) Settings

HTTPS uses Transport Layer Security (TLS) technology to encrypt all traffic to and from the PXE so it is a more secure protocol than HTTP. The PXE supports TLS *1.0*, *1.1* and *1.2*.

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

To change HTTP or HTTPS port settings:

1. Choose Device Settings > Network Services > HTTP.
2. Enable either or both protocols by selecting the corresponding 'Enable' checkbox.
3. To use a different port for HTTP or HTTPS, type a new port number.

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

4. To redirect the HTTP access to the PXE to HTTPS, select the "Redirect HTTP connections to HTTPS."
   - The redirection checkbox is configurable only when both HTTP and HTTPS have been enabled.

Special note for AES ciphers:

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

Tip: If intending to force the PXE to use a specific AES cipher, refer to your client's user documentation for information on configuring AES settings. For example, you can enable a cipher and disable the other in the Firefox via the "about:config" command.

Configuring SNMP Settings

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

Besides, you may need to configure the SNMP destination(s) if the built-in "System SNMP Notification Rule" is enabled and the SNMP destination has not been set yet. See ***Event Rules and Actions*** (on page 146).

To configure SNMP communication:

1. Choose Device Settings > Network Services > SNMP.
2. Enable or disable "SNMP v1 / v2c" and/or "SNMP v3" by clicking the corresponding checkbox.
   - The SNMP v1/v2c read-only access is enabled by default. The default Read Community String is 'public.'
   - To enable read-write access, type the Write Community String. Usually the string is 'private.'
3. Enter the MIB-II system group information, if applicable.
   - sysContact - the contact person in charge of the system
   - sysName - the name assigned to the system
   - sysLocation - the location of the system

4. To configure SNMP notifications:
   a. Select the Enable SNMP Notifications checkbox.
   b. Select a notification type -- SNMPv2c Trap, SNMPv2c Inform, SNMPv3 Trap, and SNMPv3 Inform.
   c. Specify the SNMP notification destinations and enter necessary information. For details, refer to:
      - *SNMPv2c Notifications* (on page 208)
      - *SNMPv3 Notifications* (on page 209)

   Note: Any changes made to the 'SNMP Notifications' section on the SNMP page will update the settings of the System SNMP Notification Action, and vice versa. See Available Actions *(on page 158). To add more than three SNMP destinations, you can create new SNMP notification actions. See* Send an SNMP Notification *(on page 165).*

5. You must download the SNMP MIB for your PXE to use with your SNMP manager.
   a. Click the Download MIBs title bar to show the download links.

   b. Click the PDU2-MIB download link. See *Downloading SNMP MIB* (on page 210).
6. Click Save.

Configuring SMTP Settings

The PXE can be configured to send alerts or event messages to a specific administrator by email. See *Event Rules and Actions* (on page 146).

To send emails, you have to configure the SMTP settings and enter an IP address for your SMTP server and a sender's email address.

If any email messages fail to be sent successfully, the failure event and reason are available in the event log. See *Viewing or Clearing the Local Event Log* (on page 196).

▶ To set SMTP server settings:

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

Field	Description
Server Name	Type the name or IP address of the mail server.
Port	Type the port number.

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

- **Settings for the CA Certificate:**

Field/setting	Description
Browse...	Click this button to install a certificate file. Then you can: ▪ Click Show to view the certificate's content. ▪ Click Remove to delete the installed certificate if it is inappropriate.
Allow expired and not yet valid certificates	▪ Select this checkbox to make the authentication succeed regardless of the certificate's validity period. ▪ After deselecting this checkbox, the authentication fails whenever any certificate in the selected certificate chain is outdated or not valid yet.

3. Now that you have set the SMTP settings, you can test it to ensure it works properly.

a. Type the recipient's email address in the Recipient Email Addresses field. Use a comma to separate multiple email addresses.
b. Click Send Test Email.
c. Check if the recipient(s) receives the email successfully.

4. Click Save.

Special note for AES ciphers:

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

Tip: If intending to force the PXE to use a specific AES cipher, refer to your client's user documentation for information on configuring AES settings.

Changing SSH Settings

You can enable or disable the SSH access to the command line interface, change the TCP port, or set a password or public key for login over the SSH connection.

To change SSH settings:

1. Choose Device Settings > Network Services > SSH.
2. To enable or disable the SSH access, select or deselect the checkbox.
3. To use a different port, type a port number.
4. Select one of the authentication methods.
   - Password authentication only: Enables the password-based login only.
   - Public key authentication only: Enables the public key-based login only.
   - Password and public key authentication: Enables both the password- and public key-based login. This is the default.
5. Click Save.

If the public key authentication is selected, you must enter a valid SSH public key for each user profile to log in over the SSH connection. See *Creating Users* (on page 94).

Changing Telnet Settings

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

To change Telnet settings:

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

Changing Modbus Settings

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

To change the Modbus/TCP settings:

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

Enabling Service Advertising

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 (Multicast DNS). The advertised services are discovered by clients that have implemented DNS-SD and MDNS.

The advertised services include the following:

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

By default, this feature is enabled.

Enabling this feature also enables Link-Local Multicast Name Resolution (LLMNR) and/or MDNS, which are required for resolving APIPA host names. See *APIPA and Link-Local Addressing* (on page 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 **Wired Network Settings** *(on page 106).*

To enable or disable service advertising:

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

Configuring Security Settings

The PXE provides tools to control access. You can enable the internal firewall, create firewall rules, and set login limitations. In addition, you can create and install the certificate or set up external authentication servers for access control. This product supports the SHA-2 certificate.

Tip: To force all HTTP accesses to the PXE to be redirected to HTTPS, see **Changing HTTP(S) Settings** *(on page 114).*

Submenu command	Refer to
IP Access Control	***Creating IP Access Control Rules*** (on page 121)
Role Access Control	***Creating Role Access Control Rules*** (on page 124)
SSL Certificate	***Setting Up an SSL/TLS Certificate*** (on page 126)
Authentication	***Setting Up External Authentication*** (on page 131)
Login Settings	***Configuring Login Settings*** (on page 140)
Password Policy	***Configuring Password Policy*** (on page 142)
Service Agreement	***Enabling the Restricted Service Agreement*** (on page 143)

Creating IP Access Control Rules

IP access control 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 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.

- **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.

To configure IPv4 access control rules:

1. Choose Device Settings > Security > IP Access Control.
2. Select the Enable IPv4 Access Control checkbox to enable IPv4 access control rules.
3. Determine the IPv4 default policy.
   - Accept: Accepts traffic from all IPv4 addresses.
   - Drop: Discards traffic from all IPv4 addresses, without sending any failure notification to the source host.
   - Reject: Discards traffic from all IPv4 addresses, and an ICMP message is sent to the source host for failure notification.
4. Go to the Inbound Rules section or the Outbound Rules section according to your needs.
   - Inbound rules control the data sent to the PXE.
   - Outbound rules control the data sent from the PXE.
5. Create rules. See the tables for different operations.

ADD a rule to the end of the list

▪ Click Append.
▪ Type an IP address and subnet mask in the IP/Mask field.
▪ Select an option in the Policy field.
  ▪ Accept: Accepts traffic from/to the specified IP address(es).
  ▪ Drop: Discards traffic from/to the specified IP address(es), without sending any failure notification to the source or destination host.
  ▪ Reject: Discards traffic from/to the specified IP address(es), and an ICMP message is sent to the source or destination host for failure notification.

INSERT a rule between two rules
▪ Select the rule above which you want to insert a new rule. For example, to insert a rule between rules #3 and #4, select #4. ▪ Click Insert Above. ▪ Type an IP address and subnet mask in the IP/Mask field. ▪ Select Accept, Drop or Reject in the Policy field. See the above for their descriptions.

The system automatically numbers the rule.

6. When finished, the rules are listed.

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

7. Click Save. The rules are applied.

To configure IPv6 access control rules:

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

Editing or Deleting IP Access Control Rules

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

To modify or delete a rule:

1. Choose Device Settings > Security > IP Access Control.
2. Go to the IPv4 or IPv6 section.
3. Select the desired rule in the list.
   - Ensure the IPv4 or IPv6 checkbox has been selected, or you cannot edit or delete any rule.
4. Perform the desired action.
   - Make changes to the selected rule, and then click Save. For information on each field, see ***Creating IP Access Control Rules*** (on page 121).
   - Click to remove it.
   - To resort its order, click or .
5. Click Save.
   - IPv4 rules: **Make sure you click the Save button in the IPv4 section**, or the changes made to IPv4 rules are not saved.
   - IPv6 rules: **Make sure you click the Save button in the IPv6 section**, or the changes made to IPv6 rules are not saved.

Creating Role Access Control Rules

Role-based access control rules are similar to IP access control rules, except they are applied to members of a specific role. This enables you to grant system permissions to a specific role, based on their IP addresses.

Same as IP access control rules, the order of role-based access control rules is important, since the rules are executed in numerical order.

To create IPv4 role-based access control rules:

1. Choose Device Settings > Security > Role Access Control.
2. Select the "Enable Role Based Access Control for IPv4" checkbox to enable IPv4 access control rules.
3. Determine the IPv4 default policy.
   - 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.
4. Create rules. See the tables for different operations.

ADD a rule to the end of the list

▪ Click Append.
▪ Type a starting IP address in the Start IP field.
▪ Type an ending IP address in the End IP field.
▪ Select a role in the Role field. This rule applies to members of this role only.
▪ Select an option in the Policy field.
  ▪ 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 a rule between two rules
▪ Select the rule above which you want to insert a new rule. For example, to insert a rule between rules #3 and #4, select #4. ▪ Click Insert Above. ▪ Type a starting IP address in the Start IP field. ▪ Type an ending IP address in the End IP field. ▪ Select a role in the Role field. This rule applies to members of this role only. ▪ Select Allow or Deny in the Policy field. See the above for their descriptions.

The system automatically numbers the rule.

5. When finished, the rules are listed on this page.
   - You can select any existing rule and then click or to change its priority.
6. Click Save. The rules are applied.

To configure IPv6 access control rules:

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

Editing or Deleting Role Access Control Rules

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

To modify a role-based access control rule:

1. Choose Device Settings > Security > Role Access Control.
2. Go to the IPv4 or IPv6 section.
3. Select the desired rule in the list.
   - Ensure the IPv4 or IPv6 checkbox has been selected, or you cannot select any rule.
4. Perform the desired action.
   - Make changes to the selected rule, and then click Save. For information on each field, see *Creating Role Access Control Rules* (on page 124).

- Click to remove it.
- To resort its order, click or .

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

Setting Up an SSL/TLS Certificate

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

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

To obtain a CA-signed certificate:

1. Create a Certificate Signing Request (CSR) on the PXE. See *Creating a CSR* (on page 127).
2. Submit it to a certificate authority (CA). After the CA processes the information in the CSR, it provides you with a certificate.
3. Install the CA-signed certificate onto the PXE. See *Installing a CA-Signed Certificate* (on page 128).

Note: If you are using a certificate that is part of a chain of certificates, each part of the chain is signed during the validation process.

A CSR is not required in either scenario below:

- Make the PXE create a *self-signed* certificate. See *Creating a Self-Signed Certificate* (on page 129).
- Appropriate, valid certificate and key files are already available, and you just need to install them. See *Installing or Downloading Existing Certificate and Key* (on page 130).

Creating a CSR

Follow this procedure to create the CSR for your PXE device.

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

required

▶ To create a CSR:

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

Field	Description
Country	The country where your company is located. Use the standard ISO country code. For a list of ISO codes, visit the *ISO website* (*http://www.iso.org/iso/country_codes/iso_3166_code_lists.htm*).
State or Province	The full name of the state or province where your company is located.
Locality	The city where your company is located.
Organization	The registered name of your company.
Organizational Unit	The name of your department.
Common Name	The fully qualified domain name (FQDN) of your PXE device.
Email Address	An email address where you or another administrative user can be reached.

Warning: If you generate a CSR without values entered in the required fields, you cannot obtain third-party certificates.

   - **Key Creation Parameters:**

Field	Do this
Key Length	Select an available key length (bits). A larger key length enhances the security, but slows down the PXE device's response. ▪ Only 2048 is available now.
Self Sign	**For requesting a certificate signed by the CA, ensure this checkbox is NOT selected.**

Field	Do this
Challenge, Confirm Challenge	Type a password. The password is used to protect the certificate or CSR. This information is optional. The value should be 4 to 64 characters long. Case sensitive.

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

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

   - You are prompted to open or save the file. Click Save to save it onto your computer.
6. After getting the CA-signed certificate, install it. See ***Installing a CA-Signed Certificate*** (on page 128).

Installing a CA-Signed Certificate

To get a certificate from a certificate authority (CA), first create a CSR and send it to the CA. See ***Creating a CSR*** (on page 127).

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

To install the CA-signed certificate:

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

to navigate to the CA-signed certificate file.
3. Click Upload to install it.
4. To verify whether the certificate has been installed successfully, check the data shown in the Active SSL Certificate section.

Creating a Self-Signed Certificate

When appropriate certificate and key files for the PXE device are unavailable, the alternative, other than submitting a CSR to the CA, is to generate a self-signed certificate.

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

required

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

1. Choose Device Settings > Security > SSL Certificate.
2. Enter information.

Field	Description
Country	The country where your company is located. Use the standard ISO country code. For a list of ISO codes, visit the ***ISO website*** (***http://www.iso.org/iso/country_codes/iso_3166_code_lists.htm***).
State or Province	The full name of the state or province where your company is located.
Locality	The city where your company is located.
Organization	The registered name of your company.
Organizational Unit	The name of your department.
Common Name	The fully qualified domain name (FQDN) of your PXE device.
Email Address	An email address where you or another administrative user can be reached.
Key Length	Select an available key length (bits). A larger key length enhances the security, but slows down the PXE device's response. ▪ Only 2048 is available now.
Self Sign	**Ensure this checkbox is selected, which indicates that you are creating a self-signed certificate.**
Validity in days	This field appears after the Self Sign checkbox is selected. Type the number of days for which the self-signed certificate will be valid.

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

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

4. Once complete, do the following:
   a. Double check the data shown in the New SSL Certificate section.
   b. If correct, click "Install Key and Certificate" to install the self-signed certificate and private key.

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

   If incorrect, click "Delete Key and Certificate" to remove the self-signed certificate and private key, and then repeat the above steps to re-create them.
5. (Optional) To download the self-signed certificate and/or private key, click Download Certificate or Download Key in the New SSL Certificate section.
   - You are prompted to open or save the file. Click Save to save it onto your computer.

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

Installing or Downloading Existing Certificate and Key

You can download the already-installed certificate and private key from any PXE for backup or file transfer. For example, you can install the files onto a replacement PXE device, add the certificate to your browser and so on.

If valid certificate and private key files are already available, you can install them on the PXE without going through the process of creating a CSR or a self-signed certificate.

Note: If you are using a certificate that is part of a chain of certificates, each part of the chain is signed during the validation process.

To download active key and certificate files from the PXE:

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

   Note: The Download Key button in the New SSL Certificate section, if present, is for downloading the newly-created private key rather than the one of the currently-installed certificate.
3. You are prompted to open or save the file. Click Save to save it onto your computer.

To install available key and certificate files onto the PXE:

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

Setting Up External Authentication

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

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

- Local user database on the PXE
- 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 only need to create user accounts. See *Creating Users* (on page 94).

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 accounts on the PXE in addition to providing the external AA server 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.

If the external authentication fails, an "Authentication failed" message is displayed. Details regarding the authentication failure are available in the event log. See *Viewing or Clearing the Local Event Log* (on page 196).

Note that only users who have both the "Change Authentication Settings" and "Change Security Settings" permissions can configure or modify the authentication settings.

To enable external authentication:

1. Collect external AA server information. See *Gathering LDAP/Radius Information* (on page 133).
2. Enter required data for external AA server(s) on the PXE. See *Adding LDAP/LDAPS Servers* (on page 134) or *Adding Radius Servers* (on page 137).
   - For illustrations, see *LDAP Configuration Illustration* (on page 391) or *Radius Configuration Illustration* (on page 404).
3. If both the external and local authentication is needed, or you have to return to the local authentication only, see *Managing External Authentication Settings* (on page 139).

Special note about the AES cipher:

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

Tip: If intending to force the PXE to use a specific AES cipher, refer to your client's user documentation for information on configuring AES settings.

Gathering LDAP/Radius Information

It requires knowledge of your AA server settings to configure the PXE for external authentication. If you are not familiar with these settings, consult your AA server administrator for help.

Information needed for LDAP authentication:

- The IP address or hostname of the LDAP server
- Whether the Secure LDAP protocol (LDAP over TLS) is being used
  - If Secure LDAP is in use, consult your LDAP administrator for the CA certificate file.
- The network port used by the LDAP server
- The type of the LDAP server, usually one of the following options:
  - *OpenLDAP*
    - If using an OpenLDAP server, consult the LDAP administrator for the Bind Distinguished Name (DN) and password.
  - *Microsoft Active Directory® (AD)*

  - If using a Microsoft Active Directory server, consult your AD administrator for the name of the Active Directory Domain.
- Bind Distinguished Name (DN) and password (if anonymous bind is NOT used)
- The Base DN of the server (used for searching for users)
- The login name attribute (or AuthorizationString)
- The user entry object class
- The user search subfilter (or BaseSearch)

Information needed for Radius authentication:

- The IP address or host name of the Radius server
- Authentication protocol used by the Radius server
- Shared secret for a secure communication
- UDP authentication port and accounting port used by the Radius server

Adding LDAP/LDAPS Servers

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

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

required

To add LDAP/LDAPS servers:

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

Field/setting	Description
IP Address / Hostname	The IP address or hostname of your LDAP/LDAPS server. ▪ Important: Without the encryption enabled, you can type either the domain name or IP address in this field, but you must type the fully qualified domain name if the encryption is enabled.
Copy settings from existing LDAP server	This checkbox appears only when there are existing AA server settings on the PXE. To duplicate any existing AA server's settings, refer to the duplicating procedure below.

Field/setting	Description
Type of LDAP Server	Choose one of the following options: ▪ OpenLDAP ▪ Microsoft Active Directory. Active Directory is an implementation of LDAP/LDAPS directory services by Microsoft for use in Windows environments.
Security	Determine whether you would like to use Transport Layer Security (TLS) encryption, which allows the PXE to communicate securely with the LDAPS server. Three options are available: ▪ StartTLS ▪ TLS ▪ None
Port (None/StartTLS)	The default Port is 389. Either use the standard LDAP TCP port or specify another port.
Port (TLS)	**Configurable only when "TLS" is selected in the Security field.** The default is 636. Either use the default port or specify another one.
Enable verification of LDAP Server Certificate	Select this checkbox if it is required to validate the LDAP server's certificate by the PXE prior to the connection. If the certificate validation fails, the connection is refused.
CA Certificate	Consult your AA server administrator to get the CA certificate file for the LDAPS server. Click Browse... to select and install the certificate file. ▪ Click Show to view the installed certificate's content. ▪ Click Remove to delete the installed certificate if it is inappropriate.
Allow expired and not yet valid certificates	▪ Select this checkbox to make the authentication succeed regardless of the certificate's validity period. ▪ After deselecting this checkbox, the authentication fails whenever any certificate in the selected certificate chain is outdated or not valid yet.
Anonymous Bind	Use this checkbox to enable or disable anonymous bind. ▪ To use anonymous bind, select this checkbox. ▪ When a Bind DN and password are required to bind to the external LDAP/LDAPS server, deselect this checkbox.

Field/setting	Description
Bind DN	**Required after deselecting the Anonymous Bind checkbox.** Distinguished Name (DN) of the user who is permitted to search the LDAP directory in the defined search base.
Bind Password, Confirm Bind Password	**Required after deselecting the Anonymous Bind checkbox.** Enter the Bind password.
Base DN for Search	Distinguished Name (DN) of the search base, which is the starting point of the LDAP search. ▪ Example: `ou=dev,dc=example,dc=com`
Login Name Attribute	The attribute of the LDAP user class which denotes the login name. ▪ Usually it is the `uid`.
User Entry Object Class	The object class for user entries. ▪ Usually it is `inetOrgPerson`.
User Search Subfilter	Search criteria for finding LDAP user objects within the directory tree.
Active Directory Domain	The name of the Active Directory Domain. ▪ Example: `testradius.com`

4. To verify if the authentication configuration is set correctly, click Test Connection to check whether the PXE can connect to the new server successfully.

   Tip: You can also test the connection on the Authentication page after finishing adding servers. See **Managing External Authentication Settings** *(on page 139).*

5. Click Add Server. The new LDAP server is listed on the Authentication page.
6. To add more servers, repeat the same steps.
7. **In the Authentication Type field, select LDAP.** Otherwise, the LDAP authentication does not work.
8. Click Save. The LDAP authentication is now in place.

To duplicate LDAP/LDAPS server settings:

If you have added any LDAP/LDAPS server to the PXE, and the server you will add shares identical settings with an existing one, the most convenient way is to duplicate that LDAP/LDAPS server's data and then revise the IP address/host name.

1. Repeat Steps 1 to 2 in the above procedure.
2. Select the "Copy settings from existing LDAP server" checkbox.
3. Click the "Select LDAP Server" field to select the LDAP/LDAPS server whose settings you want to copy.
4. Modify the IP Address/Hostname field.
5. Click Add Server.

Note: If the 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 Servers

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

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

required

To add Radius servers:

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

Field/setting	Description
IP Address / Hostname	The IP address or hostname of your Radius server.
Type of RADIUS Authentication	Select an authentication protocol. ▪ 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.

Field/setting	Description
Authentication Port, Accounting Port	The default are standard ports -- 1812 and 1813. To use non-standard ports, type a new port number.
Timeout	This sets the maximum amount of time to establish contact with the Radius server before timing out. Type the timeout period in seconds.
Retries	Type the number of retries.
Shared Secret, Confirm Shared Secret	The shared secret is necessary to protect communication with the Radius server.

4. To verify if the authentication configuration is set correctly, click Test Connection to check whether the PXE can connect to the new server successfully.

   Tip: You can also test the connection on the Authentication page after finishing adding servers. See **Managing External Authentication Settings** *(on page 139).*

5. Click Add Server. The new Radius server is listed on the Authentication page.
6. To add more servers, repeat the same steps.
7. **In the Authentication Type field, select Radius.** Otherwise, the Radius authentication does not work.
8. Click Save. Radius authentication is now in place.

Managing External Authentication Settings

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

- Enable both the external and local authentication
- Edit or delete a server
- Resort the access order of servers
- Test the connection to a server
- Disable external authentication without removing servers

To test, edit or delete a server, or resort the server list:

1. Select a server in the list.

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

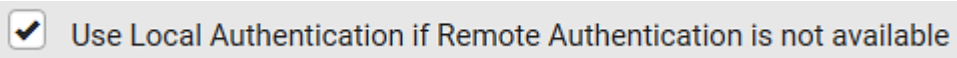
2. Perform the desired action.
   - Click Edit to edit its settings, and click Modify Server to save changes. For information on each field, see ***Adding LDAP/LDAPS Servers*** (on page 134) or ***Adding Radius Servers*** (on page 137).
   - Click Delete to delete the server, and then confirm the operation.
   - Click Test Connection to test the connection to the selected server. User credentials may be required.
   - Click or to change the server order, which determines the access priority, and click Save Order to save the new sequence.

Note: Whenever the PXE is successfully connected to one external authentication server, it STOPS trying to access the remaining servers in the authentication list regardless of the user authentication result.

To enable both the external and local authentication:

1. In the Authentication Type field, select the external authentication you want -- LDAP or Radius.

2. Select the following checkbox. Then the PXE always tries external authentication first. Whenever the external authentication fails, the PXE switches to local authentication.



3. Click Save.

To disable external authentication:

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

Configuring Login Settings

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

- Configure the user blocking feature.

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

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

To configure user blocking:

1. To enable the user blocking feature, select the "Block user on login failure" checkbox.
2. In the "Maximum number of failed logins" field, type a number. This is the maximum number of login failure the user is permitted before the user is blocked from accessing the PXE.
3. In the "Block timeout" field, type a value or click to select a time option. This setting determines how long the user is blocked.
   - If you type a value, the value must be followed by a time unit, such as '4 min.' See *Time Units* (on page 141).
4. Click Save.

Tip: If any user blocking event occurs, you can unblock that user manually by using the "unblock" CLI command over a local connection. See Unblocking a User *(on page 337).*

To set limitations for login timeout and use of identical login names:

1. In the "Idle timeout period" field, type a value or click to select a time option. This setting determines how long users are permitted to stay idle before being forced to log out.
   - If you type a value, the value must be followed by a time unit, such as '4 min.' See *Time Units* (on page 141).
   - 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.
2. Select the "Prevent concurrent login with same username" checkbox if intending to prevent multiple persons from using the same login name simultaneously.
3. Click Save.

Time Units

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

Note that different fields have different range of valid values.

Time units:

Unit	Time
min	minute(s)
h	hour(s)
d	day(s)

Configuring Password Policy

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

- Force users to use strong passwords.
- Force users to change passwords at a regular interval -- that is, password aging.

Use of strong passwords makes it more difficult for intruders to crack user passwords and access the PXE device.

To configure password aging:

1. Select the 'Enabled' checkbox of Password Aging.
2. In the Password Aging Interval field, type a value or click to select a time option. This setting determines how often users are requested to change their passwords.
   - If you type a value, the value must be followed by a time unit, such as '10 d.' See *Time Units* (on page 141).
3. Click Save.

To force users to create strong passwords:

1. Select the 'Enabled' checkbox of Strong Passwords to activate the strong password feature. The following are the default settings:

Minimum length	= 8 characters
Maximum length	= 32 characters
At least one lowercase character	= Required
At least one uppercase character	= Required
At least one numeric character	= Required
At least one special character	= Required
Number of forbidden previous passwords	= 5

Note: The maximum password length accepted by the PXE is 64 characters.

2. Make changes to the default settings as needed.
3. Click Save.

Enabling the Restricted Service Agreement

The restricted service agreement feature, if enabled, forces users to read a security agreement when they log in to the PXE.

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

An event notifying you if a user has accepted or declined the agreement can be generated. See ***Default Log Messages*** (on page 152)

To enable the service agreement:

1. Click Device Settings > Security > Service Agreement.
2. Select the Enforce Restricted Service Agreement checkbox.
3. Edit or paste the content as needed.
   - A maximum of 10,000 characters can be entered.
4. Click Save.

Login manner after enabling the service agreement:

After the Restricted Service Agreement feature is enabled, the agreement's content is displayed in the login screen.

Do either of the following, or the login fails:

- In the web interface, select the checkbox labeled "I understand and accept the Restricted Service Agreement."

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

- In the CLI, type y when the confirmation message "I understand and accept the Restricted Service Agreement" is displayed.

Setting the Date and Time

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

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.

To set the date and time:

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

- If the daylight saving time rules are not available for the selected time zone, the checkbox is not configurable.

4. Select the method for setting the date and time.

Customize the date and time

- Select User Specified Time.
- Type values in the Date field using the yyyy-mm-dd format, or click to select a date. For details, see *Calendar* (on page 145).
- Type values in the Time field using the hh:mm:ss format, or click to adjust values.
  - The time is measured in 12-hour format so you must correctly specify AM or PM by clicking the AM or PM button.

Use the NTP server

- Select "Synchronize with NTP Server."
- There are two ways to assign the NTP servers:
  - To use the DHCP-assigned NTP servers, DO NOT enter any NTP servers for the First and Second NTP Server.

    DHCP-assigned NTP servers are available only when either IPv4 or IPv6 DHCP is enabled.
  - To use the manually-specified NTP servers, specify the primary NTP server in the First Time Server field. A secondary NTP server is optional.

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

5. Click Save.

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 145).

Calendar

The calendar icon in the Date field is a convenient tool to select a custom date. Click it and a calendar appears.

Button	Function
arrows	Switch between months.
dates (01-31)	Click a date.
Today	Select today.
Clear	Clear the entry, if any, in the Date field.
Close	Close the calendar.

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 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.

Event Rules and Actions

A benefit of the product's intelligence is its ability to notify you of or react to a change in conditions. This event notification or reaction is an "event rule."

An event rule consists of two parts:

- Event: This is the situation where the PXE or a device connected to it meets a certain condition. For example, the inlet's voltage reaches the warning level.
- Action: This is the response to the event. For example, the PXE notifies the system administrator of the event via email.

If you want the PXE to perform one action at a regular interval instead of waiting until an event occurs, you can schedule that action. For example, you can make the PXE email the temperature report every hour.

Note that you need the Administrator Privileges to configure event rules.

To create an event rule:

1. Choose Device Settings > Event Rules.
2. If the needed action is not available yet, create it by clicking ➕ New Action.
   a. Assign a name to this action.
   b. Select the desired action and configure it as needed.
   c. Click Create.

   For details, see ***Available Actions*** (on page 158).
3. Click ➕ New Rule to create a new rule.
   a. Assign a name to this rule.
   b. Make sure the Enabled checkbox is selected, or the new event rule does not work.
   c. In the Event field, select the event to which you want the PXE to react.
   d. In the Available Actions field, select the desired action(s) to respond to the selected event.
   e. Click Create.

   For details, see ***Built-in Rules and Rule Configuration*** (on page 147).

To create a scheduled action:

1. If the needed action is not available yet, create it by clicking **New Action**. See above.

   Note: When creating scheduled actions, available actions are less than usual because it is meaningless to schedule certain actions like "Alarm," "Log event message," "Send email," "Syslog message" and the like.

2. Click **New Scheduled Action** to schedule the desired action.
   a. Assign a name to this scheduled action.
   b. Make sure the Enabled checkbox is selected, or the PXE does not perform this scheduled action.
   c. Set the interval time, which ranges from every minute to yearly.
   d. In the Available Actions field, select the desired action(s).
   e. Click Create.

   For details, see ***Scheduling an Action*** (on page 170).

Built-in Rules and Rule Configuration

The PXE is shipped with four built-in event rules, which cannot be deleted. If the built-in event rules do not satisfy your needs, create new rules.

Built-in rules:

- *System Event Log Rule:*

  This causes ANY event occurred to the PXE to be recorded in the internal log. It is enabled by default.

  Note: For the default log messages generated for each event, see **Default Log Messages** *(on page 152).*

- *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. It is enabled by default.

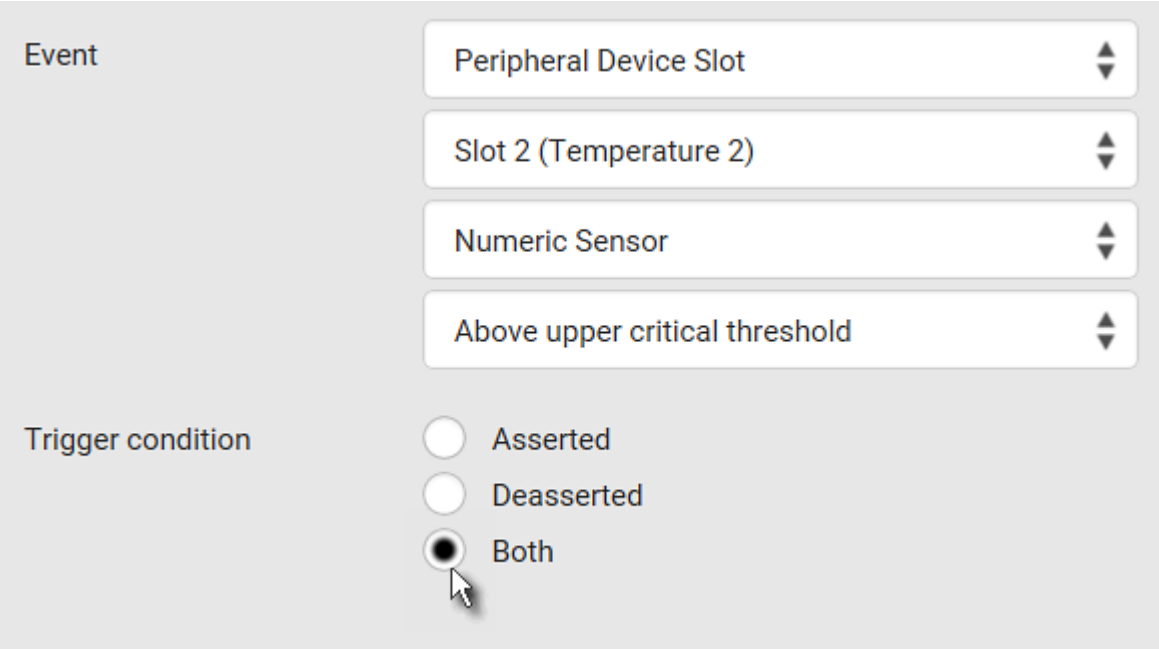
- *System Tamper Detection Unavailable:*

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

Event rule configuration illustration:

1. Choose Device Settings > Event Rules > + New Rule.
2. Click the Event field to select an event type.
   - <Any sub-event> means all events shown on the list.
   - <Any Numeric Sensor> means all numeric sensors of the PXE, including internal and environmental sensors. <Any Numeric Sensor> is especially useful if you want to receive the notifications when any numeric sensor's readings pass through a specific threshold.
3. In this example, the Peripheral Device Slot is selected, which is related to the environmental sensor packages. Then a sensor ID field for this event type appears. Click this additional field to specify which sensor should be the subject of this event.
4. In this example, sensor ID 2 (Slot 2) is selected, which is a temperature sensor. Then a new field for this sensor appears. Click this field to specify the type of event(s) you want.
5. In this example, Numeric Sensor is selected because we want to select numeric-sensor-related event(s). Then a field for numeric-sensor-related events appears. Click this field to select one of the numeric-sensor-related events from the list.

6. In this example, 'Above upper critical threshold' is selected because we want the PXE to react only when the selected temperature sensor's reading enters the upper critical range. A "Trigger condition" field appears, requiring you to define the "exact" condition related to the "upper critical" event.



7. Select the desired radio button to finish the event configuration. Refer to the following table for different types of radio buttons.
   - If needed, you may refer to event rule examples in the section titled *Sample Event Rules* (on page 177).
8. To select any action(s), select them one by one from the Available Actions list.
   - To select all available actions, click Select All.
9. To remove any action(s) from the Selected Actions field, click that action's ✖.
   - To remove all actions, click Deselect All.

Radio buttons for different events:

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

Event types	Radio buttons
Numeric sensor threshold-crossing events, or the occurrence of the selected event -- true or false	Available radio buttons include "Asserted," "Deasserted" and "Both." ▪ Asserted: The PXE takes the action only when the selected event occurs. That is, the status of the event transits from FALSE to TRUE. ▪ Deasserted: The PXE takes the action only when the selected event disappears or stops. That is, the status of the selected event transits from TRUE to FALSE. ▪ Both: The PXE takes the action both when the event occurs (asserts) and when the event stops/disappears (deasserts).
State sensor state change	Available radio buttons include "Alarmed/Open/On," "No longer alarmed/Closed/Off" and "Both." ▪ Alarmed/Open/On: The PXE takes the action only when the chosen sensor enters the alarmed, open or on state. ▪ No longer alarmed/Closed/Off: The PXE takes the action only when the chosen sensor returns to the normal, closed, or off state. ▪ Both: The PXE takes the action whenever the chosen sensor switches its state.
Sensor availability	Available radio buttons include "Unavailable," "Available" and "Both." ▪ Unavailable: The PXE takes the action only when the chosen sensor is NOT detected and becomes unavailable. ▪ Available: The PXE takes the action only when the chosen sensor is detected and becomes available. ▪ Both: The PXE takes the action both when the chosen sensor becomes unavailable or available.

Event types	Radio buttons
Network interface link state	▪ Link state is up: The PXE takes the action only when the network link state changes from down to up. ▪ Link state is down: The PXE takes the action only when the network link state changes from up to down. ▪ Both: The PXE takes the action whenever the network link state changes.
Function enabled or disabled	▪ Enabled: The PXE takes the action only when the chosen function is enabled. ▪ Disabled: The PXE takes the action only when the chosen function is disabled. ▪ Both: The PXE takes the action when the chosen function is either enabled or disabled.
Restricted service agreement	▪ Accepted: The PXE takes the action only when the specified user accepts the restricted service agreement. ▪ Declined: The PXE takes the action only when the specified user rejects the restricted service agreement. ▪ Both: The PXE takes the action both when the specified user accepts or rejects the restricted service agreement.
Server monitoring event	▪ Monitoring started: The PXE takes the action only when the monitoring of any specified server starts. ▪ Monitoring stopped: The PXE takes the action only when the monitoring of any specified server stops. ▪ Both: The PXE takes the action when the monitoring of any specified server starts or stops.

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

Default Log Messages

Following are default log messages recorded internally and emailed to specified recipients when PXE events occur (are TRUE) or, in some cases, stop or become unavailable (are FALSE). See *Send Email* (on page 163) for information configuring email messages to be sent when specified events occur.

Note: PXE does NOT support the card reader, modem, load shedding and webcam so you can ignore the related data.

Event/context	Default message when the event = TRUE	Default message when the event = FALSE
Card Reader Management > Card inserted	Card Reader with id '[CARDREADERID]' connected.	
Card Reader Management > Card Reader attached	Card Reader with id '[CARDREADERID]' disconnected.	
Card Reader Management > Card Reader detached	Card of type '[SMARTCARDTYPE]' with ID '[SMARTCARDID]' inserted.	

Event/context	Default message when the event = TRUE	Default message when the event = FALSE
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]'.	
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]'.	

Event/context	Default message when the event = TRUE	Default message when the event = FALSE
Device > Network interface link state is up	The [IFNAME] network interface link is now up.	The [IFNAME] network interface link is now down.
Device > Peripheral Device Firmware Update	Firmware update for peripheral device [EXTSENSORSERIAL] from [OLDVERSION] to [VERSION] [SENSORSTATENAME].	
Device > Sending SMTP message failed	Sending SMTP message to '[RECIPIENTS]' using server '[SERVER]' failed.	
Device > Sending SNMP inform failed or no response	Sending SNMP inform to manager [SNMPMANAGER]:[SNMPMANAGERPORT] failed or no response. [ERRORDESC].	
Device > Sending Syslog message failed	Sending Syslog message to server [SYSLOGSERVER]:[SYSLOGPORT] ([SYSLOGTRANSPORTPROTO]) failed. [ERRORDESC].	
Device > Sending SMS message failed	Sending SMS message to '[PHONENUMBER]' failed.	
Device > An LDAP error occurred	An LDAP error occurred: [LDAPERRORDESC].	
Device > An Radius error occurred	An Radius error occurred: [RADIUSERRORDESC].	
Device > Unknown peripheral device attached	An unknown peripheral device with rom code '[ROMCODE]' was attached at position '[PERIPHDEVPOSITION]'.	
Device > USB slave connected	USB slave connected.	USB slave disconnected.
Device > WLAN authentication over TLS with incorrect system clock	Established connection to wireless network '[SSID]' via Access Point with BSSID '[BSSID]' using '[AUTHPROTO]' authentication with incorrrect system clock.	
Energywise > Enabled	User '[USERNAME]' from host '[USERIP]' enabled EnergyWise.	User '[USERNAME]' from host '[USERIP]' disabled EnergyWise.

Event/context	Default message when the event = TRUE	Default message when the event = FALSE
Peripheral Device Slot > * > Numeric Sensor > Unavailable	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' unavailable.	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' available.
Peripheral Device Slot > * > Numeric Sensor > Above upper critical threshold	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' asserted 'above upper critical' at [READING].	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' deasserted 'above upper critical' at [READING].
Peripheral Device Slot > * > Numeric Sensor > Above upper warning threshold	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 threshold	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' asserted 'below lower warning' at [READING].	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' deasserted 'below lower warning' at [READING].
Peripheral Device Slot > * > Numeric Sensor > Below lower critical threshold	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/Actuator > Unavailable	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' unavailable.	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' available.
Peripheral Device Slot > * > State Sensor/Actuator > Alarmed/Open/On	Peripheral device '[EXTSENSORNAME]' in slot [EXTSENSORSLOT] is [SENSORSTATENAME].	Peripheral device '[EXTSENSORNAME]' in slot [EXTSENSORSLOT] is [SENSORSTATENAME].
Inlet > * > Enabled	Inlet '[INLET]' has been enabled by user '[USERNAME]' from host '[USERIP]'.	Inlet '[INLET]' has been disabled by user '[USERNAME]' from host '[USERIP]'.
Inlet > * > Sensor > * > Unavailable	Sensor '[INLETSENSOR]' on inlet '[INLET]' unavailable.	Sensor '[INLETSENSOR]' on inlet '[INLET]' available.
Inlet > * > Sensor > * > Above upper critical threshold	Sensor '[INLETSENSOR]' on inlet '[INLET]' asserted 'above upper critical'.	Sensor '[INLETSENSOR]' on inlet '[INLET]' deasserted 'above upper critical'.
Inlet > * > Sensor > * > Above	Sensor '[INLETSENSOR]' on inlet	Sensor '[INLETSENSOR]' on inlet

Event/context	Default message when the event = TRUE	Default message when the event = FALSE
upper warning threshold	'[INLET]' asserted 'above upper warning'.	'[INLET]' deasserted 'above upper warning'.
Inlet > * > Sensor > * > Below lower warning threshold	Sensor '[INLETSENSOR]' on inlet '[INLET]' asserted 'below lower warning'.	Sensor '[INLETSENSOR]' on inlet '[INLET]' deasserted 'below lower warning'.
Inlet > * > Sensor > * > Below lower critical threshold	Sensor '[INLETSENSOR]' on inlet '[INLET]' asserted 'below lower critical'.	Sensor '[INLETSENSOR]' on inlet '[INLET]' deasserted 'below lower critical'.
Inlet > * > Sensor > Active Energy > Reset	Sensor '[INLETSENSOR]' on inlet '[INLET]' has been reset by user '[USERNAME]' from host '[USERIP]'.	
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.	
Overcurrent Protector > * > Sensor > * > Unavailable	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' unavailable.	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' available.
Overcurrent Protector > * > Sensor > * > Above upper critical threshold	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' asserted 'above upper critical'.	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' deasserted 'above upper critical'.
Overcurrent Protector > * > Sensor > * > Above upper warning threshold	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' asserted 'above upper warning'.	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' deasserted 'above upper warning'.
Overcurrent Protector > * > Sensor > * > Below lower warning threshold	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' asserted 'below lower warning'.	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' deasserted 'below lower warning'.
Overcurrent Protector > * > Sensor > * > Below lower critical threshold	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' asserted 'below lower critical'.	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' deasserted 'below lower critical'.
Overcurrent Protector > * > Sensor > Trip > Open	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' is open.	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' is

Event/context	Default message when the event = TRUE	Default message when the event = FALSE
		closed.
PDU > Load Shedding > Started	PX placed in Load Shedding Mode by user '[USERNAME]' from host '[USERIP]'.	PX removed from Load Shedding Mode by user '[USERNAME]' from host '[USERIP]'.
Server Monitoring > * > Error	Error monitoring server '[MONITOREDHOST]': [ERRORDESC]	
Server Monitoring > * > Monitored	Server '[SERVER]' is now being monitored.	Server '[SERVER]' is no longer being monitored.
Server Monitoring > * > Unreachable	Server '[SERVER]' is unreachable.	Server '[SERVER]' is reachable.
Server Monitoring > * > Unrecoverable	Connection to server '[MONITOREDHOST]' could not be restored.	
User Activity > * > User logon state	User '[USERNAME]' from host '[USERIP]' logged in.	User '[USERNAME]' from host '[USERIP]' logged out.
User Activity > * > Authentication failure	Authentication failed for user '[USERNAME]' from host '[USERIP]'.	
User Activity > * > User accepted the Restricted Service Agreement	User '[USERNAME]' from host '[USERIP]" accepted the Restricted Service Agreement.	User '[USERNAME]' from host '[USERIP]" declined the Restricted Service Agreement.
User Activity > * > User blocked	User '[USERNAME]' from host '[USERIP]' was blocked.	
User Activity > * > Session timeout	Session of user '[USERNAME]' from host '[USERIP]' timed out.	
User Administration > User added	User '[TARGETUSER]' added by user '[USERNAME]' from host '[USERIP]'.	
User Administration > User modified	User '[TARGETUSER]' modified by user '[USERNAME]' from host '[USERIP]'.	
User Administration > User deleted	User '[TARGETUSER]' deleted by user '[USERNAME]' from host '[USERIP]'.	
User Administration > Password changed	Password of user '[TARGETUSER]' changed by user '[USERNAME]' from host '[USERIP]'.	

Event/context	Default message when the event = TRUE	Default message when the event = FALSE
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]'.	

The asterisk symbol (*) represents anything you select for the 'trigger' events.

Available Actions

The PXE comes with three built-in actions, which cannot be deleted. You can create additional actions for responding to different events.

Built-in actions:

- *System Event Log Action:*

  This action records the selected event in the internal log when the event occurs.

- *System SNMP Notification Action:*

  This action sends SNMP notifications to one or multiple IP addresses after the selected event occurs.

  Note: No IP addresses are specified for this notification action by default so you must enter IP addresses before applying this action to any event rule. See **Editing or Deleting a Rule/Action** *(on page 176). Any changes made to the 'SNMP Notifications' section on the SNMP page will update the settings of the System SNMP Notification Action, and vice versa. See* **Configuring SNMP Settings** *(on page 115).*

- *System Tamper Alarm:*

  This action causes the PXE to show the alarm for the DX tamper sensor, if any, on the Dashboard page until a person acknowledges it. By default, this action has been assigned to the built-in tamper detection event rules. For information on acknowledging an alarm, see ***Dashboard - Alarms*** (on page 63).

Actions you can create:

1. Choose Device Settings > Event Rules > ✚ New Action.
2. Click the Action field to select an action type from the list.
3. Below is the list of available actions.

Action	Function
Alarm	Requires the user to acknowledge the alert after it is generated. If needed, you can have the alert notifications regularly generated until a person takes the acknowledgment action. See ***Alarm*** (on page 160).
Execute an action group	Creates a group of actions comprising existing actions. See ***Action Group*** (on page 162).
External beeper	PXE does NOT support this feature so you can ignore this action.
Internal beeper	PXE does NOT support this feature so you can ignore this action.
Log event message	Records the selected events in the internal log. See ***Log an Event Message*** (on page 162).
Push out sensor readings	Sends internal sensor log, environmental sensor log or asset management strip data to a remote server using HTTP POST requests. See ***Push Out Sensor Readings*** (on page 162). *Note: PXE does NOT support the asset management feature so no asset management strip data is available.*
Record snapshots to webcam storage	PXE does NOT support this feature so you can ignore this action.
Send email	Emails a textual message. See ***Send Email*** (on page 163).

Action	Function
Send sensor report	Reports the readings or status of the selected sensors, including internal or external sensors. See *Send Sensor Report* (on page 164).
Send SMS message	PXE does NOT support this feature so you can ignore this action.
Send snapshots via email	PXE does NOT support this feature so you can ignore this action.
Send SNMP notification	Sends SNMP traps or informs to one or multiple SNMP destinations. See *Send an SNMP Notification* (on page 165).
Start/stop Lua script	If you are a developer who can create a Lua script, you can upload it to the PXE, and have the PXE automatically perform or stop the script in response to an event. See *Start or Stop a Lua Script* (on page 167).
Switch peripheral actuator	Switches on or off the mechanism or system connected to the specified actuator. See *Switch Peripheral Actuator* (on page 168).
Syslog message	Makes the PXE automatically forward event messages to the specified syslog server. See *Syslog Message* (on page 169).

4. Enter the information as needed and click Create.
5. Then you can assign the newly-created action to an event rule or schedule it. See *Event Rules and Actions* (on page 146).

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 the maximum number of alert notifications is sent.

For information on acknowledging an alert, see *Dashboard* (on page 56).

Operation:

1. Choose Device Settings > Event Rules > New Action.
2. Select Alarm from the Action list.

3. In the Alarm Notifications list box, specify one or multiple ways to issue the alert notifications. Available methods vary, depending on how many notification-based actions have been created. Notification-based action types include:
   - External beeper
   - Syslog message
   - Send email
   - Send SMS message
   - Internal beeper

   Note: PXE does NOT support external and internal beepers so you can ignore related actions.

   If no appropriate actions are available, create them first.

   a. To select any methods, select them one by one in the Available field.

      To add all available methods, simply click Select All.

   b. To delete any methods, click a method's ✖ in the Selected field.

      To remove all methods, simply click Deselect All.
4. To enable the notification-resending feature, select the "Enable Re-scheduling of Alarm Notifications" checkbox.
5. In the "Re-scheduling Period" field, specify the time interval (in minutes) at which the alert notification is resent or regenerated regularly.
6. In the "Re-scheduling Limit" field, specify the maximum number of times the alert notification is resent. Values range from 1 to infinite.
7. **(Optional)** You can instruct the PXE to send the acknowledgment notification after the alarm is acknowledged in the Acknowledgment Notifications field. Available methods are identical to those for generating alarm notifications.

   a. In the Available field, select desired methods one by one, or click Select All. See step 3 for details.

   b. In the Selected field, click any method's ✖ to remove unnecessary ones, or click Deselect All.

Action Group

You can create an action group that performs up to 32 actions. After creating such an action group, you can easily assign this set of actions to any event rule rather than selecting all needed actions one by one per rule.

If the needed action is not available yet, create it first. See ***Available Actions*** (on page 158).

Operation:

1. Choose Device Settings > Event Rules > New Action.
2. Select "Execute an action group" from the Action list.
3. To select any action(s), select them one by one from the Available Actions list.
   - To select all available actions, click Select All.
4. To remove any action(s) from the Selected Actions field, click that action's ✖.
   - To remove all actions, click Deselect All.

Log an Event Message

The option "Log event message" records the selected events in the internal log.

The default log message generated for each type of event is available in the section titled ***Default Log Messages*** (on page 152).

Push Out Sensor Readings

You can configure the PXE to push sensor log to a remote server after a certain event occurs, including logs of internal sensors, environmental sensors and actuators.

If you have connected Raritan's asset strips to the PXE, you can also configure the PXE to push the data to a server.

Before creating this action, make sure that you have properly defined the destination servers and the data to be sent on the Data Push page. See ***Configuring Data Push Settings*** (on page 181).

Tip: To send the data at a regular interval, schedule this action. See Scheduling an Action *(on page 170). Note that the "Asset management log" is generated only when there are changes made to any asset strips or asset tags, such as connection or disconnection events.*

Operation:

1. Choose Device Settings > Event Rules > New Action.

2. Select "Push out sensor readings" from the Action list.
3. Select a server or host which receives the asset strip data or sensor log in the Destination field.
   - If the desired destination is not available yet, go to the Data Push page to specify it.

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
```

For a list and definition of available variables, see ***Email and SMS Message Placeholders*** (on page 173).

Operation:

1. Choose Device Settings > Event Rules > New Action.
2. Select "Send email" from the Action list.
3. In the "Recipient Email Addresses" field, specify the email address(es) of the recipient(s). Use a comma to separate multiple email addresses.
4. To use the SMTP server specified on the SMTP Server page, make sure the "Use custom SMTP Server" checkbox is NOT selected.

   To use a different SMTP server, select this checkbox. The fields for customized SMTP settings appear. For information on each field, see ***Configuring SMTP Settings*** (on page 116).

   Default messages are sent based on the event. For a list of default log messages and events that trigger them, see ***Default Log Messages*** (on page 152).
5. If needed, select the Use Custom Log Message checkbox, and then create a custom message up to 1024 characters in the provided field.
   - When clicking anywhere inside the text box, the Event Context Information displays, showing a list of placeholders and their definitions. Just click the desired placeholder. For details, see ***Email and SMS Message Placeholders*** (on page 173).
   - To start a new line in the text box, press Enter.

- If needed, you can resize the text box by dragging the bottom-right corner.

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.
- Peripheral device sensors, which can be any Raritan environmental sensor packages connected to the PXE, such as temperature or humidity sensors.

An example of this action is available in the section titled ***Send Sensor Report Example*** (on page 172).

Operation:

1. Choose Device Settings > Event Rules > New Action.
2. Select "Send sensor report" from the Action list.
3. In the Destination Actions section, select the method(s) to report sensor readings or states. The number of available methods varies, depending on how many messaging actions have been created.

   The messaging action types include:

   - Log event message
   - Syslog message
   - Send email
   - Send SMS message

   a. If no messaging actions are available, create them now. See ***Available Actions*** (on page 158).

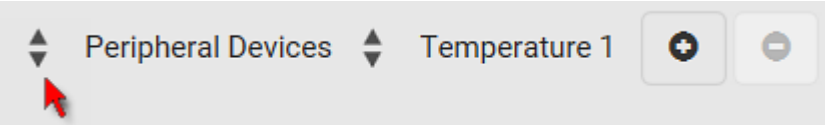
   b. To select any methods, select them one by one in the Available field.

      To add all available methods, simply click Select All.

   c. To delete any methods, click a method's ✖ in the Selected field.

      To remove all methods, simply click Deselect All.
4. In the Available Sensors field, select the desired target's sensor.

a. Click the first to select a target component from the list.



b. Click the second to select the specific sensor for the target from the list.

c. Click to add the selected sensor to the Report Sensors list box.

For example, to monitor the current reading of the Inlet 1, select Inlet 1 from the left field, and then select RMS Current from the right field.

5. To report additional sensors simultaneously, repeat the above step to add more sensors.
   - To remove any sensor from the Report Sensors list box, select it and click . To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.
6. To immediately send out the sensor report, click Send Report Now.

Tip: When intending to send a sensor report using custom messages, use the placeholder [SENSORREPORT] to report sensor readings. See **Email and SMS Message Placeholders** *(on page 173).*

Send an SNMP Notification

This option sends an SNMP notification to one or multiple SNMP destinations.

▶ **Operation:**

1. Choose Device Settings > Event Rules > New Action.
2. Select "Send SNMP notification" from the Action list.
3. Select the type of SNMP notification. See either procedure below according to your selection.

To send SNMP v2c notifications:

1. In the Notification Type field, select SNMPv2c Trap or SNMPv2c Inform.
2. For SNMP INFORM communications, leave the resend settings at their default or do the following:
   a. In the Timeout field, specify the interval of time, in seconds, after which a new inform communication is resent if the first is not received. For example, resend a new inform communication once every 3 seconds.
   b. In the Number of Retries field, specify the number of times you want to resend the inform communication if it fails. For example, inform communications are resent up to 5 times when the initial communication fails.
3. In the Host fields, enter the IP address of the device(s) you want to access. This is the address to which notifications are sent by the SNMP system agent.
4. In the Port fields, enter the port number used to access the device(s).
5. In the Community fields, enter the SNMP community string to access the device(s). The community is the group representing the PXE and all SNMP management stations.

Tip: An SNMP v2c notification action permits only a maximum of three SNMP destinations. To assign more than three SNMP destinations to a specific rule, first create several SNMP v2c notification actions, each of which contains completely different SNMP destinations, and then add all of these SNMP v2c notification actions to the same rule.

To send SNMP v3 notifications:

1. In the Notification Type field, select SNMPv3 Trap or SNMPv3 Inform.
2. For SNMP TRAPs, the engine ID is prepopulated.
3. For SNMP INFORM communications, leave the resend settings at their default or do the following:
   a. In the Timeout field, specify the interval of time, in seconds, after which a new inform communication is resent if the first is not received. For example, resend a new inform communication once every 3 seconds.
   b. In the Number of Retries field, specify the number of times you want to resend the inform communication if it fails. For example, inform communications are resent up to 5 times when the initial communication fails.

4. For both SNMP TRAPS and INFORMS, enter the following as needed and then click OK to apply the settings:
   a. Host name
   b. Port number
   c. User ID for accessing the host -- make sure the User ID has the SNMPv3 permission.
   d. Select the host security level

Security level	Description
"noAuthNoPriv"	Select this if no authorization or privacy protocols are needed.
"authNoPriv"	Select this if authorization is required but no privacy protocols are required. • Select the authentication protocol - MD5 or SHA • Enter the authentication passphrase and then confirm the authentication passphrase
"authPriv"	Select this if authentication and privacy protocols are required. • Select the authentication protocol - MD5 or SHA • Enter the authentication passphrase and confirm the authentication passphrase • Select the Privacy Protocol - DES or AES • Enter the privacy passphrase and then confirm the privacy passphrase

Start or Stop a Lua Script

If you have created or loaded a Lua script file into the PXE, you can have that script automatically run or stop in response to a specific event.

For instructions on creating or loading a Lua script into this product, see *Lua Scripts* (on page 187).

To automatically start or stop a Lua script:

1. Choose Device Settings > Event Rules > New Action.
2. Select "Start/stop Lua script" from the Action list.
3. In the Operation field, select Start Script or Stop Script.
4. In the Script field, select the script that you want it to be started or stopped when an event occurs.

- No script is available if you have not created or loaded it into the PXE.

5. To apply different arguments than the default, do the following. Note that the newly-added arguments will override this script's default arguments.
   a. Click ✚ Add argument.
   b. Type the key and value.
   c. Repeat the same steps to enter more arguments as needed.
      - To remove any existing argument, click − adjacent to it.

Switch 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 the actuator when a specific event occurs.

Note: For information on connecting actuators, see **DX Sensor Packages** *(on page 31).*

Operation:

1. Choose Device Settings > Event Rules > ✚ New Action.
2. Select "Switch peripheral actuator" from the Action list.
3. In the Operation field, select an operation for the selected actuator(s).
   - Turn On: Turns on the selected actuator(s).
   - Turn Off: Turns off the selected actuator(s).
4. To select the actuator(s) where this action will be applied, select them one by one from the Available Actuators list.
   - To add all actuators, click Select All.
5. To remove any selected actuator from the Selected Actuators field, click that actuator's ✖.
   - To remove all actuators, click Deselect All.

Syslog Message

Use this action to automatically forward event messages to the specified syslog server. Determine the syslog transmission mechanism you prefer when setting it up - UDP, TCP or TLS over TCP.

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 or Clearing the Local Event Log* (on page 196).

Operation:

1. Choose Device Settings > Event Rules > New Action.
2. Select "Syslog message" from the Action list.
3. In the Syslog Server field, specify the IP address to which the syslog is forwarded.
4. In the Transport Protocol field, select one of the syslog protocols: TCP, UDP or TCP+TLS. The default is UDP.

Transport protocols	Next steps
UDP	▪ In the UDP Port field, type an appropriate port number. Default is 514. ▪ Select the "Legacy BSD Syslog Protocol" checkbox if applicable.
TCP	NO TLS certificate is required. Type an appropriate port number in the TCP Port field.
TCP+TLS	A TLS certificate is required. Do the following: a. Type an appropriate port number in the "TCP Port" field. Default is 6514. b. In the CA Certificate field, click Browse... to select a TLS certificate. After installing the certificate, you may: ▪ Click Show to view its contents. ▪ Click Remove to delete it if it is inappropriate. c. Determine whether to select the "Allow expired and not yet valid certificates" checkbox. ▪ To always send the event message to the specified syslog server as long as a TLS certificate is available, select this checkbox. ▪ To prevent the event message from being sent to the specified syslog server when any TLS certificate in the selected certificate chain is outdated or not valid yet, deselect this checkbox.

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 sensor regularly by scheduling the "Send Sensor Report" action.

When scheduling an action, make sure you have a minimum of 1-minute buffer between this action's creation and first execution time. Otherwise, the scheduled action will NOT be performed at the specified time when the buffer time is too short. For example, if you want an action to be performed at 11:00 am, you should finish scheduling it at 10:59 am or earlier.

If the needed action is not available yet, create it first. See ***Available Actions*** (on page 158).

Operation:

1. Choose Device Settings > Event Rules > ➕ New Scheduled Action.
2. To select any action(s), select them one by one from the Available Actions list.
   - To select all available actions, click Select All.
3. To remove any action(s) from the Selected Actions field, click that action's ✖.
   - To remove all actions, click Deselect All.
4. Select the desired frequency in the Execution Time field, and then specify the time interval or a specific date and time in the field(s) that appear.

Execution time	Frequency settings
Minutes	Click the Frequency field to select an option. The frequency ranges from every minute, every 5 minutes, every 10 minutes and so on until every 30 minutes.
Hourly	Type a value in the Minute field, which is set to either of the following: ▪ The Minute field is set to 0 (zero). Then the action is performed at 1:00 am, 2:00 am, 3:00 am and so on. ▪ The Minute field is set to a non-zero value. For example, if it is set to 30, then the action is performed at 1:30 am, 2:30 am, 3:30 am and so on.
Daily	Type values or click ⌃ ⌄. The time is measured in 12-hour format so you must correctly specify AM or PM by clicking the AM/PM button. For example, if you specify 01:30PM, the action is performed at 13:30 pm every day.
Weekly	Both the day and time must be specified for the weekly option. ▪ Days range from Sunday to Saturday. ▪ The time is measured in 12-hour format so you must correctly specify AM or PM by clicking the AM/PM button.
Monthly	Both the date and time must be specified for the monthly option. ▪ The dates range from 1 to 31. ▪ The time is measured in 12-hour format so you must correctly specify AM or PM by clicking the AM/PM button. Note that NOT every month has the date 31, and February in particular does not have the date 30 and probably even 29. Check the calendar when selecting 29, 30 or 31.

Execution time	Frequency settings
Yearly	This option requires three settings: ▪ Month - January through December. ▪ Day of month - 1 to 31. ▪ Time - the value is measured in 12-hour format so you must correctly specify AM or PM by clicking the AM/PM button.

An example of the scheduled action is available in the section titled ***Send Sensor Report Example*** (on page 172).

Send Sensor Report Example

To create a scheduled action for emailing a temperature sensor report hourly, it requires:

- A 'Send email' action
- A 'Send sensor report' action
- A timer - that is, the scheduled action

Steps:

1. Click ✚ New Action to create a 'Send email' action that sends an email to the desired recipient(s). For details, see ***Send Email*** (on page 163).
   - In this example, this action is named *Email a Sensor Report*.
   - If intended, you can customize the email messages in this action.
2. Click ✚ New Action to create a 'Send sensor report' action that includes the 'Email a Sensor Report' action as its destination action. For details, see ***Send Sensor Report*** (on page 164).
   - In this example, this action is named *Send Temperature Sensor Readings*.
   - You can specify more than one temperature sensor as needed in this action.
3. Click ✚ New Scheduled Action to create a timer for performing the 'Send Temperature Sensor Readings' action hourly. For details, see ***Scheduling an Action*** (on page 170).
   - In this example, the timer is named *Hourly Temperature Sensor Reports*.
   - To perform the specified action at 12:30 pm, 01:30 pm, 02:30 pm, and so on, select Hourly, and set the Minute to 30.

Then the PXE will send out an email containing the specified temperature sensor readings hourly every day.

Whenever you want the PXE to stop sending the temperature report, simply deselect the Enabled checkbox in the timer.

Email and SMS Message Placeholders

Actions of "Send email" and "Send SMS message" allow you to customize event messages. See *Send Email* (on page 163) or Send SMS Message.

When clicking anywhere inside the text box, the Event Context Information displays, showing a list of placeholders and their definitions. Simply drag the scroll bar and then click the desired placeholder to insert it into the custom message. Or you can type a keyword in the "search" box to quickly find the desired placeholder.

If wanted, you can resort the list by clicking the desired column header. See *Sorting a List* (on page 55).

To make the Event Context Information disappear, click anywhere outside its window.

Following are placeholders that can be used in custom messages.

Placeholder	Definition
[ACTIVEINLET]	The label of the newly activated inlet
[AMSBLADESLOTPOSITION]	The (horizontal) slot position, an action applies to
[AMSLEDCOLOR]	The RGB LED color
[AMSLEDMODE]	The LED indication mode
[AMSLEDOPMODE]	The LED operating mode
[AMSNAME]	The name of an asset strip
[AMSNUMBER]	The numeric ID of an asset strip
[AMSRACKUNITPOSITION]	The (vertical) rack unit position, an action applies to
[AMSSTATE]	The human readable state of an asset strip
[AMSTAGID]	The asset tag ID
[CIRCUITCTRATING]	The circuit CT rating
[CIRCUITCURRENTRATING]	The circuit current rating
[CIRCUITNAME]	The circuit name
[CIRCUITPOLE]	The circuit power line identifier

Placeholder	Definition
[CIRCUITSENSOR]	The circuit sensor name
[CIRCUIT]	The circuit identifier
[CONFIGPARAM]	The name of a configuration parameter
[CONFIGVALUE]	The new value of a parameter
[DATETIME]	The human readable timestamp of the event occurrence
[DEVICEIP]	The IP address of the device, the event occurred on
[DEVICENAME]	The name of the device, the event occurred on
[ERRORDESC]	The error message
[EVENTRULENAME]	The name of the matching event rule
[EXTSENSORNAME]	The name of a peripheral device
[EXTSENSORSLOT]	The ID of a peripheral device slot
[EXTSENSOR]	The peripheral device identifier
[IFNAME]	The human readable name of a network interface
[INLETPOLE]	The inlet power line identifier
[INLETSENSOR]	The inlet sensor name
[INLET]	The power inlet label
[ISASSERTED]	Boolean flag whether an event condition was entered (1) or left (0)
[LDAPERRORDESC]	An LDAP error occurred
[LHXFANID]	The ID of a fan connected to an LHX/SHX
[LHXPOWERSUPPLYID]	The ID of an LHX/SHX power supply
[LHXSENSORID]	The ID of an LHX/SHX sensor probe
[MONITOREDHOST]	The name or IP address of a monitored host
[OCPSENSOR]	The overcurrent protector sensor name
[OCP]	The overcurrent protector label
[OLDVERSION]	The firmware version the device is being upgraded from

Placeholder	Definition
[OUTLETNAME]	The outlet name *Note: If any outlet does not have a name, neither an outlet name nor an outlet number will be shown in the custom message for it. Therefore, it is recommended to check the availability of all outlet names if intending to use this placeholder.*
[OUTLETPOLE]	The outlet power line identifier
[OUTLETSENSOR]	The outlet sensor name
[OUTLET]	The outlet label
[PDUPOLESENSOR]	The sensor name for a certain power line
[PDUSENSOR]	The PDU sensor name
[PERIPHDEVPOSITION]	The position of an attached peripheral device
[PHONENUMBER]	The phone number an SMS was sent to
[PORTID]	The label of the external port, the event triggering device is connected to
[PORTTYPE]	The type of the external port (for example, 'feature' or 'auxiliary'), the event triggering device is connected to
[POWERMETERPOLE]	The PMC power meter line identifier
[POWERMETERSENSOR]	The PMC power meter sensor name
[POWERMETER]	The PMC power meter ID
[RADIUSERRORDESC]	A Radius error occurred
[ROMCODE]	The rom code of an attached peripheral device
[SENSORREADINGUNIT]	The unit of a sensor reading
[SENSORREADING]	The value of a sensor reading
[SENSORREPORT]	The formatted sensor report contents
[SENSORSTATENAME]	The human readable state of a sensor
[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

Placeholder	Definition
[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

Editing or Deleting a Rule/Action

You can change the settings of an event rule, action or scheduled action, or delete them.

Exception: Some settings of the built-in event rules or actions are not user-configurable. Besides, you cannot delete built-in rules and actions. See **Built-in Rules and Rule Configuration** *(on page 147) or* **Available Actions** *(on page 158).*

To edit or delete an event rule, action or scheduled action:

1. Choose Device Settings > Event Rules.
2. Click the desired one in the list of rules, actions or scheduled actions. Its setup page opens.
3. Perform the desired action.
   - To modify settings, make necessary changes and then click Save.
   - To delete it, click Delete on the top-right corner. Then click Delete on the confirmation message.

Sample Event Rules

Sample PDU-Level Event Rule

In this example, we want the PXE to record the firmware upgrade failure in the internal log when it happens.

The event rule involves:

- Event: Device > Firmware update failed
- Action: System Event Log Action

To create this PDU-level event rule:

1. For an event at the PDU level, select "Device" in the Event field.
2. Select "Firmware update failed" so that the PXE responds to the event related to firmware upgrade failure.
3. To make the PXE record the firmware update failure event in the internal log, select "System Event Log Action" in the Available Actions field.

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.

The event rule involves:

- Event: Inlet > Sensor > Any sub-event
- Action: System SNMP Notification Action

To create the above event rule:

1. For an event at the inlet level, select "Inlet" in the Event field.
2. Select "Sensor" to refer to sensor-related events.
3. Select "Any sub-event" to include all events related to all sensors of this inlet and all thresholds, such as current, voltage, upper critical threshold, upper warning threshold, lower critical threshold, lower warning threshold, and so on.
4. To make the PXE send SNMP notifications, select "System SNMP Notification Action" in the Available Actions box.

   Note: The SNMP notifications may be SNMP v2c or SNMP v3 traps/informs, depending on the settings for the System SNMP Notification Action. See **Enabling and Configuring SNMP** *(on page 207).*

   Then the SNMP notifications are sent when:

   - Any numeric sensor's reading enters the warning or critical range.
   - Any sensor reading or state returns to normal.

- Any sensor becomes unavailable.
- The active energy sensor is reset.

For example, when the Inlet I1's voltage exceeds the upper warning threshold, the SNMP notifications are sent, and when the voltage drops below the upper warning threshold, the SNMP notifications are sent again.

Sample Sensor-Level Event Rule

In this example, we want the PXE to send a notification email when a contact closure sensor enters the alarmed state. This event rule requires creating a new action before creating the rule.

Step 1: create a new action for sending an email

1. Choose Device Settings > Event Rules > New Action.
2. In this illustration, assign the name "Send a Notification" to the new action.
3. In the Action field, select "Send email."
4. In the Recipient Email Addresses field, type one or multiple recipients' email addresses.
5. (Optional) Specify the SMTP settings and custom log message if needed.
6. Click Create to finish the creation.

After the new action is created, follow the procedure below to create an event rule that sends a notification email when the contact closure sensor enters the alarmed state. This event rule involves the following:

- Event: Peripheral Device Slot > Slot 1 > State Sensor/Actuator > Alarmed/Open/On
- Trigger condition: Alarmed
- Action: Send a Notification

Step 2: create the contact closure-triggered email event rule

1. Click New Rule on the Event Rules page.
2. In this illustration, assign the name "Contact Closure Triggered Email" to the new rule.
3. In the Event field, select "Peripheral Device Slot" to indicate we are specifying an event related to the environmental sensor package.
4. Select the ID number of the desired contact closure sensor. In this illustration, the ID number of the desired contact closure sensor is 1, so select Slot 1.

Note: ID numbers of all sensors/actuators are available on the Peripherals page. See **Peripherals** *(on page 76).*

5. Select "State Sensor/Actuator" because the contact closure sensor is a state sensor.
6. Select "Alarmed" since we want the PXE to respond when the selected contact closure sensor changes its state related to the "alarmed" state.
7. In the "Trigger condition" field, select the Alarmed/Open/On radio button so that the action is taken only when the contact closure sensor enters the alarmed state.
8. Select "Send a Notification" from the Available Actions list.

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 more event.

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

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 451).

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: The PXE device's SNMP agent must be enabled for this feature to work. See **Enabling and Configuring SNMP** *(on page 207). In addition, using an NTP time server ensures accurately time-stamped measurements.*

By default, data logging is enabled. You must have the "Administrator Privileges" or "Change Pdu, Inlet, Outlet & Overcurrent Protector Configuration" permissions to change the setting.

▶ To configure the data logging feature:

1. Choose Device Settings > Data Logging.
2. To enable the data logging feature, select the "Enable" checkbox in the General Settings section.
3. Type a number in the Measurements Per Log Entry field. Valid range is from 1 to 600. The default is 60.
4. Verify that all sensor logging is enabled. If not, click Enable All at the bottom of the page to have all sensors selected.
   - You can also click the topmost checkbox labeled "Logging Enabled" in the header row of each section to select all sensors of the same type.

- If any section's number of sensors exceeds 35, the remaining sensors are listed on next page(s). If so, a pagination bar similar to the following diagram displays in this section, which you can click any button to switch between pages.

5. Click Save. This button is located at the bottom of the page.

Important: Although it is possible to selectively enable/disable logging for individual sensors on the PXE, it is NOT recommended to do so.

Configuring Data Push Settings

You can push the sensor log to a remote server for data synchronization. The data will be sent in JSON format using HTTP POST requests. You need to set up the destination and authentication for data push on the PXE.

After configuring the destination and authentication settings, do either or both of the following:

- To perform the data push after the occurrence of a certain event, create the data push action and assign it to an event rule.
- To push the data at a regular interval, schedule the data push action.

See ***Event Rules and Actions*** (on page 146).

To configure data push settings:

1. Choose Device Settings > Data Push.
2. To specify a destination, click

.
3. Do the following to set up the URL field.
   a. Click to select *http* or *https*.
   b. Type the URL or host name in the accompanying text box.
4. If selecting https, a CA certificate is required for making the connection. Click

to install it. Then you can:
   - Click Show to view the certificate's content.
   - Click Remove to delete the installed certificate if it is inappropriate.
5. If the destination server requires authentication, select the Use Authentication checkbox, and enter the following data.
   - User name

- Password

6. In the Entry Type field, determine the data that will be transmitted.
   - Asset management tag list: Transmit the information of the specified asset strip(s), including the general status of the specified strip(s) and a list of asset tags. The asset tags list also includes those on blade extension strips, if any.
   - Asset management log: Transmit the log of all asset strips, which is generated when there are changes made to asset tags and asset strips, including asset tag connection or disconnection events.
   - Sensor log: Transmit the record of all logged sensors, including their sensor readings and/or status. Logged sensors refer to all internal and/or environmental sensors/actuators that you have selected on the Data Logging page. See ***Setting Data Logging*** (on page 180).

Note: PXE does NOT support asset management strips so you can ignore asset management-related data.

7. Click Create.
8. Repeat the same steps for additional destinations.

To modify or delete data push settings:

1. On the Data Push page, click the one you want in the list.
2. Perform either action below.
   - To modify settings, make necessary changes and then click Save.
   - To delete it, click Delete, and then confirm it on the confirmation message.

Monitoring Server Accessibility

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

PXE can monitor the accessibility of any IT device, such as database servers, remote authentication servers, power distribution units (PDUs), and so on. It supports monitoring a maximum of 8 devices.

The default ping settings may not be suitable for monitoring devices that require high connection reliability so it is strongly recommended that you should adjust the ping settings for optimal results.

Tip: To make the PXE automatically log, send notifications or perform other actions for any server monitoring events, you can create event rules. See **Event Rules and Actions** *(on page 146). An example is available in* **Example: Ping Monitoring and SNMP Notifications** *(on page 185).*

To add IT equipment for ping monitoring:

1. Choose Device Settings > Server Reachability.
2. Click **+ Monitor New Server**.
3. By default, the "Enable ping monitoring for this server" checkbox is selected. If not, select it to enable this feature.
4. Configure the following.

Field	Description
IP address/hostname	IP address or host name of the IT equipment which you want to monitor.
Number of successful pings to enable feature	The number of successful pings required to declare that the monitored equipment is "Reachable." Valid range is 0 to 200.
Wait time after successful ping	The wait time before sending the next ping if the previous ping was successfully responded. Valid range is 5 to 600 (seconds).
Wait time after unsuccessful ping	The wait time before sending the next ping if the previous ping was not responded. Valid range is 3 to 600 (seconds).

Field	Description
Number of consecutive unsuccessful pings for failure	The number of consecutive pings without any response before the monitored equipment is declared "Unreachable." Valid range is 1 to 100.
Wait time before resuming pinging after failure	The wait time before the 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 Create.
6. To add more IT devices, repeat the same steps.

In the beginning, the status of the added IT equipment shows "Waiting for reliable connection," which means the requested number of consecutive successful or unsuccessful pings has not reached before the PXE can declare that the monitored device is reachable or unreachable.

To check the server monitoring states and results:

1. After adding IT equipment for monitoring, all IT devices are listed on the Server Reachability page.
2. The column labeled "Ping Enabled" indicates whether the monitoring for the corresponding IT device is activated or not.
3. The column labeled "Status" indicates the accessibility of 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.

Editing or Deleting Ping Monitoring Settings

You can edit the ping monitoring settings of any IT device or simply delete it if no longer needed.

To modify or delete any monitored IT device:

1. Choose Device Settings > Server Reachability.
2. Click the desired one in the list.
3. Perform the desired action.
   - To modify settings, make necessary changes and then click Save. For information on each field, see *Monitoring Server Accessibility* (on page 183).
   - To delete it, click on the top-right corner.

Example: Ping Monitoring and SNMP Notifications

In this illustration, it is assumed that a significant PDU (IP address: 192.168.84.95) shall be monitored by your 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 sources are different between your PXE and the monitored PDU.

This requires the following two steps.

Step 1: Set up the ping monitoring for the target PDU

1. Choose Device Settings > Server Reachability.
2. Click Monitor New Server.
3. Ensure the "Enable ping monitoring for this server" checkbox is selected.
4. Enter the data shown below.
   - Enter the server's data.

Field	Data entered
IP address/hostname	192.168.84.95

   - To make the PXE declare the accessibility of the monitored PDU every 15 seconds (3 pings * 5 seconds) when that PDU is accessible, enter the following data.

Field	Data entered
Number of successful pings to enable feature	3

Field	Data entered
Wait time after successful ping	5

- To make the PXE declare the inaccessibility of the monitored PDU when that PDU becomes inaccessible for around 12 seconds (4 seconds * 3 pings), enter the following data.

Field	Data entered
Wait time after unsuccessful ping	4
Number of consecutive unsuccessful pings for failure	3

- To make the PXE stop 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, enter the following data.

Field	Data entered
Wait time before resuming pinging after failure	60

- The "Number of consecutive failures before disabling feature (0 = unlimited)" can be set to any value you want.

5. Click Create.

Step 2: Create an event rule to send SNMP notifications for the target PDU

1. Choose Device Settings > Event Rules.
2. Click + New Rule.
3. Select the Enabled checkbox to enable this new rule.
4. Configure the following.

Field/setting	Data specified
Rule name	Send SNMP notifications for PDU (192.168.84.95) inaccessibility
Event	Choose Server Monitoring > 192.168.84.95 > Unreachable
Trigger condition	Select the Unreachable radio button

This will make the PXE react only when the target PDU becomes inaccessible.

5. Select the System SNMP Notification Action.

Note: If you have not configured the System SNMP Notification Action to specify the SNMP destination(s), see **Editing or Deleting a Rule/Action** *(on page 176).*

Lua Scripts

If you can write or obtain any Lua scripts, you can create or load them into the PXE to control its behaviors.

Raritan also provides some Lua scripts examples, which you can load as needed.

Note: Not all Raritan Lua script examples can apply to your PXE model. You should read each example's introduction before applying them.

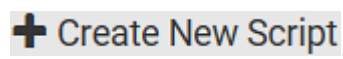
You must have the Administrator Privileges to manage Lua scripts.

Writing or Loading a Lua Script

You can enter or load up to 4 scripts to the PXE.

Tip: If you can no longer enter or load a new script after reaching the upper limit, you can either delete any existing script or simply modify/replace an existing script's codes. See **Modifying or Deleting a Script** *(on page 191).*

To write or load a Lua script:

1. Choose Device Settings > Lua Scripts > 

.
2. Type a name for this script. Its length ranges between 1 to 63 characters.

   The name must contain the following characters only.

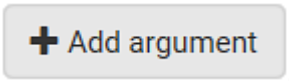
   - Alphanumeric characters
   - Underscore (_)
   - Minus (-)

   Note: Spaces are NOT permitted.

3. Determine whether and when to automatically execute the loaded script.

Checkbox	Behavior when selected
Start automatically at system boot	Whenever the PXE reboots, the script is automatically executed.

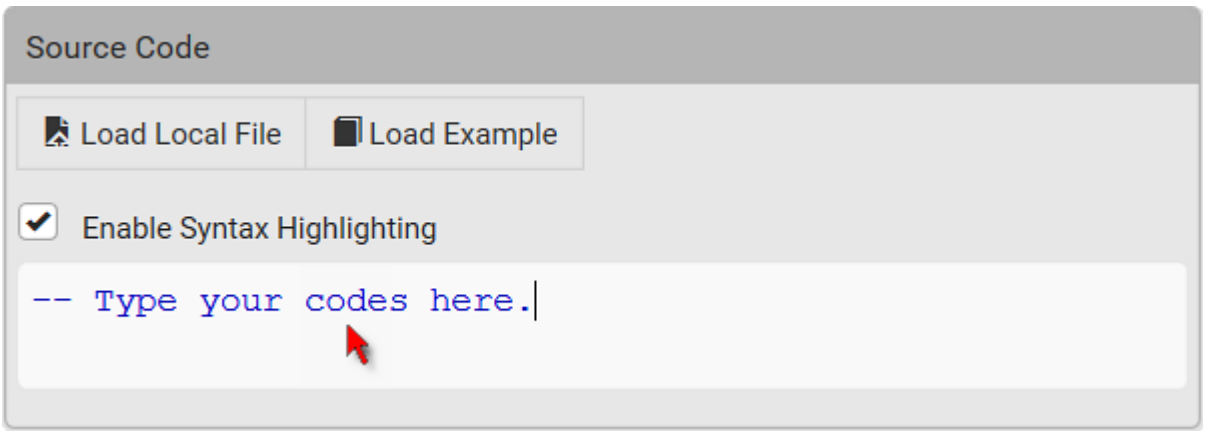
Checkbox	Behavior when selected
Restart after termination	The script is automatically executed each time after 10 seconds since the script execution finishes.

4. (Optional) Determine the arguments that will be executed by default.
   a. Click 

   .
   b. Type the key and value.
   c. Repeat the same steps to enter more arguments as needed.
      - To remove any existing argument, click adjacent to it.

Note: Default arguments are overridden by the new arguments specified with the "Start with Arguments" command or with any Lua-script-related event rule. See **Manually Starting or Stopping a Script** *(on page 189) or* **Start or Stop a Lua Script** *(on page 167).*

5. In the Source Code section, do one of the following. It is recommended to leave the Enable Syntax Highlighting checkbox selected unless you do not need different text colors to identify diverse code syntaxes.
   - To write a Lua script, type the codes in the Source Code section.



   - To load an existing Lua script file, click Load Local File.
   - To use one of Raritan's Lua script examples, click Load Example.

Warning: The newly-loaded script will overwrite all existing codes in the Source Code section. Therefore, do not load a new script if the current script meets your needs.

6. If you chose to load a script or Raritan's example in the previous step, its codes are then displayed in the Source Code section. Double check the codes. If needed, modify the codes to meet your needs.
7. Click Create.

Next steps:

- To execute the newly-added script now, click ▶ Start, or click ⋮ > Start with Arguments. See ***Manually Starting or Stopping a Script*** (on page 189).
- To add more scripts, return to the scripts list by clicking "Lua Scripts" again in the ***Menu*** (on page 53), and then repeat the above steps.

Manually Starting or Stopping a Script

You can manually start or stop an existing Lua script at any time.

When starting a script, you can choose to start it either with its default arguments or with new arguments.

Tip: To have the PXE automatically start or stop a script in response to an event, create an event rule. See **Event Rules and Actions** *(on page 146) and* **Start or Stop a Lua Script** *(on page 167).*

To manually start a script:

1. Choose Device Settings > Lua Scripts. The Lua scripts list displays.

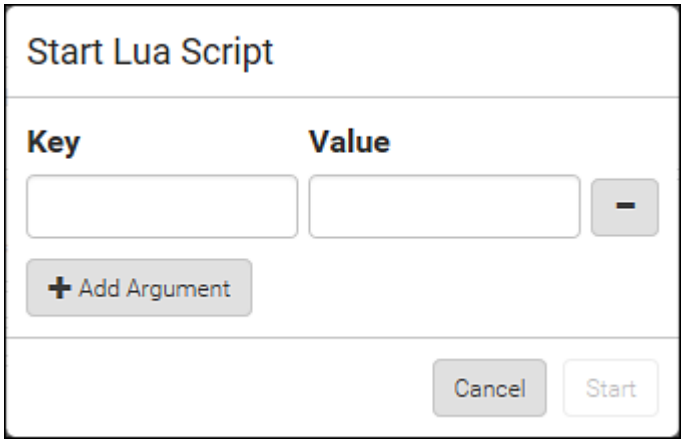
Lua Scripts ✚ Create New Script

Name	State	Autostart	Restart
script-1	Terminated	yes	no
script-2	New	no	yes
script-3	Running	no	no

2. Click the desired script whose state is either 'Terminated' or 'New.' For details, see ***Checking Lua Scripts States*** (on page 191).
3. To start with default arguments, click ▶ Start.

   To start with new arguments, click ⋮ > Start with Arguments. Newly-assigned arguments will override default ones.

4. If you chose "Start with Arguments" in the above step, enter the key and value in the Start Lua Script dialog.
   - Click + Add argument if needing additional arguments.



5. Click Start.
6. The script output will be shown in the Script Output section.
   - If needed, click Clear to delete the existing output data.

To manually stop a script:

1. Choose Device Settings > Lua Scripts.
2. Click the desired script whose state is either 'Running' or 'Restarting.' For details, see *Checking Lua Scripts States* (on page 191).
3. Click Stop on the top-right corner.
4. Click Stop on the confirmation message.

Checking Lua Scripts States

Choose Device Settings > Lua Scripts to show the scripts list, which indicates the current state and settings of each script.

Lua Scripts ✚ Create New Script

Name	State	Autostart	Restart
script-1	Terminated	yes	no
script-2	New	no	yes
script-3	Running	no	no

State:

Four script states are available.

- *New*: The script is never executed since the device boot.
- *Running*: The script is currently being executed.
- *Terminated*: The script was once executed, but stops now.
- *Restarting*: The script will be executed. Only the scripts with the "Restart" column set to "yes" will show this state.

Autostart:

This column indicates whether the checkbox labeled "Start automatically at system boot" is enabled. See ***Writing or Loading a Lua Script*** (on page 187).

Restart:

This column indicates whether the checkbox labeled "Restart after termination" is enabled. See ***Writing or Loading a Lua Script*** (on page 187).

Modifying or Deleting a Script

You can edit an existing script's codes or even replace it with a new script. Or you can simply remove a unnecessary script from the PXE.

To modify or replace a script:

1. Choose Device Settings > Lua Scripts.
2. Click the desired one in the scripts list.

3. Click ⋮ > Edit Script.
4. Make changes to the information shown, except for the script's name, which cannot be revised.
   - To replace the current script, click Load Local File or Load Example to select a new script.

To delete a script:

1. Choose Device Settings > Lua Scripts.
2. Click the desired one in the scripts list.
3. Click ⋮ > Delete.
4. Click Delete on the confirmation message.

Miscellaneous

By default, the Schroff LHX/SHX heat exchanger support and Cisco EnergyWise feature implemented on the PXE are disabled.

However, PXE does NOT support Schroff LHX/SHX so you can ignore the checkbox for this device.

If a Cisco® EnergyWise energy management architecture is implemented in your place, you can enable the Cisco EnergyWise endpoint implemented on the PXE so that this PXE becomes part of the Cisco EnergyWise domain.

To set the Cisco EnergyWise configuration:

1. Choose Device Settings > Miscellaneous.
2. Select the Enable EnergyWise checkbox.
3. Configure the following:

Field	Description
Domain name	Type the name of a Cisco EnergyWise domain where the PXE belongs ▪ Up to 127 printable ASCII characters are permitted. ▪ Spaces and asterisks are NOT acceptable.
Domain password	Type the authentication password (secret) for entering the Cisco EnergyWise domain ▪ Up to 127 printable ASCII characters are permitted. ▪ Spaces and asterisks are NOT acceptable.

Field	Description
Port	Type a User Datagram Protocol (UDP) port number for communications in the Cisco EnergyWise domain. ▪ Range from 1 to 65535. ▪ Default is 43440.
Polling interval	Type a polling interval to determine how often the PXE is queried in the Cisco EnergyWise domain. ▪ Range from 30 to 600 ms. ▪ Default is 180 ms.

4. Click Save in the *EnergyWise* section.

Maintenance

Click 'Maintenance' in the ***Menu*** (on page 53), and the following submenu displays.

Submenu command	Refer to...
Device Information	***Device Information*** (on page 194)
Connected Users	***Viewing Connected Users*** (on page 195)
Event Log	***Viewing or Clearing the Local Event Log*** (on page 196)
Update Firmware	***Updating the PXE Firmware*** (on page 197)
Firmware History	***Viewing Firmware Update History*** (on page 199)
Bulk Configuration	***Bulk Configuration*** (on page 199)
Backup/Restore	***Backup and Restore of Device Settings*** (on page 202)
Network Diagnostic	***Network Diagnostics*** (on page 203)
Download Diagnostic	***Downloading Diagnostic Information*** (on page 204)
Unit Reset	▪ ***Rebooting the PXE Device*** (on page 205) ▪ ***Resetting All Settings to Factory Defaults*** (on page 205)
About iPDU	***Retrieving Software Packages Information*** (on page 206)

Device Information

Using the web interface, you can retrieve hardware and software information of components or peripheral devices connected to your PXE.

Tip: If the information shown on this page does not match the latest status, press F5 to reload it.

To display device information:

1. Choose Maintenance > Device Information.
2. Click the desired section's title bar to show that section's information. For example, click the Network section.

The number of available sections is model dependent.

Section title	Information shown
Information	General device information, such as model name, serial number, firmware version, hardware revision, MIB download link(s) and so on. Note that the download link of LHX-MIB is available only after enabling the Schroff LHX/SHX support. See ***Miscellaneous*** (on page 192).
Network	The network information, such as the current networking mode, IPv4 and/or IPv6 addresses and so on.
Port Forwarding	If the port forwarding mode is activated, this section will show a list of port numbers for all cascaded devices.
Outlets	Each outlet's receptacle type, operating voltage and rated current.
Overcurrent Protectors	Each overcurrent protector's type, rated current and the outlets that it protects.
Controllers	Each inlet or outlet controller's serial number, board ID, firmware version and hardware version.

Section title	Information shown
Inlets	Each inlet's plug type, rated voltage and current.
Peripheral Devices	Serial numbers, model names, position and firmware-related information of connected environmental sensor packages.

Viewing Connected Users

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

To view and manage connected users:

1. Choose Maintenance > Connected Users. A list of logged-in users displays.

   If wanted, you can resort the list by clicking the desired column header. See ***Sorting a List*** (on page 55).

Column	Description
User name	The login name of each connected user.
IP Address	The IP address of each user's host. For the login via a local connection (USB), <local> is displayed instead of an IP address.
Client Type	The interface through which the user is being connected to the PXE. ▪ Web GUI: Refers to the web interface. ▪ CLI: Refers to the command line interface (CLI). The information in parentheses following "CLI" indicates how this user is connected to the CLI. - Serial: The local connection, such as the USB connection. - SSH: The SSH connection. - Telnet: The Telnet connection.
Idle Time	The length of time for which a user remains idle.

2. To disconnect any user, click the corresponding Disconnect.
   a. Click Disconnect on the confirmation message.

b. The disconnected user is forced to log out.

Viewing or Clearing the Local Event Log

By default, the PXE captures certain system events and saves them in a local (internal) event log.

You can view over 2000 historical events that occurred on the PXE in the local event log. When the log size exceeds 256KB, each new entry overwrites the oldest one.

To display the local log:

1. Choose Maintenance > Event Log.

   Each event entry consists of:

   - ID number of the event
   - Date and time of the event
   - Event type
   - A description of the event
2. To view a specific type of events only, select the desired event type in the Filter Event Class field.
   - To refresh the data, press F5 as needed.
3. To go to other pages of the log, click the pagination bar at the bottom of the page.
   - If there are more than 5 pages and the page numbers displayed in the bar does not show the desired one, click ... to have it show the next or previous five page numbers, if available.

4. If wanted, you can resort the list by clicking the desired column header. See *Sorting a List* (on page 55).

To clear the local log:

1. Click on the top-right corner.
2. Click Clear Log on the confirmation message.

Updating the PXE Firmware

Firmware files are available on Raritan website's *Support page* (*http://www.raritan.com/support/*).

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

You must be the administrator or a user 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.

On a multi-inlet PDU (any model with X2 or X3 suffixes), all inlets must be connected to power for the PDU to successfully upgrade its firmware.

Note that firmware upgrade via some mobile devices, such as iPad, requires the use of a file manager app.

To update the firmware:

1. Choose Maintenance > Update Firmware.
2. Click Browse... to select an appropriate firmware file.
3. Click Upload. A progress bar appears to indicate the upload process.
4. Once complete, information of both installed and uploaded firmware versions as well as compatibility and signature-checking results are displayed.
   - If anything is incorrect, click Discard Upload.
5. To proceed with the update, click Update Firmware.

   Warning: Do NOT power off the PXE during the update.

6. During the firmware update:
   - A progress bar appears on the web interface, indicating the update status.
   - The front panel display shows the firmware upgrade message. See *Three-Digit Row* (on page 42).
   - No users can successfully log in to the PXE.
   - Other users' operation, if any, is forced to suspend.
7. When the update is complete, the PXE resets, and the Login page re-appears.
   - Other logged-in users are logged out when the firmware update is complete.

Important: If you are using the 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).

Alternatives:

To use a different method to update the firmware, refer to:

- *Firmware Update via SCP* (on page 344)
- *Bulk Configuration or Firmware Upgrade via DHCP/TFTP* (on page 355)

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 Sunbird's Power IQ, may take additional time beyond the control of the PDU itself. This note does not address the upgrades using other management systems.

Full Disaster Recovery

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/7/10 and Linux. In addition, an appropriate PXE firmware file is required in the recovery procedure.

Viewing Firmware Update History

The firmware upgrade history is permanently stored on the PXE. It remains available even though you perform a device reboot or any firmware update.

To view the firmware update history:

1. Choose Maintenance > Firmware History.

   Each firmware update event consists of:

   - Update date and time
   - Previous firmware version
   - Update firmware version
   - Update result
2. If wanted, you can resort the list by clicking the desired column header. See *Sorting a List* (on page 55).

Bulk Configuration

The Bulk Configuration feature lets you save generic settings of a configured PXE device to your computer. You can use this configuration file to copy common settings to other PXE devices of the same model and firmware version. See *Bulk Configuration Restrictions* (on page 201).

Note that **NO device-specific data is saved** to the bulk configuration file, such as environmental sensors or certain network settings. For a list of device-specific settings that are *not* saved, see *Device-Specific Settings NOT Included* (on page 201).

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.

Tip: To back up or restore "all" settings of a particular PXE device, use the Backup/Restore feature instead. See **Backup and Restore of Device Settings** *(on page 202).*

To save a bulk configuration file:

You must have the Administrator Privileges or "Unrestricted View Privileges" to download the configuration.

1. Log in to the PXE whose settings you want to copy.
2. Choose Maintenance > Bulk Configuration.
3. Click Download Bulk Configuration.
4. When prompted to open or save the configuration file, click Save.

- The file is saved in the XML format, and its content is encrypted using the AES-128 encryption algorithm.

To perform bulk configuration:

You must have the Administrator Privileges to upload the configuration.

1. Log in to another PXE of the same model running the same firmware.
2. Choose Maintenance > Bulk Configuration.
3. Click Browse... to select the configuration file.
4. Click 'Upload & Restore Bulk Configuration' to copy it.
5. A message appears, prompting you to confirm the operation and enter the admin password.

   Enter the admin password, and click Restore.
6. Wait until the PXE device resets and the login page re-appears.

Note: On startup, the PXE performs all of its functions, including event rules and logs, based on the new configuration you have copied instead of the previous configuration prior to the device reset. For example, the "Bulk configuration copied" event is logged only when the new configuration file contains the "Bulk configuration copied" event rule.

The last configuration-copying record:

If you once copied any bulk configuration or device backup file to the PXE, the last record similar to the following is displayed at the bottom of both the Bulk Configuration and Backup/Restore pages.

Last Restore: 2/24/2017, 6:05:53 PM, Status: OK

Alternatives:

To use a different method to perform bulk configuration, refer to:

- *Bulk Configuration via SCP* (on page 345)
- *Bulk Configuration or Firmware Upgrade via DHCP/TFTP* (on page 355)

Device-Specific Settings NOT Included

The settings saved in the bulk configuration file include user and role configurations, thresholds, event rules, security settings, date/time and so on.

Note: 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.

The bulk configuration file does NOT contain device-specific information, including:

- Device name
- SNMP system name, contact and location
- Network settings (IP address, gateway, netmask and so on)
- Device logs
- Names, states and values of environmental sensors and actuators
- TLS certificate
- Server monitoring entries
- Outlet names

Bulk Configuration Restrictions

A source device is the PXE device where the bulk configuration file is downloaded/saved.

A target device is the PXE device that loads this bulk configuration file.

Restrictions for bulk configuration:

- The target device must be running the same firmware version as the source device.
- The target device must be of the same model type as the source device.
- Bulk configuration is permitted if the differences between the target and source devices are only "mechanical" designs 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*

Example:

You can perform bulk configuration between Raritan's PX2-4724-E2N1**K2** and PX2-4724-E2N1**K9**.

- Reason: The two models share the same technical specifications, and the only difference is their chassis colors represented by K2 (blue) and K9 (gray).

Backup and Restore of Device Settings

Unlike the bulk configuration file, the backup file contains ALL device settings, including device-specific data like device names and network settings. To back up or restore a PXE device's 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 bulk configuration among multiple PXE devices, use the Bulk Configuration feature instead. See **Bulk Configuration** *(on page 199).*

To download a backup PXE XML file:

You must have the Administrator Privileges or "Unrestricted View Privileges" to download a backup file.

1. Choose Maintenance > Backup/Restore.
2. 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:

You must have the Administrator Privileges to restore the device settings.

1. Choose Maintenance > Backup/Restore.
2. Click Browse... to select the backup file.
3. Click 'Upload & Restore Device Settings' to upload the file.
   - A message appears, prompting you to confirm the operation and enter the admin password.
4. Enter the admin password, then click Restore.
5. Wait until the 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 you have copied instead of the previous configuration prior to the device reset. For example, the "Bulk configuration copied" event is logged only when the new configuration file contains the "Bulk configuration copied" event rule.

The last configuration-copying record:

If you once copied any bulk configuration or device backup file to the PXE, the last record similar to the following is displayed at the bottom of both the Bulk Configuration and Backup/Restore pages.

Last Restore: 2/24/2017, 6:05:53 PM, Status: OK

Alternative:

To use a different method to perform backup/restore, refer to:

- *Backup and Restore via SCP* (on page 346)

Network Diagnostics

The PXE provides the following tools in the web interface for diagnosing potential networking issues.

- Ping: The tool is useful for checking whether a host is accessible through the network or Internet.
- Trace Route: The tool lets you find out the route over the network between two hosts or systems.
- List TCP Connections: You can use this function to display a list of TCP connections.

Tip: These network diagnostic tools are also available through CLI. See Network Troubleshooting *(on page 339).*

Choose Maintenance > Network Diagnostics, and then perform any function below.

Ping:

1. Type values in the following fields.

Field	Description
Network Host	The name or IP address of the host that you want to check.
Number of Requests	A number up to 20. This determines how many packets are sent for pinging the host.

2. Click Run Ping to ping the host. The Ping results are then displayed.

Trace Route:

1. Type values in the following fields.

Field/setting	Description
Host Name	The IP address or name of the host whose route you want to check.
Timeout(s)	A timeout value in seconds to end the trace route operation.
Use ICMP Packets	To use the Internet Control Message Protocol (ICMP) packets to perform the trace route command, select this checkbox.

2. Click Run. The Trace Route results are then displayed.

List TCP Connections:

1. Click the List TCP Connections title bar to show the list.

Downloading Diagnostic Information

Important: This function is for use by Raritan Field Engineers or when you are directed by Raritan Technical Support.

You can download the diagnostic file from the PXE 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 > Download Diagnostic.
2. The system prompts you to save or open the file. Click Save.
3. E-mail this file as instructed by Raritan Technical Support.

Rebooting the PXE Device

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

Resetting the PXE does not interrupt the operation of connected servers because there is no loss of power to outlets.

▶ **To reboot the device:**

1. Choose Maintenance > Unit Reset > Reboot Unit.
2. Click Reboot to restart 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 restart is complete, the login page opens.

Note: If you are not redirected to the login page after the restart is complete, click the text "this link" in the countdown message.

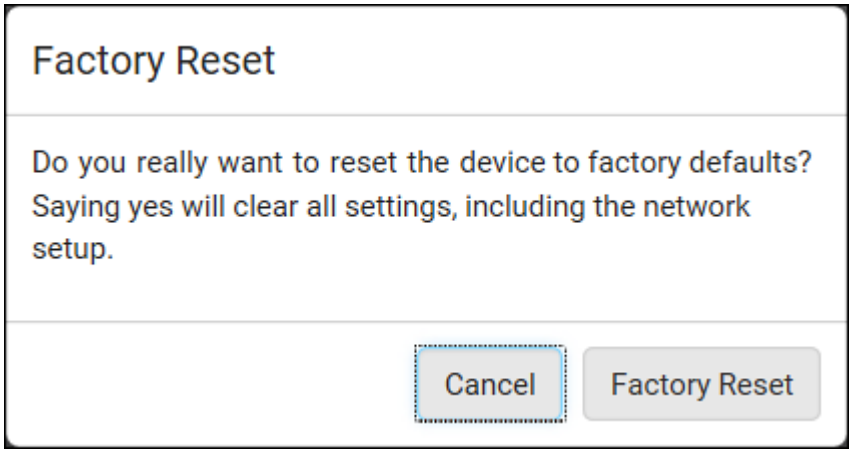
Resetting All Settings to Factory Defaults

You must have the Administrator Privileges to reset all settings of the PXE to factory defaults.

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.

▶ **To reset the device to factory defaults:**

1. Choose Maintenance > Unit Reset > Reset to Factory Defaults.



2. Click Factory Reset to reset the PXE to factory defaults.
3. A message appears, with a countdown timer showing the remaining time of the operation. It takes about two minutes to complete.
4. When the reset is complete, the login page opens.

Note: If you are not redirected to the login page after the reset is complete, click the text "this link" in the countdown message.

Alternative:

There are two more methods to reset the device to factory defaults.

- Use the "mechanical" reset button
- Perform the CLI command

For details, see ***Resetting to Factory Defaults*** (on page 389).

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 Maintenance > About iPDU. A list of open source packages is displayed.
2. You can click any link to access related information or download any software package.

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 and Configuring SNMP.....207
Downloading SNMP MIB 210
SNMP Gets and Sets.....211

Enabling and Configuring SNMP

To communicate with an SNMP manager, you must enable SNMP protocols on the PXE. By default the "read-only" mode of SNMP v1/v2c is enabled.

The SNMP v3 protocol allows for encrypted communication. To take advantage of this, you must configure the users with the SNMP v3 access permission and set Authentication Pass Phrase and Privacy Pass Phrase, which act as shared secrets between SNMP and the PXE.

Important: You must download the SNMP MIB for your PXE to use with your SNMP manager. See *Downloading SNMP MIB* (on page 210).

To enable SNMP v1/v2c and/or v3 protocols:

1. Choose Device Settings > Network Services > SNMP.
2. In the SNMP Agent section, enable SNMP v1/v2c or SNMP v3, and configure related fields, such as the community strings.
   - If SNMP v3 is enabled, you must determine which users shall have the SNMP v3 access permission. See below.

   For details, see ***Configuring SNMP Settings*** (on page 115).

To configure users for SNMP v3 access:

1. Choose User Management > Users.
2. Create or modify users to enable their SNMP v3 access permission.
   - If authentication and privacy is enabled, configure the SNMP password(s) in the user settings.

   For details, see ***Creating Users*** (on page 94).

To enable SNMP notifications:

1. Choose Device Settings > Network Services > SNMP.
2. In the SNMP Notifications section, enable the SNMP notification feature, and configure related fields. For details, refer to:
   - *SNMPv2c Notifications* (on page 208)
   - *SNMPv3 Notifications* (on page 209)

Note: Any changes made to the 'SNMP Notifications' section on the SNMP page will update the settings of the System SNMP Notification Action, and vice versa. See Available Actions *(on page 158).*

SNMPv2c Notifications

1. Choose Device Settings > Network Services > SNMP.
2. In the SNMP Agent, make sure the Enable SNMP v1/v2c checkbox is selected.
3. In the SNMP Notifications section, make sure the Enable SNMP Notifications checkbox is selected.
4. Select SNMPv2c Trap or SNMPv2c Inform as the notification type.
5. Type values in the following fields.

Field	Description
Timeout	The interval of time, in seconds, after which a new inform communication is resent if the first is not received. ▪ For example, resend a new inform communication once every 3 seconds.
Number of Retries	The number of times you want to resend the inform communication if it fails. ▪ For example, inform communications are resent up to 5 times when the initial communication fails.
Host	The IP address of the device(s) you want to access. This is the address to which notifications are sent by the SNMP agent. You can specify up to 3 SNMP destinations.
Port	The port number used to access the device(s).
Community	The SNMP community string to access the device(s). The community is the group representing the PXE and all SNMP management stations.

6. Click Save.

SNMPv3 Notifications

1. Choose Device Settings > Network Services > SNMP.
2. In the SNMP Agent, make sure the Enable SNMP v1/v2c checkbox is selected.
3. In the SNMP Notifications section, make sure the Enable SNMP Notifications checkbox is selected.
4. Select SNMPv3 Trap or SNMPv3 Inform as the notification type.
5. For SNMP TRAPs, the engine ID is prepopulated.
6. Type values in the following fields.

Field	Description
Host	The IP address of the device(s) you want to access. This is the address to which notifications are sent by the SNMP agent.
Port	The port number used to access the device(s).
User ID	User name for accessing the device. ▪ Make sure the user has the SNMP v3 access permission.
Timeout	The interval of time, in seconds, after which a new inform communication is resent if the first is not received. ▪ For example, resend a new inform communication once every 3 seconds.
Number of Retries	Specify the number of times you want to resend the inform communication if it fails. ▪ For example, inform communications are resent up to 5 times when the initial communication fails.
Security Level	Three types are available. ▪ noAuthNoPriv - neither authentication nor privacy protocols are needed. ▪ AuthNoPriv - only authentication is required. ▪ authPriv - both authentication and privacy protocols are required.

Field	Description
Authentication Protocol, Authentication Passphrase, Confirm Authentication Passphrase	The three fields are available when the security level is set to AuthNoPriv or authPriv. ▪ Select the authentication protocol - MD5 or SHA ▪ Enter the authentication passphrase
Privacy Protocol, Privacy Passphrase, Confirm Privacy Passphrase	The three fields are available when the security level is set to authPriv. ▪ Select the Privacy Protocol - DES or AES ▪ Enter the privacy passphrase and then confirm the privacy passphrase

7. Click Save.

Downloading SNMP MIB

You must download an appropriate SNMP MIB file for successful SNMP communications. Always use the latest SNMP MIB downloaded from the current firmware of your PXE.

You can download the MIBs from two different pages of the web interface.

▶ MIB download via the SNMP page:

1. Choose Device Settings > Network Services > SNMP.
2. Click the Download MIBs title bar.

3. Select the desired MIB file to download.
   - PDU2-MIB: The SNMP MIB file for PXE power management.
   - ASSETMANAGEMENT-MIB: The SNMP MIB file for asset management.

   Note: PXE does NOT support the asset management feature so you can ignore the asset management MIB.

4. Click Save to save the file onto your computer.

MIB download via the Device Information page:

1. Choose Maintenance > Device Information.
2. In the Information section, click the desired download link:
   - PDU2-MIB
   - ASSETMANAGEMENT-MIB
3. Click Save to save the file onto your computer.

Note: LHX-MIB is available only after the LHX/SHX support has been enabled. See **Miscellaneous** *(on page 192).*

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.
- 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.

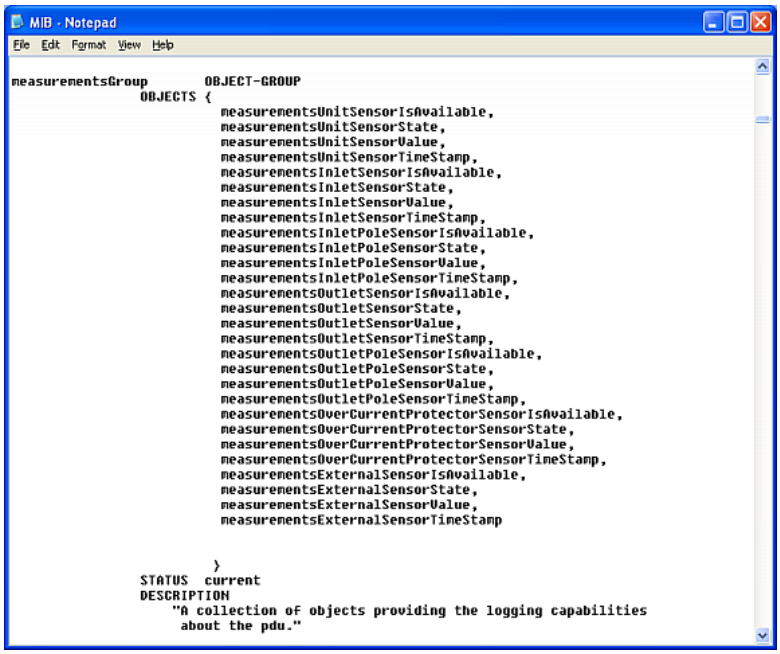
The PXE MIB

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

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.



```
MIB - Notepad
File  Edit  Format  View  Help

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 ***Sensor Threshold Settings*** (on page 446) for a description of how thresholds work.

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

Configuring NTP Server Settings

Using SNMP, you can change the following NTP server-related settings in the unitConfigurationTable:

- Enable or disable synchronization of the device's date and time with NTP servers (synchronizeWithNTPServer)
- Enable or disable the use of DHCP-assigned NTP servers if synchronization with NTP servers is enabled (useDHCPProvidedNTPServer)
- Manually assign the primary NTP server if the use of DHCP-assigned NTP servers is disabled (primaryNTPServerAddressType and primaryNTPServerAddress)
- Manually assign the secondary NTP server (optional) (secondaryNTPServerAddressType and secondaryNTPServerAddress)

Tip: To specify the time zone, use the CLI or web interface instead. For the CLI, see Setting the Time Zone *(on page 271). For the web interface, see* Setting the Date and Time *(on page 143).*

When using the SNMP SET command to specify or change NTP servers, it is required that both the NTP server's address type and address be set in the command line simultaneously.

For example, the SNMP command to change the primary NTP server's address from IPv4 (192.168.84.84) to host name looks similar to the following:

```
snmpset -v2c -c private 192.168.84.84
firstNTPServerAddressType = dns firstNTPServerAddress =
"angu.pep.com"
```

A Note about Enabling Thresholds

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

Chapter 8 Using the Command Line Interface

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

CLI commands are case sensitive.

In This Chapter

About the Interface 215
Logging in to CLI 216
Logging out of CLI 218
Help Command 219
Querying Available Parameters for a Command 220
Showing Information 220
Clearing Information 245
Configuring the PXE Device and Network 246
Actuator Control Operations 335
Unblocking a User 337
Resetting the PXE 337
Network Troubleshooting 339
Retrieving Previous Commands 342
Automatically Completing a Command 342

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 **Changing Telnet Settings** *(on page 119).*

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 218) 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 ***Configuring Network Services*** (on page 114) 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 218) 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 246).
- 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 339).

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 220).*

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 218).*

Network Configuration

This command shows all network configuration and all network interfaces' information, such as the IP address, MAC address, the Ethernet interface's duplex mode, and the wireless interface's status/settings.

```
#        show network
```

Note: PXE does NOT support wireless networking so you can ignore the wireless information in the CLI.

IP Configuration

This command shows the IP-related configuration only, such as IPv4 and IPv6 configuration, address(es), gateway, and subnet mask.

Tip: To show IPv4-only and IPv6-only configuration data, see **IPv4-Only or IPv6-Only Configuration** *(on page 222).*

```
#        show network ip common
```

To show the IP-related configuration of a specific network interface, use the following command.

```
#        show network ip interface <ETH>
```

Variables:

- <ETH> is one of the network interfaces: *ethernet*, *wireless*, *bridge* or *all*. Note that you must choose/configure the bridge interface if your PXE is set to the bridging mode.

  Note: In the bridging mode, only the IP parameters of the BRIDGE interface function. The IP parameters of the ETHERNET and WIRELESS interfaces do NOT function.

Option	Description
ethernet	Show the IP-related configuration of the ETHERNET interface.
wireless	Show the IP-related configuration of the WIRELESS interface.
bridge	Show the IP-related configuration of the BRIDGE interface.

Option	Description
all	Show the IP-related configuration of all interfaces. You can type the CLI command without the word 'all.' For example, *show network ip interface*.

Note: PXE does NOT support wireless networking so you can ignore the wireless information in the CLI.

IPv4-Only or IPv6-Only Configuration

To show IPv4-only configuration or IPv6-only configuration, use any of the following commands.

Tip: To show both IPv4 and IPv6 configuration data, see IP Configuration *(on page 221).*

▶ **To show all IPv4 configuration:**

```
#        show network ipv4 common
```

▶ **To show all IPv6 configuration:**

```
#        show network ipv6 common
```

▶ **To show the IPv4 configuration of a specific network interface:**

```
#        show network ipv4 interface <ETH>
```

▶ **To show the IPv6 configuration of a specific network interface:**

```
#        show network ipv6 interface <ETH>
```

Variables:

- <ETH> is one of the network interfaces: *ethernet*, *wireless*, *bridge* or *all*. Note that you must choose/configure the bridge interface if your PXE is set to the bridging mode.

  Note: In the bridging mode, only the IP parameters of the BRIDGE interface function. The IP parameters of the ETHERNET and WIRELESS interfaces do NOT function.

Option	Description
ethernet	Show the IPv4 or IPv6 configuration of the ETHERNET interface.
wireless	Show the IPv4 or IPv6 configuration of the WIRELESS interface.
bridge	Show the IPv4 or IPv6 configuration of the BRIDGE interface.
all	Show the IPv4 or IPv6 configuration of all interfaces. You can type the CLI command without the word 'all.' For example, *show network ipv4 interface*.

Note: PXE does NOT support wireless networking so you can ignore the wireless information in the CLI.

Network Interface Settings

This command shows the specified network interface's information which is NOT related to IP configuration. For example, the Ethernet port's LAN interface speed and duplex mode, or the wireless interface's SSID parameter and authentication protocol.

```
#        show network interface <ETH>
```

Variables:

- <ETH> is one of the network interfaces: *ethernet*, *wireless*, *bridge* or *all*. Note that you must choose/configure the bridge interface if your PXE is set to the bridging mode.

  Note: In the bridging mode, only the IP parameters of the BRIDGE interface function. The IP parameters of the ETHERNET and WIRELESS interfaces do NOT function.

Option	Description
ethernet	Show the ETHERNET interface's non-IP settings.
wireless	Show the WIRELESS interface's non-IP settings.
bridge	Show the BRIDGE interface's non-IP settings.

Option	Description
all	Show the non-IP settings of all interfaces. You can type the CLI command without the word 'all.' For example, *show network interface*.

Note: PXE does NOT support wireless networking so you can ignore the wireless information in the CLI.

Network Service Settings

This command shows the network service settings only, including the Telnet setting, TCP ports for HTTP, HTTPS, SSH and Modbus/TCP services, and SNMP settings.

```
#        show network services <option>
```

Variables:

- <option> is one of the options: *all*, *http*, *https*, *telnet*, *ssh*, *snmp*, *modbus* and *zeroconfig*.

Option	Description
all	Displays the settings of all network services, including HTTP, HTTPS, Telnet, SSH and SNMP. *Tip: You can also type the command without adding this option "all" to get the same data.*
http	Only displays the TCP port for the HTTP service.
https	Only displays the TCP port for the HTTPS service.
telnet	Only displays the settings of the Telnet service.
ssh	Only displays the settings of the SSH service.
snmp	Only displays the SNMP settings.
modbus	Only displays the settings of the Modbus/TCP service.
zeroconfig	Only displays the settings of the zero configuration advertising.

PDU Configuration

This command shows the PDU configuration, such as the device name, firmware version and model type.

```
#          show pdu
```

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

```
#          show pdu details
```

Outlet Information

This command syntax shows the outlet information.

```
#          show outlets <n>
```

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

```
#          show outlets <n> details
```

Variables:

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

Option	Description
all	Displays the information for all outlets. *Tip: You can also type the command without adding this option "all" to get the same data.*
A specific outlet number	Displays the information for the specified outlet only.

Displayed information:

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

Inlet Information

This command syntax shows the inlet information.

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

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

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

Variables:

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

Option	Description
all	Displays the information for all inlets. *Tip: You can also type the command without adding this option "all" to get the same data.*
A specific inlet number	Displays the information for the specified inlet only. An inlet number needs to be specified only when there are more than 1 inlet on your PDU.

Displayed information:

- Without the parameter "details," only the inlet's name and RMS current are displayed.
- With the parameter "details," more inlet information is displayed in addition to the inlet name and RMS current, such as the inlet's RMS voltage, active power and active energy.

Overcurrent Protector Information

This command is only available for models with overcurrent protectors for protecting outlets.

This command syntax shows the overcurrent protector information, such as a circuit breaker or a fuse.

```
#        show ocp <n>
```

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

```
#        show ocp <n> details
```

Variables:

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

Option	Description
all	Displays the information for all overcurrent protectors. *Tip: You can also type the command without adding this option "all" to get the same data.*
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 238) for the preferred measurement units for a specific user.*

Environmental Sensor Information

This command syntax shows the environmental sensor's information.

```
#        show externalsensors <n>
```

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

```
#        show externalsensors <n> details
```

```
External sensor 3 ('Temperature 1')
Sensor type: Temperature
Reading:    31.8 deg C (normal)

Serial number:        AEI0950133
Description:          Not configured
Location:            X Not configured
                    Y Not configured
                    Z Not configured
Position:             Port 1
Using default thresholds: yes
```

Variables:

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

Option	Description
all	Displays the information of all environmental sensors. *Tip: You can also type the command without adding this option "all" to get the same data.*
A specific environmental sensor number*	Displays the information for the specified environmental sensor only.

* The environmental sensor number is the ID number assigned to the sensor, which can be found on the Peripherals page of the PXE web interface.

Displayed information:

- Without the parameter "details," only the sensor ID, sensor type and reading are displayed.

  Note: A state sensor displays the sensor state instead of the reading.

- With the parameter "details," more information is displayed in addition to the ID number and sensor reading, such as the serial number, sensor position, and X, Y, and Z coordinates.

Note: DPX sensor packages do not provide chain position information.

Actuator Information

This command syntax shows an actuator's information.

```
#        show actuators <n>
```

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

```
#        show actuators <n> details
```

Variables:

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

Option	Description
all	Displays the information for all actuators. *Tip: You can also type the command without adding this option "all" to get the same data.*
A specific actuator number*	Displays the information for the specified actuator only.

* The actuator number is the ID number assigned to the actuator. The ID number can be found using the 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 Peripherals 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 state sensor, the threshold-related and accuracy-related data is NOT available.

Environmental Sensor Default Thresholds

This command syntax shows a certain sensor type's default thresholds, which are the initial thresholds applying to the specified type of sensor.

```
#        show defaultThresholds <sensor type>
```

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

```
#        show defaultThresholds <sensor type> details
```

Variables:

- <sensor type> is one of the following numeric sensor types:

Sensor types	Description
absoluteHumidity	Absolute humidity sensors
relativeHumidity	Relative humidity sensors
temperature	Temperature sensors
airPressure	Air pressure sensors
airFlow	Air flow sensors
vibration	Vibration sensors
all	All of the above numeric sensors *Tip: You can also type the command without adding this option "all" to get the same data.*

Displayed information:

- Without the parameter "details," only the default upper and lower thresholds, deassertion hysteresis and assertion timeout settings of the specified sensor type are displayed.
- With the parameter "details," the threshold range is displayed in addition to default thresholds settings.

Security Settings

This command shows the security settings of the 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. *Tip: You can also type the command without adding this option "all" to get the same data.*
a specific user's name	This option shows the profile of the specified user only.

Displayed information:

- Without the parameter "details," only four pieces of user information are displayed: user name, user "Enabled" status, SNMP v3 access privilege, and role(s).
- With the parameter "details," more user information is displayed, such as the telephone number, e-mail address, preferred measurement units and so on.

Existing Roles

This command shows the data of one or all existing roles.

```
#        show roles <role_name>
```

Variables:

- <role_name> is the name of the role whose permissions you want to query. The variable can be one of the following options:

Option	Description
all	This option shows all existing roles. *Tip: You can also type the command without adding this option "all" to get the same data.*
a specific role's name	This option shows the data of the specified role only.

Displayed information:

- Role settings are displayed, including the role description and privileges.

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.

Event type	Description
sensor	Internal or external sensor events, such as state changes of any sensors.
serverMonitor	Server-monitoring records, such as a server being declared reachable or unreachable.
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. *Tip: You can also type the command without adding this option "0" to get all data.*
A specific integer number	Displays the specified number of last entries in the reliability error log.

Examples

This section provides examples of the show command.

Example 1 - Basic Security Information

The diagram shows the output of the *show security* command.

```
# show security
IPv4 access control: Disabled

IPv6 access control: Disabled

Role based access control for IPv4: Disabled

Role based access control for IPv6: Disabled

Password aging: Disabled

Prevent concurrent user login:   No

Strong passwords: Disabled

Enforce HTTPS for web access: Yes

Restricted Service Agreement: disabled
```

Example 2 - In-Depth Security Information

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

```
# show security details
IPv4 access control: Disabled

IPv6 access control: Disabled


Role based access control for IPv4: Disabled

Role based access control for IPv6: Disabled

Password aging: Disabled

Prevent concurrent user login:   No
Maximum number of failed logins: 3
User block time:                 10 minutes

User idle timeout: 1440 minutes

Strong passwords: Disabled

Enforce HTTPS for web access: Yes

Restricted Service Agreement: disabled
Restricted Service Agreement Banner Content:
Unauthorized access prohibited; all access and activities not explicitly authori
zed by management are unauthorized. All activities are monitored and logged. The
re is no privacy on this system. Unauthorized access and activities or any crimi
nal activity will be reported to appropriate authorities.
```

Example 3 - Basic PDU Information

The diagram shows the output of the *show pdu* command.

```
# show pdu
PDU 'my PX'
Model:            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 218).*

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 218).*

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 246).**

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 218).

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 180).

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 180).

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 455).

```
config:#    pdu deviceAltitude <altitude>
```

Variables:

- <altitude> is an integer between 1 and 3000 meters.

Setting the Z Coordinate Format for Environmental Sensors

This command enables or disables the use of rack units for specifying the height (Z coordinate) of environmental sensors.

```
config:#   pdu externalSensorsZCoordinateFormat <option>
```

Variables:

- <option> is one of the options: *rackUnits* or *freeForm*.

Option	Description
rackUnits	The height of the Z coordinate is measured in standard rack units. When this is selected, you can type a numeric value in the rack unit to describe the Z coordinate of any environmental sensors or actuators.
freeForm	Any alphanumeric string can be used for specifying the Z coordinate.

Note: After determining the format for the Z coordinate, you can set a value for it. See Setting the Z Coordinate *(on page 316).*

Enabling or Disabling Peripheral Device Auto Management

This command enables or disables the Peripheral Device Auto Management feature.

```
config:#   pdu peripheralDeviceAutoManagement <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	Enables the automatic management feature for environmental sensor packages.
disable	Disables the automatic management feature for environmental sensor packages.

For more information, see ***How the Automatic Management Function Works*** (on page 67).

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.

Configuring IPv4 Parameters

An IPv4 configuration command begins with *network ipv4*.

Setting the IPv4 Configuration Mode

This command determines the IP configuration mode.

```
config:#   network ipv4 interface <ETH> configMethod <mode>
```

Variables:

- <ETH> is one of the network interfaces: *ethernet*, *wireless*, *bridge* or *all*. Note that you must choose/configure the bridge interface if your PXE is set to the bridging mode.

  Note: In the bridging mode, only the IP parameters of the BRIDGE interface function. The IP parameters of the ETHERNET and WIRELESS interfaces do NOT function.

Interface	Description
ethernet	Determine the IPv4 configuration mode of the ETHERNET interface (that is, wired networking).

Interface	Description
wireless	Determine the IPv4 configuration mode of the WIRELESS interface (that is, wireless networking).
bridge	Determine the IPv4 configuration mode of the BRIDGE interface (that is, bridging mode).

- <mode> is one of the modes: *dhcp* or *static*.

Mode	Description
dhcp	The IPv4 configuration mode is set to DHCP.
static	The IPv4 configuration mode is set to static IP address.

Note: PXE does NOT support wireless networking so you can ignore the wireless information in the CLI.

Setting the IPv4 Preferred Host Name

After selecting DHCP as the IPv4 configuration mode, you can specify the preferred host name, which is optional. The following is the command:

```
config:#   network ipv4 interface <ETH> preferredHostName <name>
```

Variables:

- <ETH> is one of the network interfaces: *ethernet*, *wireless*, *bridge* or *all*. Note that you must choose/configure the bridge interface if your PXE is set to the bridging mode.

  Note: In the bridging mode, only the IP parameters of the BRIDGE interface function. The IP parameters of the ETHERNET and WIRELESS interfaces do NOT function.

Interface	Description
ethernet	Determine the IPv4 preferred host name of the ETHERNET interface (that is, wired networking).
wireless	Determine the IPv4 preferred host name of the WIRELESS interface (that is, wireless networking).
bridge	Determine the IPv4 preferred host name of the BRIDGE interface (that is, bridging mode).

- <name> is a host name which:
  - Consists of alphanumeric characters and/or hyphens
  - Cannot begin or end with a hyphen
  - Cannot contain more than 63 characters
  - Cannot contain punctuation marks, spaces, and other symbols

Note: PXE does NOT support wireless networking so you can ignore the wireless information in the CLI.

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 interface <ETH> address <ip address>
```

Variables:

- <ETH> is one of the network interfaces: *ethernet*, *wireless*, *bridge* or *all*. Note that you must choose/configure the bridge interface if your PXE is set to the bridging mode.

  Note: In the bridging mode, only the IP parameters of the BRIDGE interface function. The IP parameters of the ETHERNET and WIRELESS interfaces do NOT function.

Interface	Description
ethernet	Determine the IPv4 address of the ETHERNET interface (that is, wired networking).
wireless	Determine the IPv4 address of the WIRELESS interface (that is, wireless networking).
bridge	Determine the IPv4 address of the BRIDGE interface (that is, the bridging mode).

- <ip address> is the IP address being assigned to your PXE device. Its format is "IP address/prefix". For example, *192.168.84.99/32*.

Note: PXE does NOT support wireless networking so you can ignore the wireless information in the CLI.

Setting the IPv4 Gateway

After selecting the static IP configuration mode, you can use this command to specify the gateway.

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

Variables:

- <ip address> is the IP address of the gateway. The value ranges from 0.0.0.0 to 255.255.255.255.

Setting IPv4 Static Routes

If the IPv4 network mode is set to static IP and your local network contains two subnets, you can configure static routes to enable or disable communications between the PXE and devices in the other subnet.

These commands are prefixed with *network ipv4 staticRoutes*.

Depending on whether the other network is directly reachable or not, there are two methods for adding a static route. For further information, see ***Static Route Examples*** (on page 110).

▶ **Method 1: add a static route when the other network is NOT directly reachable:**

```
config:#   network ipv4 staticRoutes add <dest-1> <hop>
```

▶ **Method 2: add a static route when the other network is directly reachable:**

```
config:#   network ipv4 staticRoutes add <dest-1> interface <ETH>
```

▶ **Delete an existing static route:**

```
config:#   network ipv4 staticRoutes delete <route_ID>
```

▶ **Modify an existing static route:**

```
config:#   network ipv4 staticRoutes modify <route_ID> <dest-2> <hop>
```

-- OR --

```
config:#   network ipv4 staticRoutes modify <route_ID> <dest-2> interface <ETH>
```

Variables:

- <dest-1> is a combination of the IP address and subnet mask of the other subnet. The format is *IP address/subnet mask*.
- <hop> is the IP address of the next hop router.
- <ETH> is one of the interfaces: *ethernet*, *wireless* and *bridge*. Type "bridge" only when your PXE is in the bridging mode.
- <route_ID> is the ID number of the route setting which you want to delete or modify.
- <dest-2> is a modified route setting that will replace the original route setting. Its format is *IP address/subnet mask*. You can modify either the IP address or the subnet mask or both.

Note: PXE does NOT support wireless networking so you can ignore the wireless information in the CLI.

Configuring IPv6 Parameters

An IPv6 configuration command begins with *network ipv6*.

Setting the IPv6 Configuration Mode

This command determines the IP configuration mode.

```
config:#   network ipv6 interface <ETH> configMethod <mode>
```

Variables:

- <ETH> is one of the network interfaces: *ethernet*, *wireless*, *bridge* or *all*. Note that you must choose/configure the bridge interface if your PXE is set to the bridging mode.

  Note: In the bridging mode, only the IP parameters of the BRIDGE interface function. The IP parameters of the ETHERNET and WIRELESS interfaces do NOT function.

Interface	Description
ethernet	Determine the IPv6 configuration mode of the ETHERNET interface (that is, wired networking).
wireless	Determine the IPv6 configuration mode of the WIRELESS interface (that is, wireless networking).

Interface	Description
bridge	Determine the IPv6 configuration mode of the BRIDGE interface (that is, bridging mode).

- <mode> is one of the modes: *automatic* or *static*.

Mode	Description
automatic	The IPv6 configuration mode is set to automatic.
static	The IPv6 configuration mode is set to static IP address.

Note: PXE does NOT support wireless networking so you can ignore the wireless information in the CLI.

Setting the IPv6 Preferred Host Name

After selecting DHCP as the IPv6 configuration mode, you can specify the preferred host name, which is optional. The following is the command:

```
config:#   network ipv6 interface <ETH> preferredHostName <name>
```

Variables:

- <ETH> is one of the network interfaces: *ethernet*, *wireless*, *bridge* or *all*. Note that you must choose/configure the bridge interface if your PXE is set to the bridging mode.

  Note: In the bridging mode, only the IP parameters of the BRIDGE interface function. The IP parameters of the ETHERNET and WIRELESS interfaces do NOT function.

Interface	Description
ethernet	Determine the IPv6 preferred host name of the ETHERNET interface (that is, wired networking).
wireless	Determine the IPv6 preferred host name of the WIRELESS interface (that is, wireless networking).
bridge	Determine the IPv6 preferred host name of the BRIDGE interface (that is, bridging mode).

Note: PXE does NOT support wireless networking so you can ignore the wireless information in the CLI.

- <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 interface <ETH> address <ip
           address>
```

Variables:

- <ETH> is one of the network interfaces: *ethernet*, *wireless*, *bridge* or *all*. Note that you must choose/configure the bridge interface if your PXE is set to the bridging mode.

  Note: In the bridging mode, only the IP parameters of the BRIDGE interface function. The IP parameters of the ETHERNET and WIRELESS interfaces do NOT function.

Interface	Description
ethernet	Determine the IPv6 address of the ETHERNET interface (that is, wired networking).
wireless	Determine the IPv6 address of the WIRELESS interface (that is, wireless networking).
bridge	Determine the IPv6 address of the BRIDGE interface (that is, the bridging mode).

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

Note: PXE does NOT support wireless networking so you can ignore the wireless information in the CLI.

Setting the IPv6 Gateway

After selecting the static IP configuration mode, you can use this command to specify the gateway.

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

Variables:

- <ip address> is the IP address of the gateway. This value uses the IPv6 address format.

Setting IPv6 Static Routes

If the IPv6 network mode is set to static IP and your local network contains two subnets, you can configure static routes to enable or disable communications between the PXE and devices in the other subnet.

These commands are prefixed with *network ipv6 staticRoutes*.

Depending on whether the other network is directly reachable or not, there are two methods for adding a static route. For further information, see ***Static Route Examples*** (on page 110).

▶ **Method 1: add a static route when the other network is NOT directly reachable:**

```
config:#   network ipv6 staticRoutes add <dest-1> <hop>
```

▶ **Method 2: add a static route when the other network is directly reachable:**

```
config:#   network ipv6 staticRoutes add <dest-1> interface <ETH>
```

▶ **Delete an existing static route:**

```
config:#   network ipv6 staticRoutes delete <route_ID>
```

▶ **Modify an existing static route:**

```
config:#   network ipv6 staticRoutes modify <route_ID> <dest-2> <hop>
```

-- OR --

```
config:#    network ipv6 staticRoutes modify <route_ID> <dest-2> interface <ETH>
```

Variables:

- <dest-1> is the IP address and prefix length of the subnet where the PXE belongs. The format is *IP address/prefix length*.
- <hop> is the IP address of the next hop router.
- <ETH> is one of the interfaces: *ethernet*, *wireless* and *bridge*. Type "bridge" only when your PXE is in the bridging mode.
- <route_ID> is the ID number of the route setting which you want to delete or modify.
- <dest-2> is a modified route setting that will replace the original route setting. Its format is *IP address/prefix length*. You can modify either the IP address or the prefix length or both.

Note: PXE does NOT support wireless networking so you can ignore the wireless information in the CLI.

Configuring DNS Parameters

Use the following commands to configure DNS-related settings.

- **Specify the primary DNS server:**

```
config:#   network dns firstServer <ip address>
```

- **Specify the secondary DNS server:**

```
config:#   network dns secondServer <ip address>
```

- **Specify the third DNS server:**

```
config:#   network dns thirdServer <ip address>
```

- **Determine which IP address is used when the DNS server returns both IPv4 and IPv6 addresses:**

```
config:#   network dns resolverPreference <resolver>
```

Variables:

- <ip address> is the IP address of the DNS server.
- <resolver> is one of the options: *preferV4* or *preferV6.*

Option	Description
preferV4	Use the IPv4 addresses returned by the DNS server.
preferV6	Use the IPv6 addresses returned by the DNS server.

Setting LAN Interface Parameters

A LAN interface configuration command begins with *network ethernet*.

Enabling or Disabling the LAN Interface

This command enables or disables the LAN interface.

```
config:#   network ethernet ETHERNET enabled <option>
```

Variables:

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

Option	Description
true	The specified network interface is enabled.
false	The specified network interface is disabled.

Changing the LAN Interface Speed

This command determines the LAN interface speed.

```
config:#   network ethernet ETHERNET speed <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 ethernet ETHERNET duplexMode <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.

Option	Description
false	The Telnet service is disabled.

Changing the Telnet Port

This command changes the Telnet port.

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

Variables:

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

Changing the SSH Configuration

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

An SSH command begins with *network services ssh*.

Enabling or Disabling SSH

This command enables or disables the SSH service.

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

Variables:

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

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

Changing the SSH Port

This command changes the SSH port.

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

Variables:

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

Determining the SSH Authentication Method

This command syntax determines the SSH authentication method.

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

Variables:

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

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

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

This command enables or disables the zero configuration protocol, which enables advertising or auto discovery of network services. See *Enabling Service Advertising* (on page 120) 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.

Deleting an NTP Server

The following commands delete the primary and/or secondary time server(s).

▶ **To delete the primary time server:**

```
config:#   time ntp firstServer ""
```

▶ **To delete the secondary time server:**

```
config:#   time ntp secondServer ""
```

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 *2015-11-30* for November 30, 2015.
<hh:mm:ss>	Type the time in the format of hh:mm:ss in the 24-hour format. For example, type *13:50:20* for 1:50:20 pm.

Setting the Automatic Daylight Savings Time

This command determines whether the daylight savings time is applied to the time settings.

```
config:#   time autoDST <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Mode	Description
enable	Daylight savings time is enabled.
disable	Daylight savings time is disabled.

Examples

This section illustrates several time configuration examples.

Example 1 - Time Setup Method

The following command sets the date and time settings by using the NTP servers.

```
config:#   time method ntp
```

Example 2 - Primary NTP Server

The following command sets the primary time server to 192.168.80.66.

```
config:#   time ntp firstServer 192.168.80.66
```

Checking the Accessibility of NTP Servers

This command verifies the accessibility of NTP servers specified manually on your 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 218).

▶ 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 334).*

Managing Firewall Rules

You can add, delete or modify firewall rules using the CLI commands.

- An IPv4 firewall control rule command begins with *security ipAccessControl ipv4 rule*.
- An IPv6 firewall control rule command begins with *security ipAccessControl ipv6 rule*.

Adding a Firewall Rule

Depending on where you want to add a new firewall rule in the list, the command for adding a rule varies.

- *IPv4 commands*

▶ **Add a new rule to the bottom of the IPv4 rules list:**

```
config:#    security ipAccessControl ipv4 rule add <direction> <ip_mask> <policy>
```

▶ **Add a new IPv4 rule by inserting it above or below a specific rule:**

```
config:#    security ipAccessControl ipv4 rule add <direction> <ip_mask> <policy> <insert>
            <rule_number>
```

-- OR --

```
config:#    security ipAccessControl ipv4 rule add <direction> <insert> <rule_number>
            <ip_mask> <policy>
```

- *IPv6 commands*

▶ **Add a new rule to the bottom of the IPv6 rules list:**

```
config:#    security ipAccessControl ipv6 rule add <direction> <ip_mask> <policy>
```

▶ **Add a new IPv6 rule by inserting it above or below a specific rule:**

```
config:#    security ipAccessControl ipv6 rule add <direction> <ip_mask> <policy> <insert>
            <rule_number>
```

-- OR --

```
config:#    security ipAccessControl ipv6 rule add <direction> <insert> <rule_number>
            <ip_mask> <policy>
```

Variables:

- <direction> is one of the options: *in* or *out*.

Direction	Description
in	Inbound traffic.
out	Outbound traffic.

- <ip_mask> is the combination of the IP address and subnet mask values (or prefix length), which are separated with a slash. For example, an IPv4 combination looks like this: *192.168.94.222/24*.
- <policy> is one of the options: *accept, drop* or *reject*.

Policy	Description
accept	Accepts traffic from/to the specified IP address(es).
drop	Discards traffic from/to the specified IP address(es), without sending any failure notification to the source or destination host.
reject	Discards traffic from/to the specified IP address(es), and an ICMP message is sent to the source or destination host for failure notification.

- <insert> is one of the options: *insertAbove* or *insertBelow*.

Option	Description
insertAbove	Inserts the new rule above the specified rule number. Then: *new rule's number = the specified rule number*
insertBelow	Inserts the new rule below the specified rule number. Then: *new rule's number = the specified rule number + 1*

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

Modifying a Firewall Rule

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

- *IPv4 commands*

▶ **Modify an IPv4 rule's IP address and/or subnet mask:**

```
config:#    security ipAccessControl ipv4 rule modify <direction> <rule_number> ipMask
            <ip_mask>
```

▶ **Modify an IPv4 rule's policy:**

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

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

```
config:#    security ipAccessControl ipv4 rule modify <direction> <rule_number> ipMask
            <ip_mask> policy <policy>
```

- *IPv6 commands*

▶ **Modify an IPv6 rule's IP address and/or prefix length:**

```
config:#    security ipAccessControl ipv6 rule modify <direction> <rule_number> ipMask
            <ip_mask>
```

▶ **Modify an IPv6 rule's policy:**

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

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

```
config:#    security ipAccessControl ipv6 rule modify <direction> <rule_number> ipMask
            <ip_mask> policy <policy>
```

Variables:

- <direction> is one of the options: *in* or *out*.

Direction	Description
in	Inbound traffic.
out	Outbound traffic.

- <rule_number> is the number of the existing rule that you want to modify.
- <ip_mask> is the combination of the IP address and subnet mask values (or prefix length), which are separated with a slash. For example, an IPv4 combination looks like this: *192.168.94.222/24*.
- <policy> is one of the options: *accept, drop* or *reject*.

Option	Description
accept	Accepts traffic from/to the specified IP address(es).
drop	Discards traffic from/to the specified IP address(es), without sending any failure notification to the source or destination host.
reject	Discards traffic from/to the specified IP address(es), and an ICMP message is sent to the source or destination host for failure notification.

Deleting a Firewall Rule

The following commands remove a specific IPv4 or IPv6 rule from the list.

▶ IPv4 commands

```
config:#   security ipAccessControl ipv4 rule delete <direction> <rule_number>
```

▶ IPv6 commands

```
config:#   security ipAccessControl ipv6 rule delete <direction> <rule_number>
```

Variables:

- <direction> is one of the options: *in* or *out*.

Direction	Description
in	Inbound traffic.
out	Outbound traffic.

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

Restricted Service Agreement

The CLI command used to set the Restricted Service Agreement feature begins with `security restrictedServiceAgreement`,

Enabling or Disabling the Restricted Service Agreement

This command activates or deactivates the Restricted Service Agreement.

```
config:#   security restrictedServiceAgreement enabled <option>
```

Variables:

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

Option	Description
true	Enables the Restricted Service Agreement feature.
false	Disables the Restricted Service Agreement feature.

After the Restricted Service Agreement feature is enabled, the agreement's content is displayed in the login screen.

Do either of the following, or the login fails:

- In the web interface, select the checkbox labeled "I understand and accept the Restricted Service Agreement."

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

- In the CLI, type y when the confirmation message "I understand and accept the Restricted Service Agreement" is displayed.

Specifying the Agreement Contents

This command allows you to create or modify contents of the Restricted Service Agreement.

```
config:#   security restrictedServiceAgreement bannerContent
```

After performing the above command, do the following:

1. Type the text comprising up to 10,000 ASCII characters when the CLI prompts you to enter the content.
2. To end the content:

a. Press Enter.
b. Type `--END--` to indicate the end of the content.
c. Press Enter again.

If the content is successfully entered, the CLI displays this message "Successfully entered Restricted Service Agreement" followed by the total number of entered characters in parentheses.

Note: The new content of Restricted Service Agreement is saved only after typing the `apply` *command. See* **Quitting Configuration Mode** *(on page 246).*

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 334).

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 334).

▶ **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 334).

Enabling or Disabling Strong Passwords

This command enables or disables the strong password feature.

```
config:#   security strongPasswords enabled <option>
```

Variables:

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

Option	Description
true	Enables the strong password feature.
false	Disables the strong password feature.

Minimum Password Length

This command determines the minimum length of the password.

```
config:#   security strongPasswords minimumLength <value>
```

Variables:

- <value> is an integer between 8 and 32.

Maximum Password Length

This command determines the maximum length of the password.

```
config:#   security strongPasswords maximumLength <value>
```

Variables:

- <value> is an integer between 16 and 64.

Lowercase Character Requirement

This command determines whether a strong password includes at least a lowercase character.

```
config:#   security strongPasswords enforceAtLeastOneLowerCaseCharacter <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	At least one lowercase character is required.
disable	No lowercase character is required.

Uppercase Character Requirement

This command determines whether a strong password includes at least a uppercase character.

```
config:#   security strongPasswords enforceAtLeastOneUpperCaseCharacter <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	At least one uppercase character is required.
disable	No uppercase character is required.

Numeric Character Requirement

This command determines whether a strong password includes at least a numeric character.

```
config:#   security strongPasswords enforceAtLeastOneNumericCharacter <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	At least one numeric character is required.

Option	Description
disable	No numeric character is required.

Special Character Requirement

This command determines whether a strong password includes at least a special character.

```
config:#   security strongPasswords enforceAtLeastOneSpecialCharacter <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	At least one special character is required.
disable	No special character is required.

Maximum Password History

This command determines the number of previous passwords that CANNOT be repeated when changing the password.

```
config:#   security strongPasswords passwordHistoryDepth <value>
```

Variables:

- <value> is an integer between 1 and 12.

Role-Based Access Control

In addition to firewall access control based on IP addresses, you can configure other access control rules that are based on both IP addresses and users' roles.

- An IPv4 role-based access control command begins with *security roleBasedAccessControl ipv4*.
- An IPv6 role-based access control command begins with *security roleBasedAccessControl ipv6*.

Modifying Role-Based Access Control Parameters

There are different commands for modifying role-based access control parameters.

- *IPv4 commands*

▶ **Enable or disable the IPv4 role-based access control feature:**

```
config:#   security roleBasedAccessControl ipv4 enabled <option>
```

▶ **Determine the IPv4 role-based access control policy:**

```
config:#   security roleBasedAccessControl ipv4 defaultPolicy <policy>
```

- *IPv6 commands*

▶ **Enable or disable the IPv6 role-based access control feature:**

```
config:#   security roleBasedAccessControl ipv6 enabled <option>
```

▶ **Determine the IPv6 role-based access control policy:**

```
config:#   security roleBasedAccessControl ipv6 defaultPolicy <policy>
```

Variables:

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

Option	Description
true	Enables the role-based access control feature.
false	Disables the role-based access control feature.

- <policy> is one of the options: *allow* or *deny*.

Policy	Description
allow	Accepts traffic from all IP addresses regardless of the user's role.
deny	Drops traffic from all IP addresses regardless of the user's role.

Tip: You can combine both commands to modify all role-based access control parameters at a time. See Multi-Command Syntax *(on page 334).*

Managing Role-Based Access Control Rules

You can add, delete or modify role-based access control rules.

- An IPv4 role-based access control command for managing rules begins with *security roleBasedAccessControl ipv4 rule*.
- An IPv6 role-based access control command for managing rules begins with *security roleBasedAccessControl ipv6 rule*.

Adding a Role-Based Access Control Rule

Depending on where you want to add a new rule in the list, the command syntax for adding a rule varies.

- *IPv4 commands*

▶ Add a new rule to the bottom of the IPv4 rules list:

```
config:#   security roleBasedAccessControl ipv4 rule add <start_ip> <end_ip> <role>
           <policy>
```

▶ Add a new IPv4 rule by inserting it above or below a specific rule:

```
config:#   security roleBasedAccessControl ipv4 rule add <start_ip> <end_ip> <role>
           <policy> <insert> <rule_number>
```

- *IPv6 commands*

▶ Add a new rule to the bottom of the IPv6 rules list:

```
config:#   security roleBasedAccessControl ipv6 rule add <start_ip> <end_ip> <role>
           <policy>
```

▶ Add a new IPv6 rule by inserting it above or below a specific rule:

```
config:#   security roleBasedAccessControl ipv6 rule add <start_ip> <end_ip> <role>
           <policy> <insert> <rule_number>
```

Variables:

- <start_ip> is the starting IP address.
- <end_ip> is the ending IP address.
- <role> is the role for which you want to create an access control rule.
- <policy> is one of the options: *allow* or *deny*.

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

- <insert> is one of the options: *insertAbove* or *insertBelow*.

Option	Description
insertAbove	Inserts the new rule above the specified rule number. Then: *new rule's number = the specified rule number*
insertBelow	Inserts the new rule below the specified rule number. Then: *new rule's number = the specified rule number + 1*

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

Modifying a Role-Based Access Control Rule

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

- *IPv4 commands*

▶ **Modify a rule's IPv4 address range:**

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

▶ **Modify an IPv4 rule's role:**

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

▶ **Modify an IPv4 rule's policy:**

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

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

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

- *IPv6 commands*

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

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

▶ **Modify an IPv6 rule's role:**

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

▶ **Modify an IPv6 rule's policy:**

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

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

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

Variables:

- <rule_number> is the number of the existing rule that you want to modify.
- <start_ip> is the starting IP address.
- <end_ip> is the ending IP address.
- <role> is one of the existing roles.
- <policy> is one of the options: *allow* or *deny*.

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

Deleting a Role-Based Access Control Rule

These commands remove a specific rule from the list.

▶ IPv4 commands

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

▶ IPv6 commands

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

Variables:

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

Examples

This section illustrates several security configuration examples.

Example 1 - IPv4 Firewall Control Configuration

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

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

Results:

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

Example 2 - Adding an IPv4 Firewall Rule

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

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

Results:

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

Example 3 - User Blocking

The following command sets up two user blocking parameters.

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

Results:

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

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

The following command creates a newIPv4 role-based access control rule and specifies its location in the list.

```
config:#   security roleBasedAccessControl ipv4 rule add 192.168.78.50 192.168.90.100
           admin deny insertAbove 3
```

Results:

- A new IPv4 role-based access control rule is added, dropping all packets from any IPv4 address between 192.168.78.50 and 192.168.90.100 when the user is a member of the role "admin."
- The newly-added IPv4 rule is inserted above the 3rd rule. That is, the new rule becomes the 3rd rule, and the original 3rd rule becomes the 4th rule.

Outlet Configuration Commands

An outlet configuration command begins with *outlet*. Such a command allows you to configure an individual outlet.

Changing the Outlet Name

This command names an outlet.

```
config:#   outlet <n> name "<name>"
```

Variables:

- <n> is the number of the outlet that you want to configure.
- <name> is a string comprising up to 32 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.

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 334).*

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 246).
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 334).

▶ **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 334).

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 309).

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 334).

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 246).
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 246).
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 334).

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 309).
- <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

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

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

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

Note: The ID number of each actuator is shown in the 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 309).
- <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 309).
- <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 327)*.

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 327)**.*

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.

Type	Description
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 334).

- **Set the Default Upper Critical Threshold for a specific sensor type:**

```
config:#   defaultThresholds <sensor type> upperCritical <value>
```

- **Set the Default Upper Warning Threshold for a specific sensor type:**

```
config:#   defaultThresholds <sensor type> upperWarning <value>
```

- **Set the Default Lower Critical Threshold for a specific sensor type:**

```
config:#   defaultThresholds <sensor type> lowerCritical <value>
```

- **Set the Default Lower Warning Threshold for a specific sensor type:**

```
config:#   defaultThresholds <sensor type> lowerWarning <value>
```

▶ **Set the Default Deassertion Hysteresis for a specific sensor type:**

```
config:#   defaultThresholds <sensor type> hysteresis <hy_value>
```

▶ **Set the Default Assertion Timeout for a specific sensor type:**

```
config:#   defaultThresholds <sensor type> assertionTimeout <as_value>
```

Variables:

- <sensor type> is one of the following numeric sensor types:

Sensor types	Description
absoluteHumidity	Absolute humidity sensors
relativeHumidity	Relative humidity sensors
temperature	Temperature sensors
airPressure	Air pressure sensors
airFlow	Air flow sensors
vibration	Vibration sensors

- <value> is the value for the specified threshold of the specified sensor type. Note that diverse sensor types use different measurement units.

Sensor types	Measurement units
absoluteHumidity	g/m^3 (that is, g/m^3)
relativeHumidity	%
temperature	Degrees Celsius (°C) or Fahrenheit (°F), depending on your measurement unit settings.
airPressure	Pascal (Pa) or psi, depending on your measurement unit settings.
airFlow	m/s

Sensor types	Measurement units
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 334).

▶ **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

Sensor type	Description
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 451).
- <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 449).

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 334).

▶ **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 451).
- <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 449).

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 334).

▶ **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 451).
- <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 449).

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 334).

▶ **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 334).

▶ **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 218).

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
```

Unblocking 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 216).
2. When the Username prompt appears, type `unblock` and press Enter.

```
Username: unblock
```

3. When the "Username to unblock" prompt appears, type the name of the blocked user and press Enter.

```
Username to unblock:
```

4. A message appears, indicating that the specified user was unblocked successfully.

Resetting the 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 389) 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 218).

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.

Chapter 9 Using 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 344
Bulk Configuration via SCP 345
Backup and Restore via SCP 346
Downloading Diagnostic Data via SCP 347

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 ***Updating the PXE Firmware*** (on page 197).

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

To update the firmware via SCP:

1. Type the following SCP command and press Enter.
   `scp <firmware file> <user name>@<device ip>:/fwupdate`
   - *<firmware file>* is the 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 example:

```
scp  pdu-px2-030000-41270.bin
admin@192.168.87.50:/fwupdate
```

Windows PSCP command:

PSCP in Windows works in a similar way to the SCP.

- `pscp <firmware file> <user name>@<device ip>:/fwupdate`

Bulk Configuration via SCP

Like performing bulk configuration via the web interface, there are two steps with the bulk configuration using the SCP commands:

a. Save a configuration from a source 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 199).

To save the configuration via SCP:

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 whose configuration you want to save.
2. Type the user password when prompted.
3. The system saves the configuration from the PXE to a file named "bulk_config.xml."

To copy the configuration via SCP:

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 whose configuration you want to copy.
2. Type the user password when prompted.

3. The system copies the configuration included in the file "bulk_config.xml" to another PXE, and displays the following message.

```
Starting restore operation. The connection will be
closed now.
```

SCP examples:

- Save operation:

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

- Copy operation:

```
scp  bulk_config.xml
admin@192.168.87.47:/bulk_restore
```

Windows PSCP commands:

PSCP in Windows works in a similar way to the SCP.

- Save operation:

```
pscp <user name>@<device ip>:/bulk_config.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 via SCP:

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 whose settings you want to back up.
2. Type the user password when prompted.
3. The system saves the settings from the PXE to a file named "backup_settings.xml."

To restore the settings via SCP:

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 whose settings you want to restore.

2. Type the user password when prompted.
3. The system copies the configuration included in the file "backup_settings.xml" to the PXE, and displays the following message.

```
Starting restore operation. The connection will be
closed now.
```

SCP examples:

- Backup operation:

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

- Restoration operation:

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

Windows PSCP commands:

PSCP in Windows works in a similar way to the SCP.

- Backup operation:

```
pscp <user name>@<device ip>:/backup_settings.xml
```

- Restoration operation:

```
pscp backup_settings.xml <user name>@<device
ip>:/settings_restore
```

Downloading Diagnostic Data via SCP

You can download the diagnostic data via SCP.

To download the diagnostic data via SCP:

1. Type the following SCP command and press Enter.

```
scp <user name>@<device ip>:/diag-data.tgz
```

- *<user name>* is the "admin" or any user profile with the Administrator or "Unrestricted View Privileges" privileges.
- *<device ip>* is the IP address of the PXE whose diagnostic data you want to download.

2. Type the password when the system prompts you to type it.

3. The system saves the diagnostic data from the PXE to a file named "diag-data.tgz."

SCP example:

```
scp  admin@192.168.87.50:/diag-data.tgz
```

Windows PSCP command:

PSCP in Windows works in a similar way to the SCP.

- `pscp <user name>@<device ip>:/diag-data.tgz`

Appendix A Specifications

In This Chapter

Maximum Ambient Operating Temperature 349
Sensor RJ-12 Port Pinouts 349
RS-485 Port Pinouts 349

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

RS-485 Pin/signal definition			
1	—	—	—
2	—	—	—
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

OUTLET 7	OUTLET 8	OUTLET 9
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE
OUTLET 10	OUTLET 11	OUTLET 12
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE
OUTLET 13	OUTLET 14	OUTLET 15
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE

OUTLET 16	OUTLET 17	OUTLET 18
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE
OUTLET 19	OUTLET 20	OUTLET 21
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE

OUTLET 22	OUTLET 23	OUTLET 24
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE

Types of adapters

_____

Types of cables

_____

Name of software program

_____

Appendix C 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..... 355
Configuration Files..... 356
TFTP Requirements 367
DHCP IPv4 Configuration in Windows 368
DHCP IPv6 Configuration in Windows 378
DHCP IPv4 Configuration in Linux 385
DHCP IPv6 Configuration in Linux 387

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 356) 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 367).
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 368)
   - ***DHCP IPv6 Configuration in Windows*** (on page 378)
   - ***DHCP IPv4 Configuration in Linux*** (on page 385)
   - ***DHCP IPv6 Configuration in Linux*** (on page 387)
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 358).
- **config.txt:**

  This file is used for configuring device settings. See ***config.txt*** (on page 362).

- devices.csv:

  This file is required only when there are device-specific settings to configure for multiple PXE devices. See *devices.csv* (on page 364).

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 365).

fwupdate.cfg

The configuration file, *fwupdate.cfg*, is an ASCII text file containing key-value pairs, one per line.

Each value in the file must be separated by an equal sign (=), without any surrounding spaces. Keys are not case sensitive.

Illustration:

```
user=admin
password=raritan
logfile=log.txt
config=config.txt
device_list=devices.csv
```

This section only explains common options in the file.

Note: To 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 362).

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 364).

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 **Bulk Configuration** *(on page 199) 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 Device Settings** *(on page 202) 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.

execute_lua_script

- Supported as of release 3.3.0.
- Specify a LUA binding script file. For example:
  `execute_lua_script=my_script.lua`
- Script output will be recorded to a log file -- <BASENAME_OF_SCRIPT>.<SERIAL_NUMBER>.log. Note this log file's size is limited on dhcp/tftp.
- A dhcp/tftp-located script has a timeout of 60 seconds. After that duration the script will be removed.
- If you unplug the USB drive while the LUA script is still running, the script will be removed.
- An exit handler can be used but the execution time is limited to three seconds. Note that this is not implemented on dhcp/tftp yet.
- This feature can be used to manage LuaService, such as upload, start, get output, and so on.

config.txt

To perform device configuration, you must:

- Copy the device configuration file "config.txt" to the root directory of the TFTP server.
- Reference the "config.txt" file in the *config* option of the "fwupdate.cfg" file. See ***fwupdate.cfg*** (on page 358).

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.

Tip: As of release 3.2.20, you can choose to encrypt important data in the "config.txt" file so that people cannot easily recognize it, such as the SNMP write community string. See **Data Encryption in 'config.txt'** *(on page 366).*

Regular configuration key syntax:

- Each configuration key and value pair is in a single line as shown below:

  ```
  key=value
  ```

  Note: Each value in the file must be separated by an equal sign (=), without any surrounding spaces.

- 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 364)
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}
   ```

To rename the admin user:

As of release 3.1.0, you can rename the admin user by adding the following configuration key:

```
users[0].name=new admin name
```

Example:

```
users[0].name=May
```

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.
- Referenced in the *device_list* option of the "fwupdate.cfg" file. See ***fwupdate.cfg*** (on page 358).

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",Valu
  e-3

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

Creating Configuration Files via Mass Deployment Utility

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

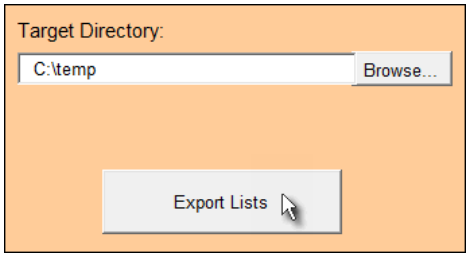
After entering required information, you can generate all configuration files with only one click, including *fwupdate.cfg*, *config.txt* and *devices.csv*.

To use the Mass Deployment Utility:

1. Download the Mass Deployment Utility from the Raritan website.
   - The utility is named *mass_deployment-xxx* (where xxx is the firmware version number).
   - It is available on the PXE section of the ***Support page*** (***http://www.raritan.com/support/***).
2. Launch Excel to open this utility.

   Note: Other office suites, such as OpenOffice and LibreOffice, are not supported.

3. Read the instructions in the 1st worksheet of the utility, and make sure Microsoft Excel's security level has been set to Medium or the equivalent for executing unsigned macros of this utility.
4. Enter information in the 2nd and 3rd worksheets.
   - The 2nd worksheet contains information required for *fwupdate.cfg* and *config.txt*.
   - The 3rd worksheet contains device-specific information for *devices.csv*.
5. Return to the 2nd worksheet to execute the export macro.
   a. In the Target Directory field, specify the folder where to generate the configuration files. For example, you can specify the root directory of a connected USB drive.
   b. Click Export Lists to generate configuration files.



6. Verify that at least 3 configuration files are created - *fwupdate.cfg*, *config.txt* and *devices.csv*. You are ready to configure or upgrade any PXE with these files.

Data Encryption in 'config.txt'

Encryption for any settings in the file "config.txt" is supported as of release 3.2.20.

When intending to prevent people from identifying the values of any settings, you can encrypt them. Encrypted data still can be properly interpreted and performed by any PXE running firmware version 3.2.20 or later.

Data encryption procedure:

1. Open the "config.txt" file to determine which setting(s) to encrypt.
   - If an appropriate "config.txt" is not created yet, see *Creating Configuration Files via Mass Deployment Utility* (on page 365).
2. Launch a terminal to log in to the CLI of any PXE running version 3.2.20 or later. See *Logging in to CLI* (on page 216).
3. Type the encryption command and the value of the setting you want to encrypt.
   - The value *cannot* contain any double quotes (") or backslashes (-).
   - If the value contains spaces, it must be enclosed in double quotes.

```
# config encrypt <value>
```

-- OR --

```
# config encrypt "<value with spaces>"
```

4. Press Enter. The CLI generates and displays the encrypted form of the typed value.
5. Go to the "config.txt" file and replace the chosen value with the encrypted one by typing or copying the encrypted value from the CLI.
6. Add the text "encrypted:" to the beginning of the encrypted setting.
7. Repeat steps 3 to 6 for additional settings you intend to encrypt.
8. Save the changes made to the "config.txt" file. Now you can use this file to configure any PXE running version 3.2.20 or later. See *Bulk Configuration/Upgrade Procedure* (on page 355).

Illustration:

In this example, we will encrypt the word "private", which is the value of the SNMP write community in the "config.txt" file.

```
snmp.write_community=private
```

1. In the CLI, type the following command to encrypt "private."

```
# config encrypt private
```

2. The CLI generates and shows the encrypted form of "private."

```
ZTtnYcvQUw==
```

3. In the "config.txt" file, make the following changes to the SNMP write community setting.
   a. Replace the word "private" with the encrypted value that CLI shows.

```
snmp.write_community=ZTtnYcvQUw==
```

   b. Add "encrypted:" to the beginning of that setting.

```
encrypted:snmp.write_community=ZTtnYcvQUw==
```

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 355).

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.

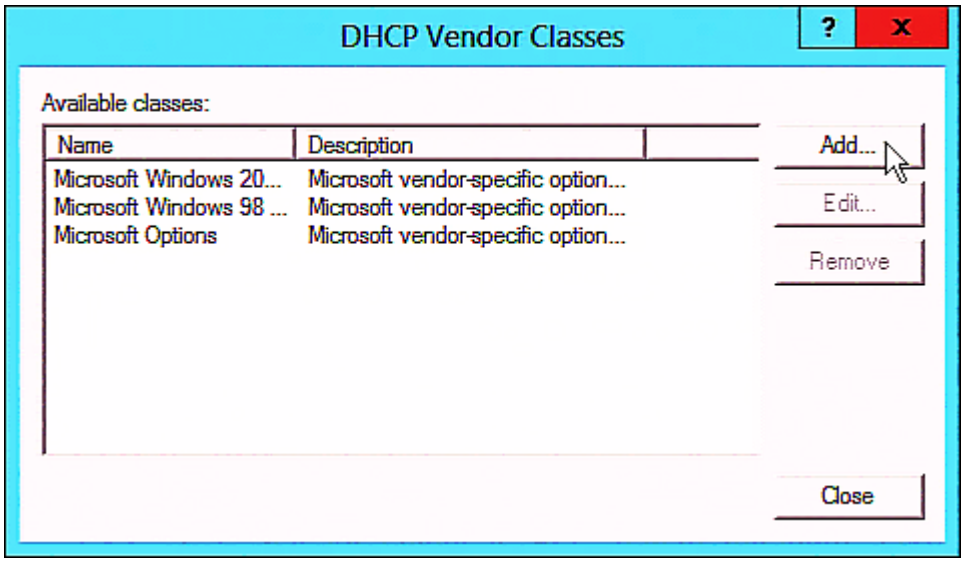
- **Required for uploading the diagnostic file only** - the timeout for file upload is set to one minute or larger.

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.

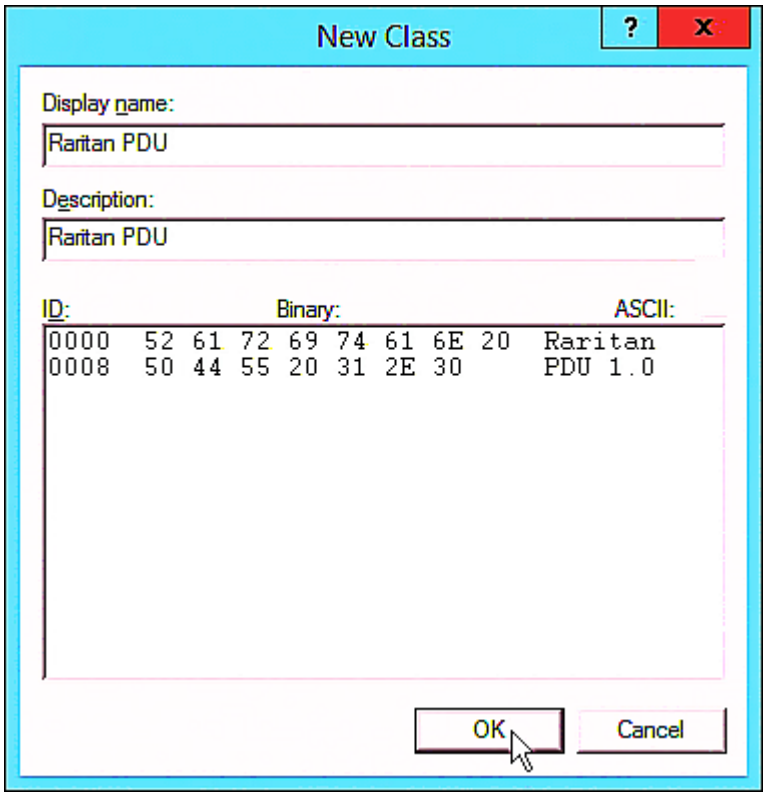
Required Windows IPv4 settings in DHCP:

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.



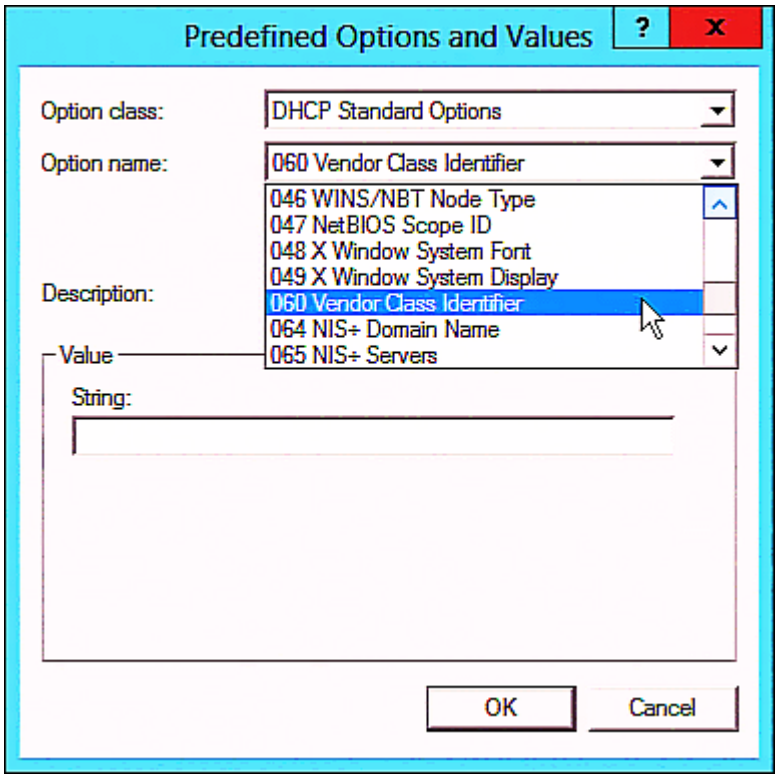
   c. Specify a unique name for this vendor class and type the binary codes of "Raritan PDU 1.0" in the New Class dialog.

The vendor class is named "Raritan PDU" in this illustration.



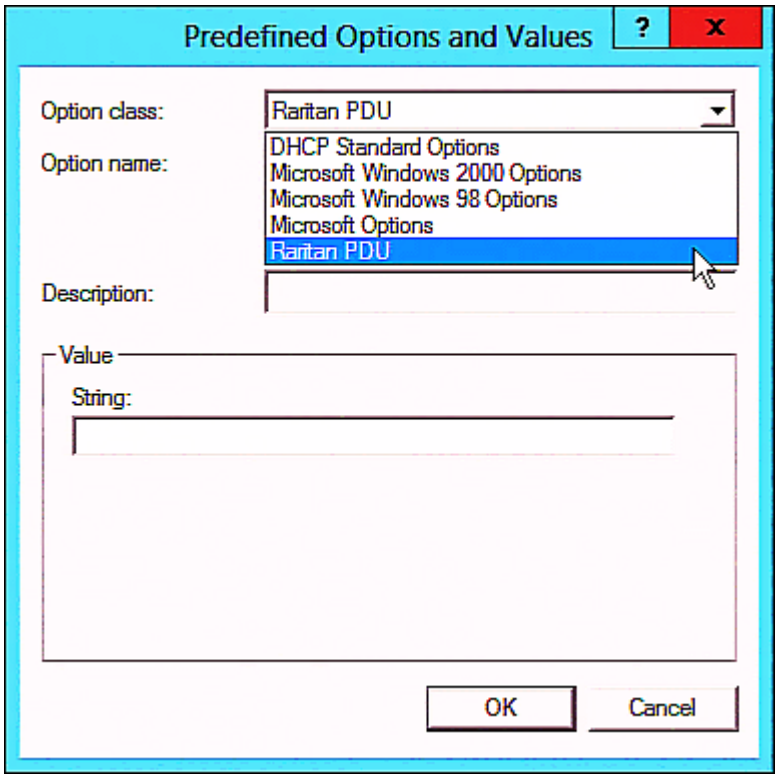
2. Define one DHCP standard option - Vendor Class Identifier.
   a. Right-click the IPv4 node in DHCP to select Set Predefined Options.

b. Select DHCP Standard Options in the "Option class" field, and Vendor Class Identifier in the "Option name" field. Leave the String field blank.

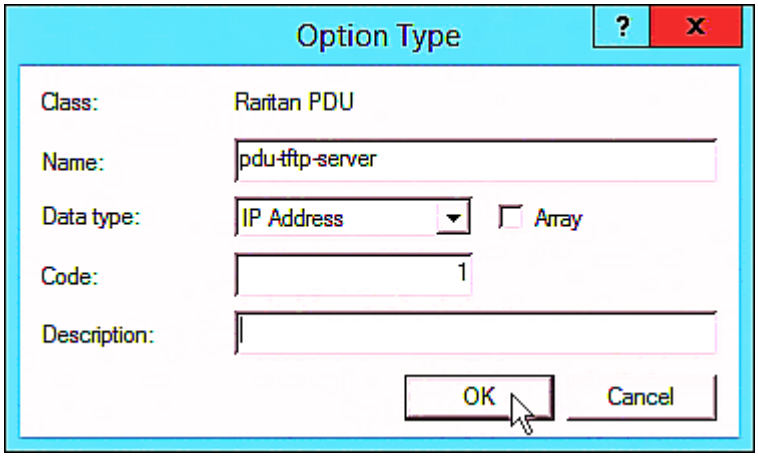


3. Add three options to the new vendor class "Raritan PDU" in the same dialog.

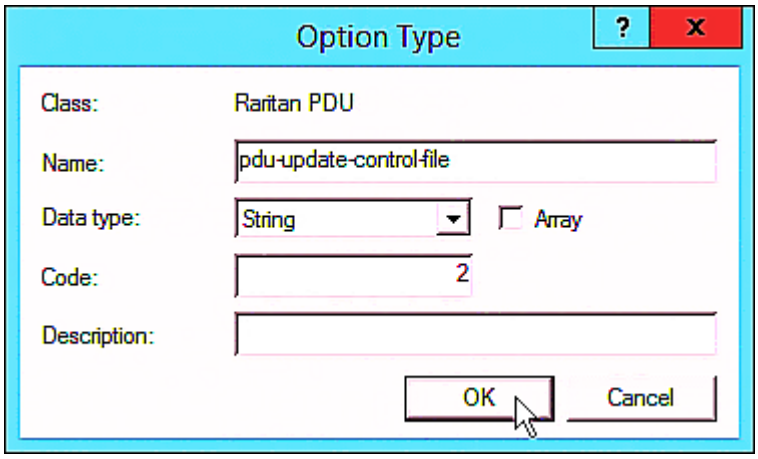
a. Select Raritan PDU in the "Option class" field.



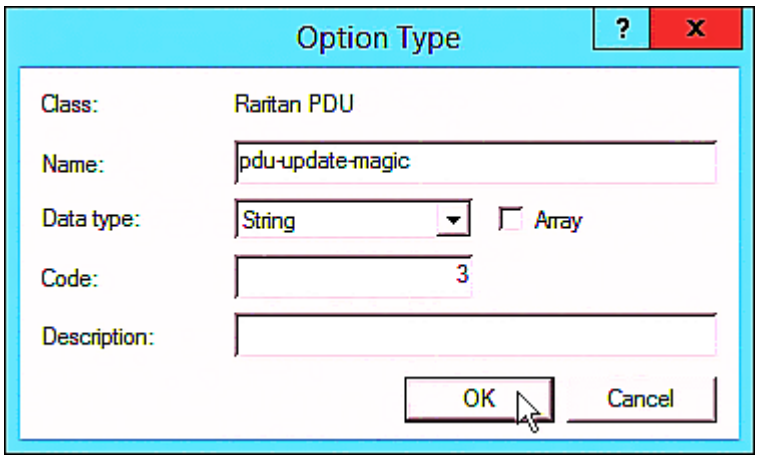
b. Click Add to add the first option. Type "pdu-tftp-server" in the Name field, select IP Address as the data type, and type 1 in the Code field.



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



d. Click Add to add the third one. Type "pdu-update-magic" in the Name field, select String as the data type, and type 3 in the Code field.

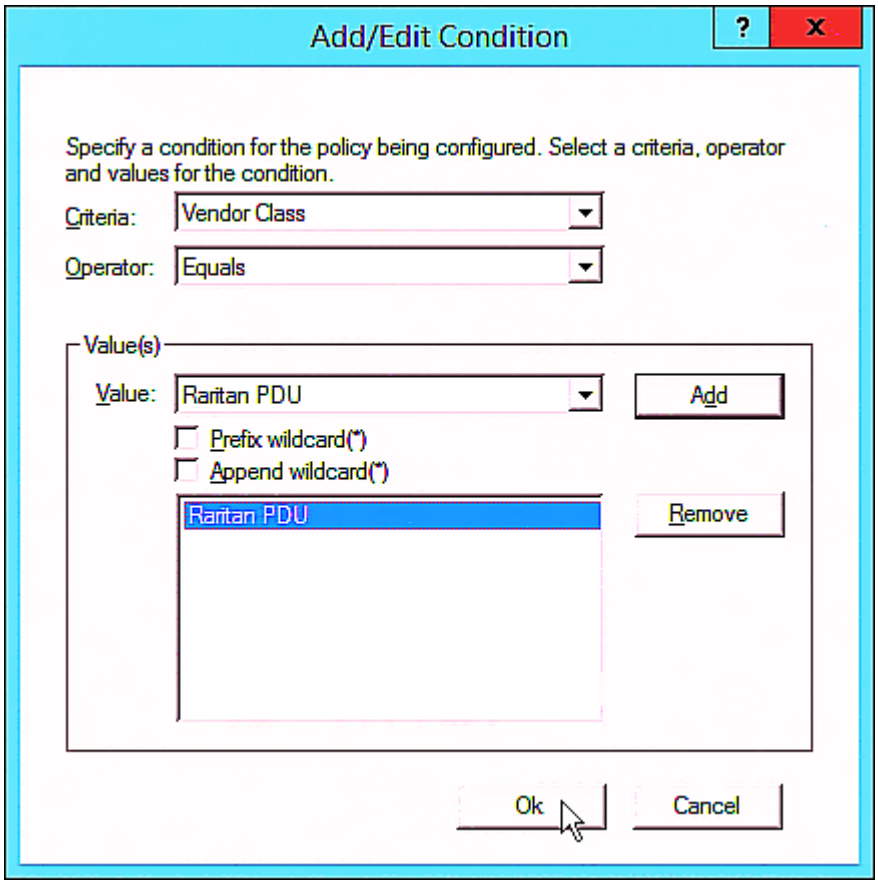


4. Create a new policy associated with the "Raritan PDU" vendor class.
   a. Right-click the Policies node under IPv4 to select New Policy.
   b. Specify a policy name, and click Next.

The policy is named "PDU" in this illustration.

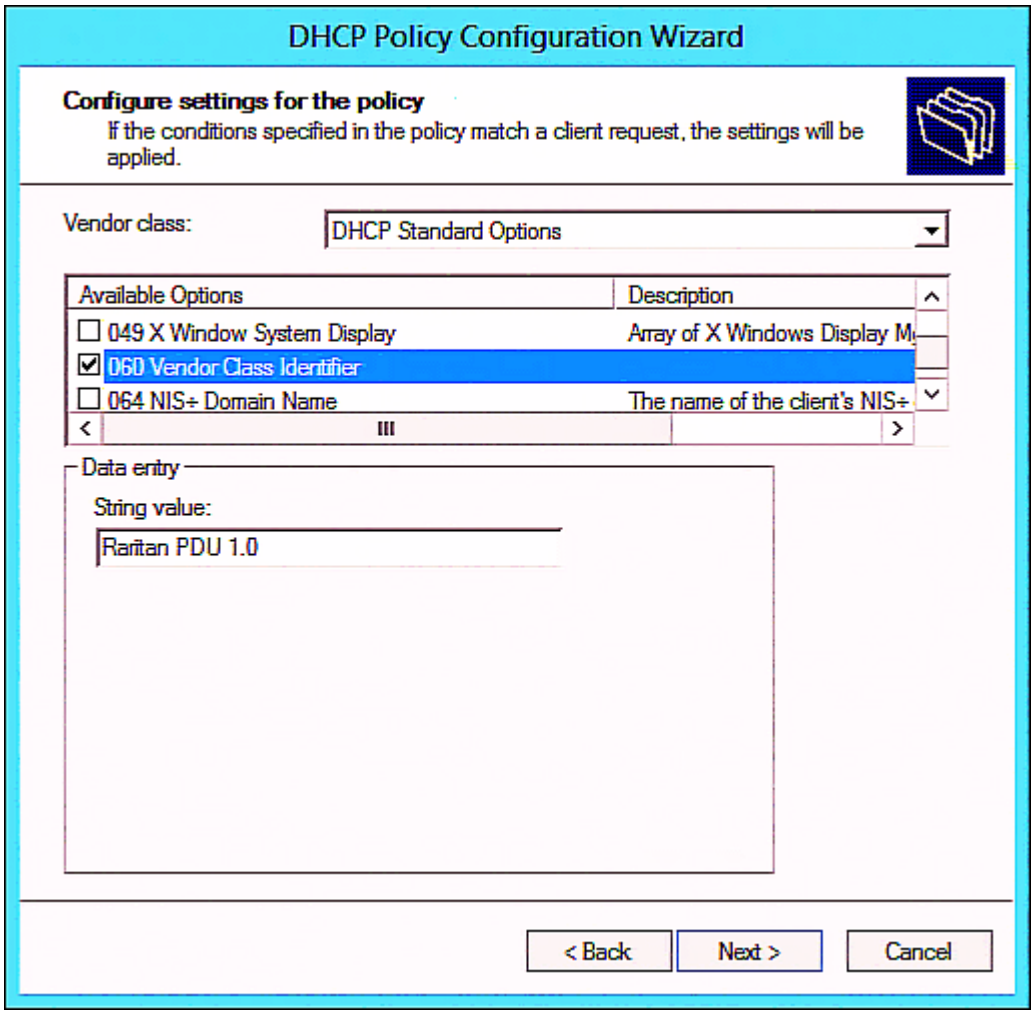
c. Click Add to add a new condition.

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

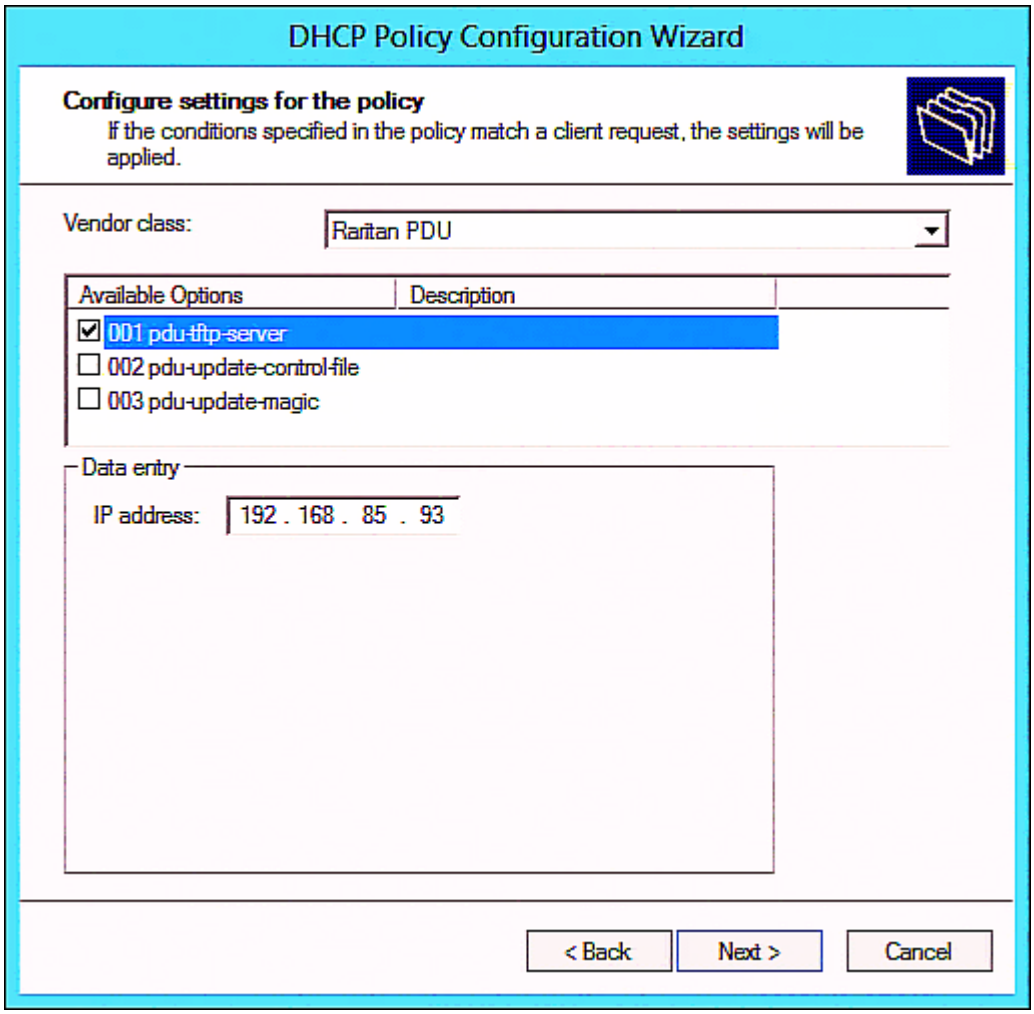


e. Click Next.

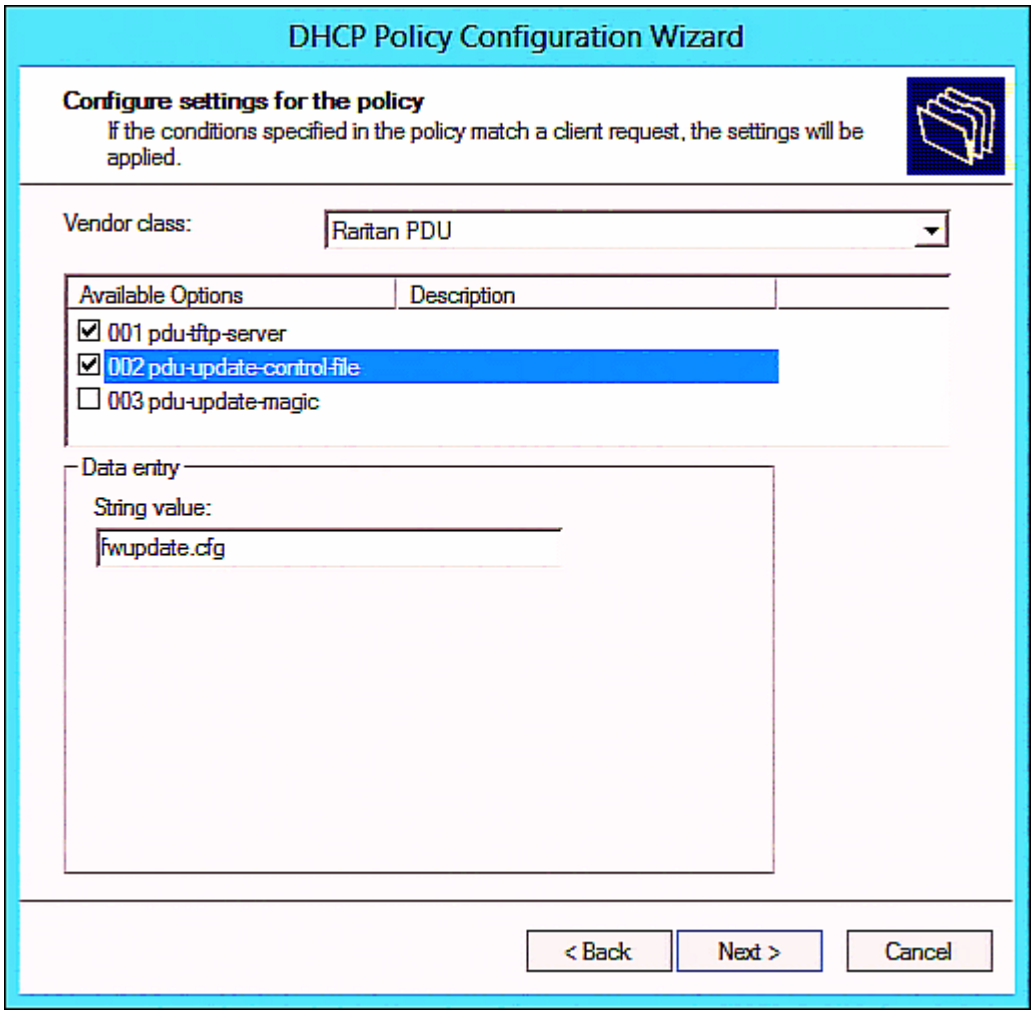
f. Select DHCP Standard Options in the "Vendor class" field, select "060 Vendor Class Identifier" from the Available Options list, and type "Raritan PDU 1.0" in the "String value" field.



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



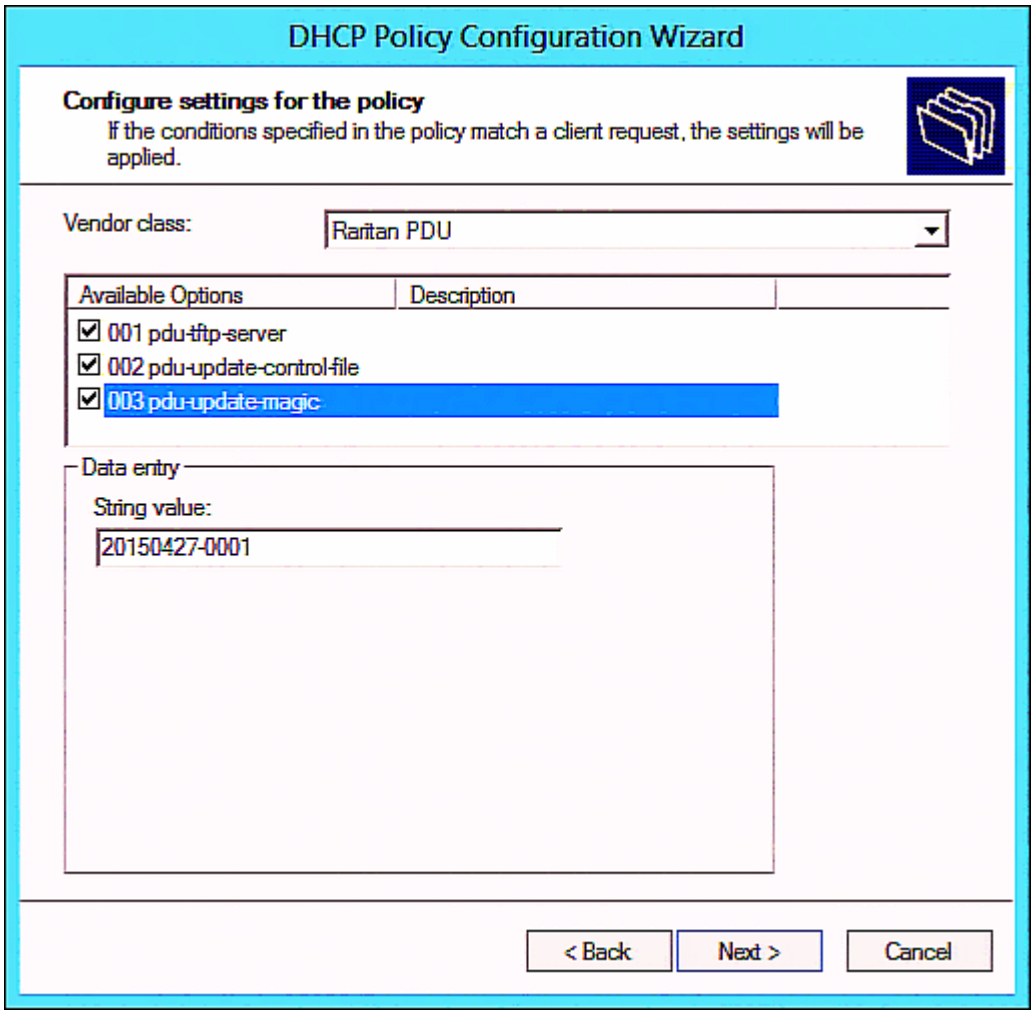
h. Select "002 pdu-update-control-file" from the Available Options list, and type the filename "fwupdate.cfg" in the "String value" field.



i. Select "003 pdu-update-magic" from the Available Options list, and type any string in the "String value" field. This third option/code is the magic cookie to prevent the *fwupdate.cfg* commands from being executed repeatedly. It does NOT matter whether the IPv4 magic cookie is identical to or different from the IPv6 magic cookie.

The magic cookie is a string comprising numerical and/or alphabetical digits in any format. In the following illustration diagram, it is a combination of a date and a serial number.

Important: The magic cookie is transmitted to and stored in 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 IPv6 Configuration in Windows

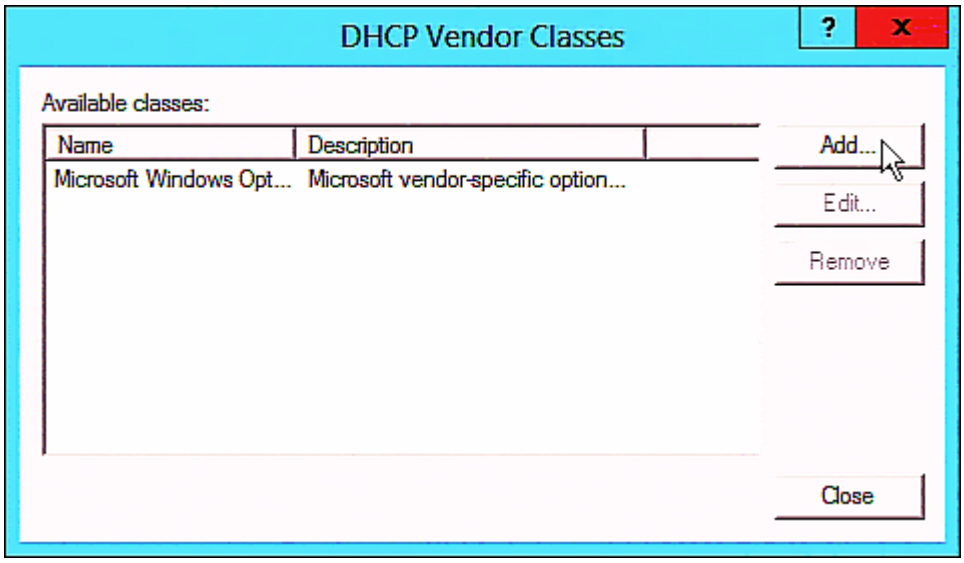
For those PXE devices using IPv6 addresses, follow this procedure to configure your DHCP server. The following illustration is based on Microsoft® Windows Server 2012 system.

Required Windows IPv6 settings in DHCP:

1. Add a new vendor class for Raritan PXE under IPv6.

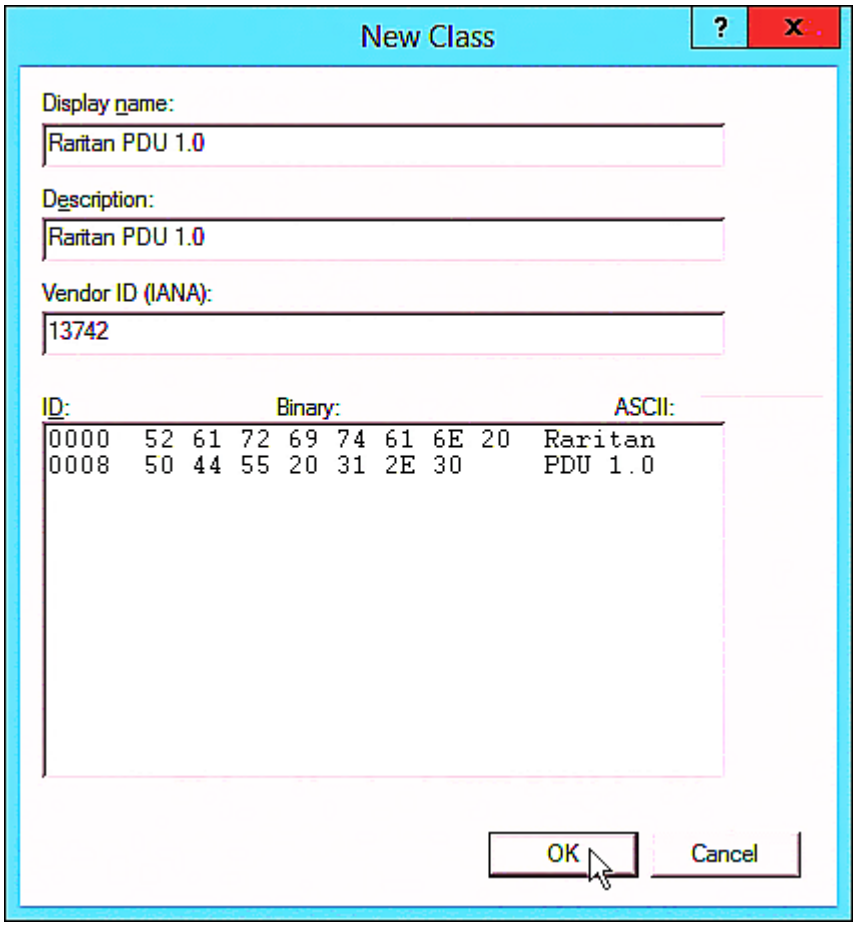
a. Right-click the IPv6 node in DHCP to select Define Vendor Classes.

b. Click Add to add a new vendor class.



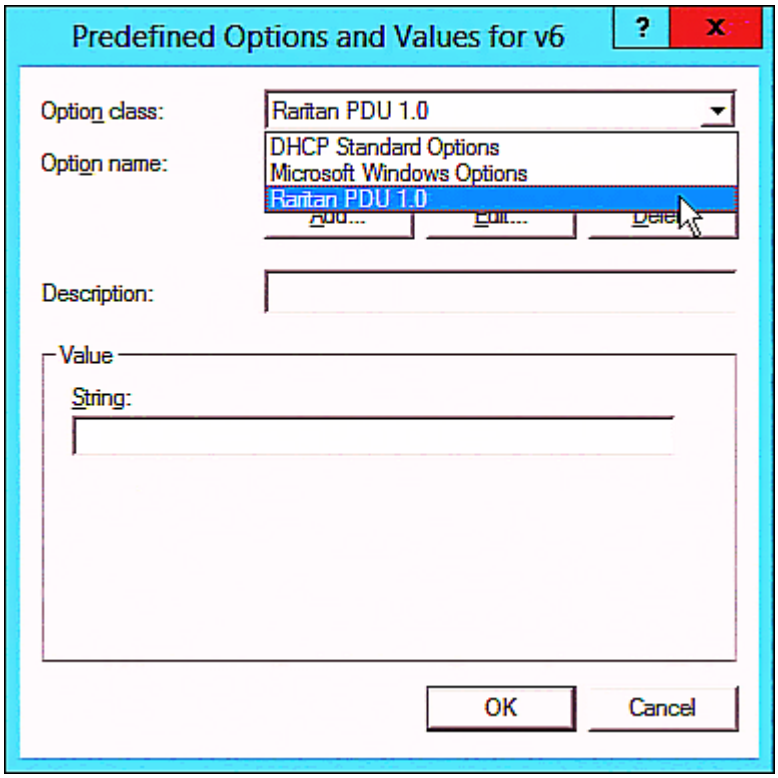
c. Specify a unique name for the vendor class, type "13742" in the "Vendor ID (IANA)" field, and type the binary codes of "Raritan PDU 1.0" in the New Class dialog.

The vendor class is named "Raritan PDU 1.0" in this illustration.

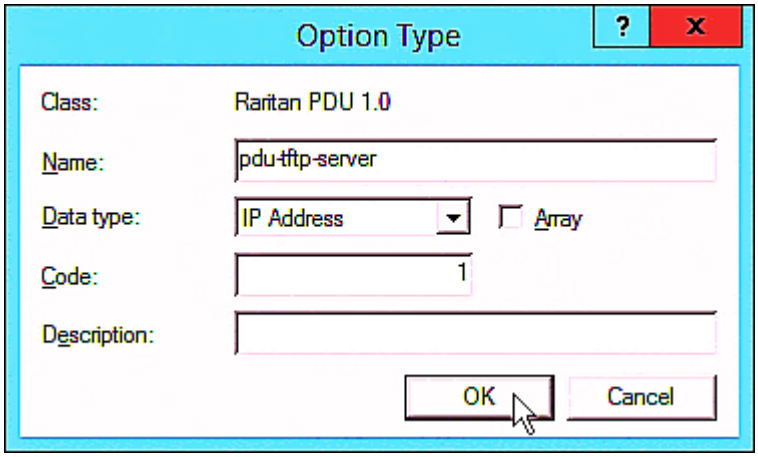


2. Add three options to the "Raritan PDU 1.0" vendor class.
   a. Right-click the IPv6 node in DHCP to select Set Predefined Options.

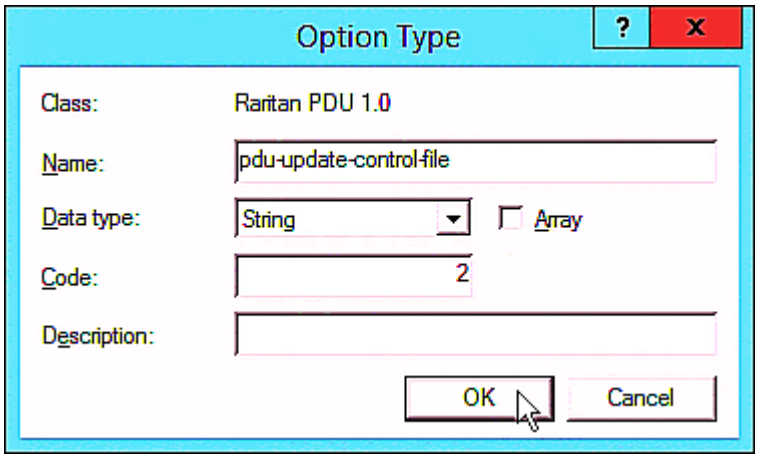
b. Select Raritan PDU 1.0 in the "Option class" field.



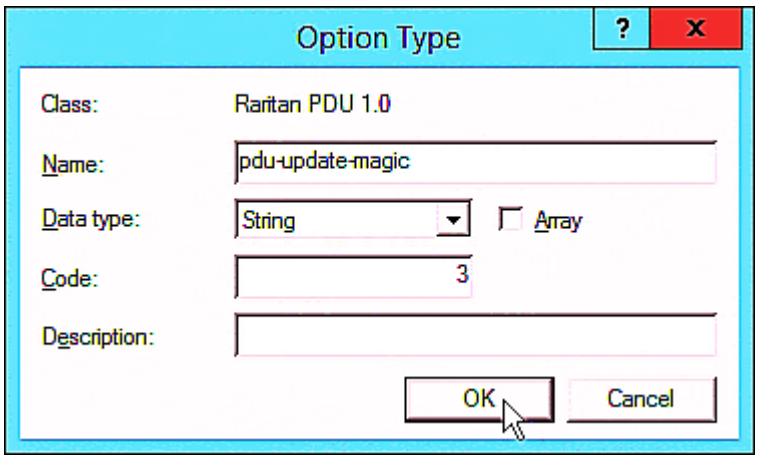
c. Click Add to add the first option. Type "pdu-tftp-server" in the Name field, select IP Address as the data type, and type 1 in the Code field.



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

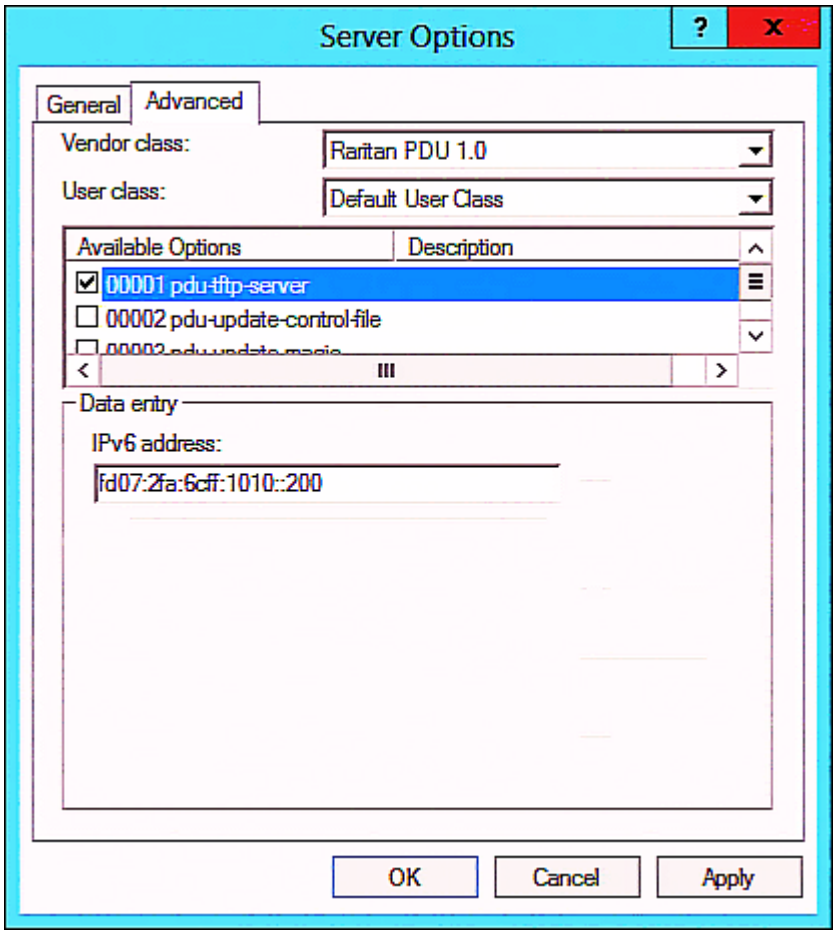


e. Click Add to add the third one. Type "pdu-update-magic" in the Name field, select String as the data type, and type 3 in the Code field.

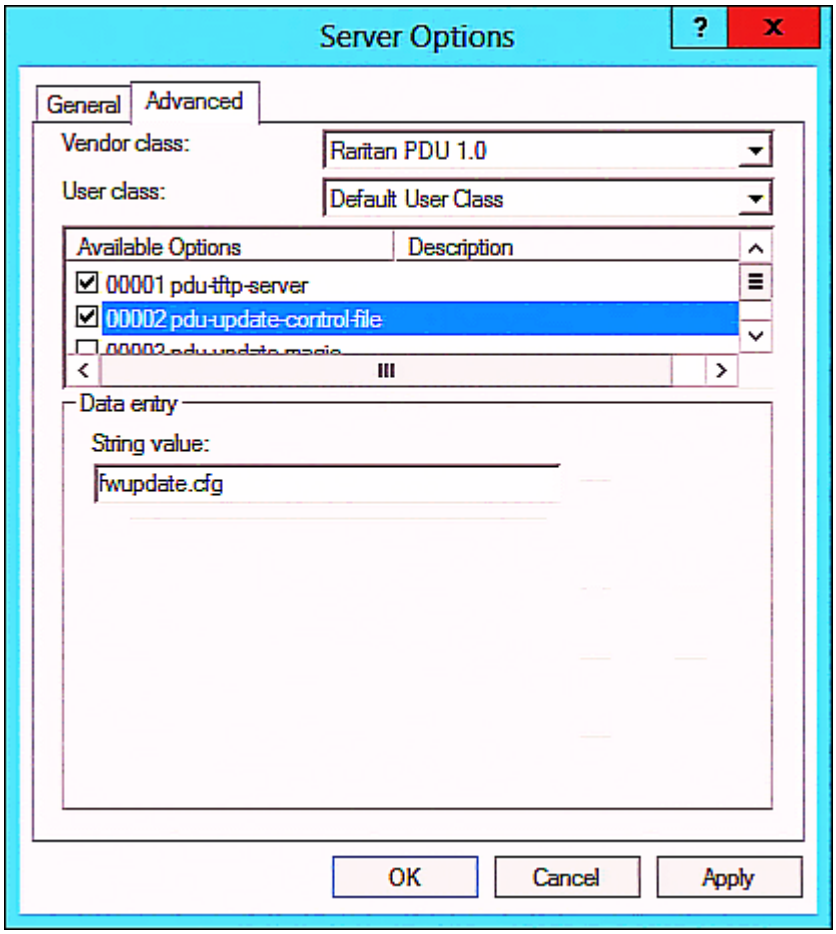


3. Configure server options associated with the "Raritan PDU 1.0" vendor class.
   a. Right-click the Server Options node under IPv6 to select Configure Options.
   b. Click the Advanced tab.

c. Select "Raritan PDU 1.0" in the "Vendor class" field, select "00001 pdu-tftp-server" from the Available Options list, and type your TFTP server's IPv6 address in the "IPv6 address" field.



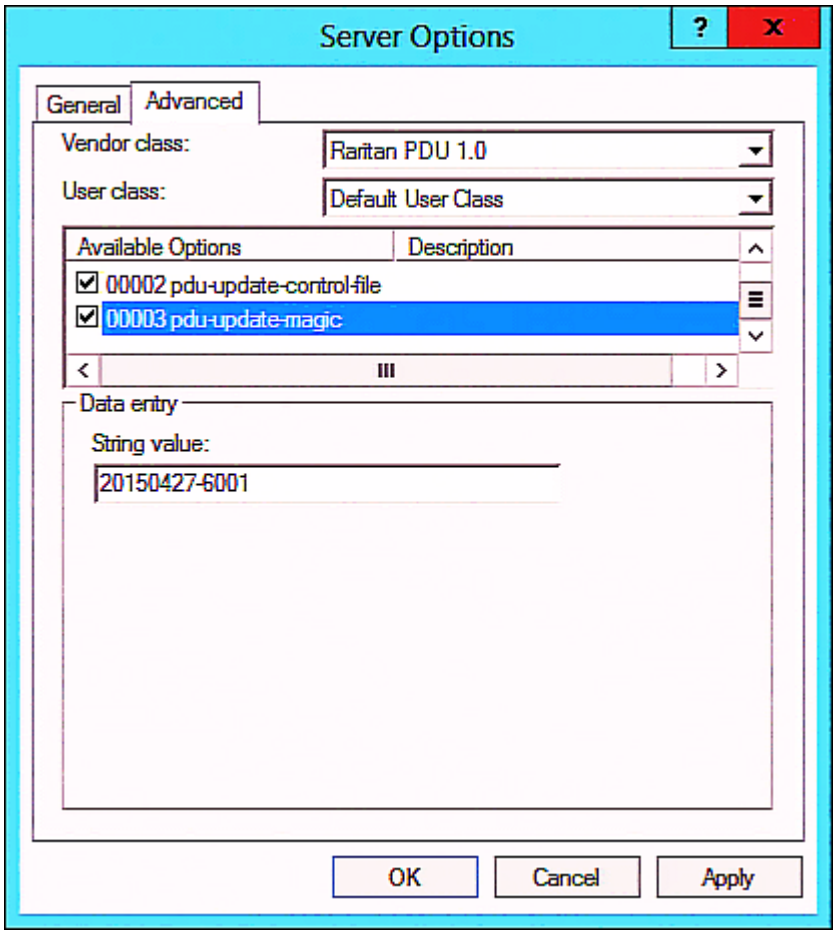
d. Select "00002 pdu-update-control-file" from the Available Options list, and type the filename "fwupdate.cfg" in the "String value" field.



e. Select "00003 pdu-update-magic" from the Available Options list, and type any string in the "String value" field. This third option/code is the magic cookie to prevent the *fwupdate.cfg* commands from being executed repeatedly. It does NOT matter whether the IPv6 magic cookie is identical to or different from the IPv4 magic cookie.

The magic cookie is a string comprising numerical and/or alphabetical digits in any format. In the following illustration diagram, it is a combination of a date and a serial number.

Important: The magic cookie is transmitted to and stored in 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 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 389

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 215).

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

1. Connect to the PXE device. See *Logging in to CLI* (on page 216) 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 15).
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 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 391
Step B. Configure User Groups on the AD Server 392
Step C. Configure LDAP Authentication on the PXE Device 393
Step D. Configure Roles on the PXE Device 394

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:

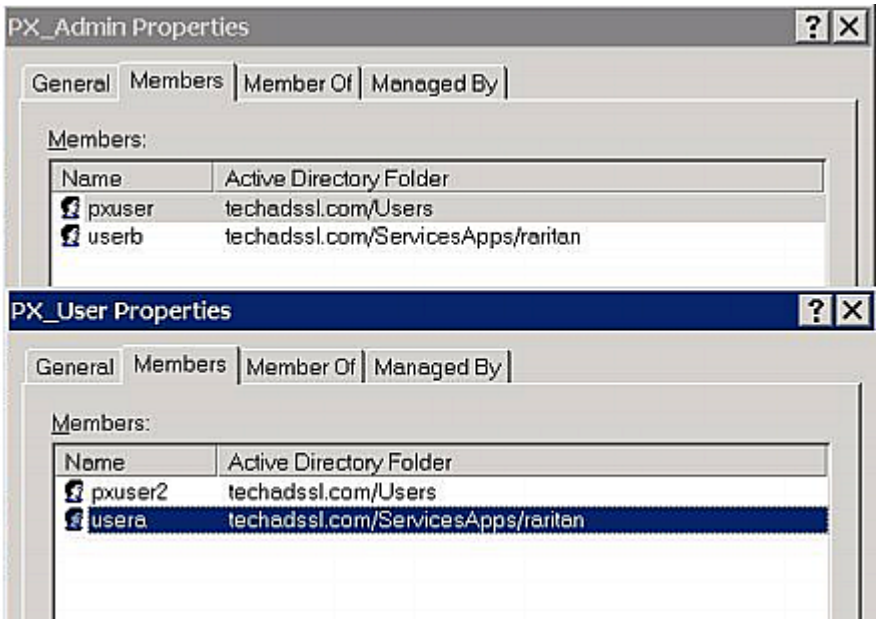
- The groups (roles) for the PXE are named *PX_Admin* and *PX_User*.
- User accounts *pxuser*, *pxuser2*, *usera* and *userb* already exist on the AD server.

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 ***Wired Network Settings*** (on page 106) and Role of a DNS Server.
- The AD server's domain name is *techadssl.com*, and its IP address is *192.168.56.3*.
- The AD protocol is NOT encrypted over TLS.
- The AD server uses the default TCP port *389*.
- Anonymous bind is used.

To configure LDAP authentication:

1. Choose Device Settings > Security > Authentication.
2. In the LDAP Servers section, click New to add an LDAP/LDAPS server.
3. Provide the PXE with the information about the AD server.

Field/setting	Do this...
IP Address / Hostname	Type the domain name `techadssl.com` or IP address `192.168.56.3`. *Important: Without the encryption enabled, you can type either the domain name or IP address in this field, but you must type the fully qualified domain name if the encryption is enabled.*
Copy settings from existing LDAP server	Leave the checkbox deselected unless the new LDAP server's settings are similar to any existing LDAP settings.
Type of LDAP Server	Select "Microsoft Active Directory."
Security	Select "None" since the TLS encryption is not applied in this example.
Port (None/StartTLS)	Ensure the field is set to 389.
Port (TLS), CA Certificate	Skip the two fields since the TLS encryption is not enabled.
Anonymous Bind	Select this checkbox because anonymous bind is used.
Bind DN, Bind Password, Confirm Bind Password	Skip the three fields because of anonymous bind.

Field/setting	Do this...
Base DN for Search	Type `dc=techadssl,dc=com` as the starting point where your search begins on the AD server.
Login Name Attribute	Ensure the field is set to `sAMAccountName` because the LDAP server is Microsoft Active Directory.
User Entry Object Class	Ensure the field is set to `user` because the LDAP server is Microsoft Active Directory.
User Search Subfilter	The field is optional. The subfilter information is also useful for filtering out additional objects in a large directory structure. In this example, we leave it blank.
Active Directory Domain	Type `techadssl.com`.

4. Click Add Server.The LDAP server is saved.
5. In the Authentication Type field, select LDAP.
6. Click Save. The LDAP authentication is activated.

Note: If the 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.

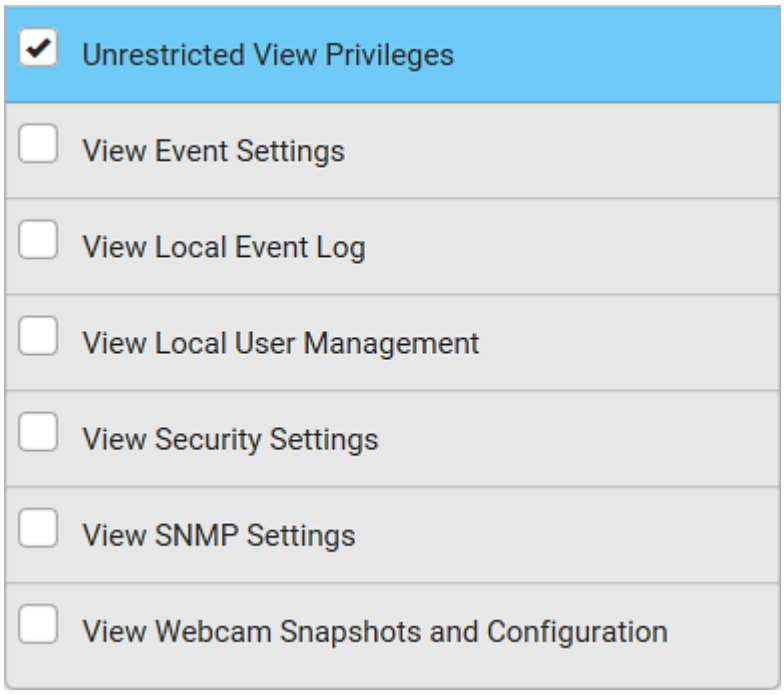
In this illustration, we assume:

- 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 Privileges so they can both configure PXE and access the outlets.

To create the PX_User role with appropriate permissions assigned:

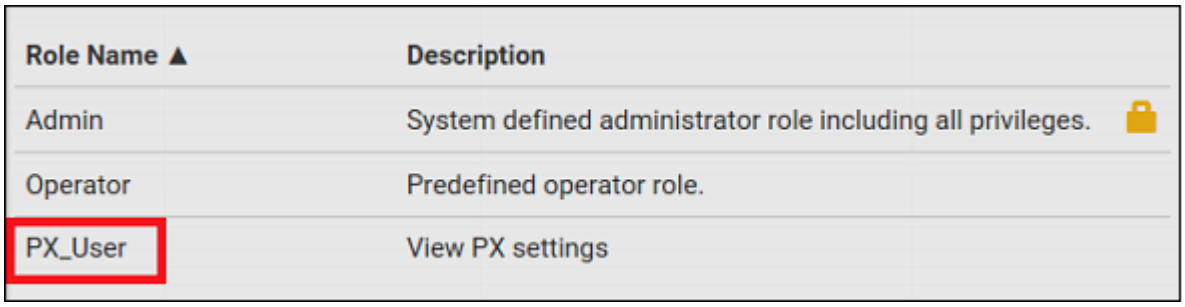
1. Choose User Management > Roles.
2. Click to add a new role.
   a. Type `PX_User` in the Role Name field.
   b. Type a description for the PX_User role in the Description field. In this example, we type "View PX settings" to describe the role.

c. In the Privileges list, select Unrestricted View Privileges, which includes all View permissions. The Unrestricted View Privileges permission lets users view all settings without the capability to configure or change them.



d. Click Save.

3. The PX_User role is created.



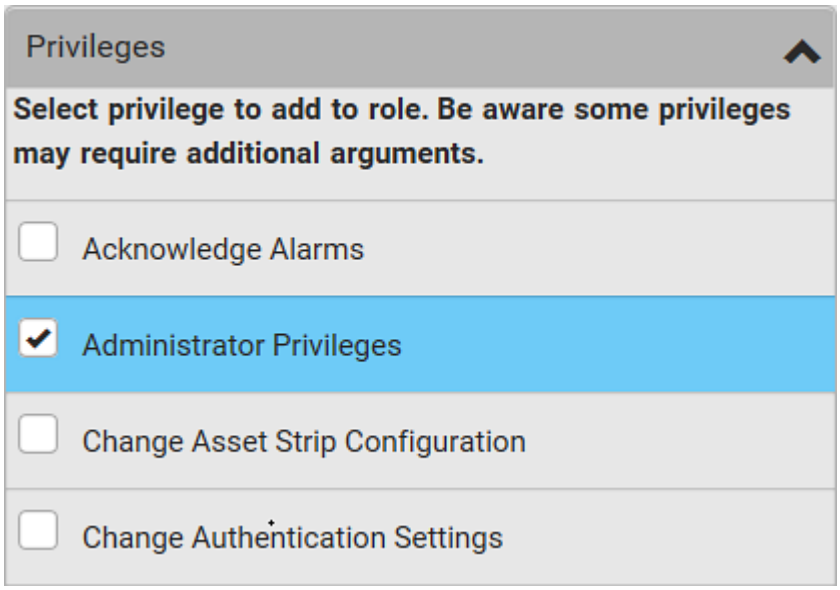
Role Name ▲	Description
Admin	System defined administrator role including all privileges.
Operator	Predefined operator role.
PX_User	View PX settings

4. Keep the Roles page open to create the PX_Admin role.

To create the PX_Admin role with full permissions assigned:

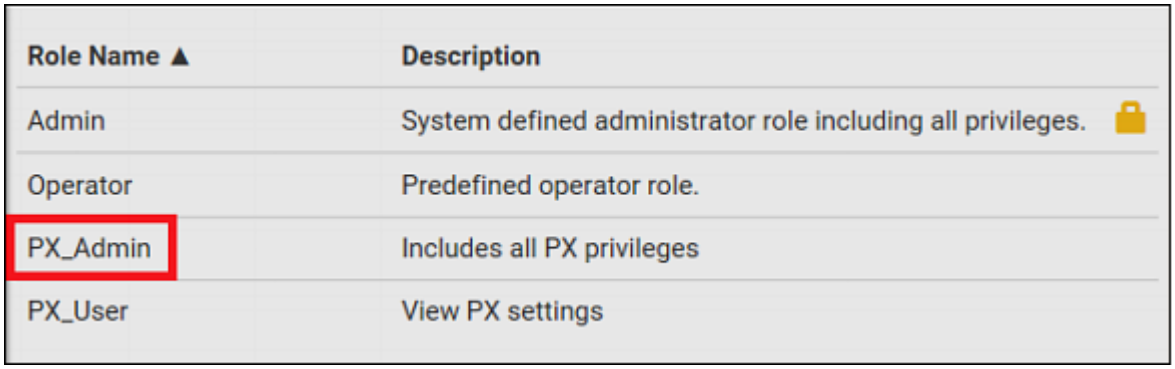
1. Click to add another role.
   a. Type `PX_Admin` in the Role Name field.
   b. Type a description for the PX_Admin role in the Description field. In this example, we type "Includes all PX privileges" to describe the role.

c. In the Privileges list, select Administrator Privileges. The Administrator Privileges allows users to configure or change all PXE settings.



d. Click Save.

2. The PX_Admin role is created.



Role Name ▲	Description
Admin	System defined administrator role including all privileges.
Operator	Predefined operator role.
PX_Admin	Includes all PX privileges
PX_User	View PX settings

Appendix F Updating the LDAP Schema

In This Chapter

Returning User Group Information 397
Setting the Registry to Permit Write Operations to the Schema 398
Creating a New Attribute 398
Adding Attributes to the Class 399
Updating the Schema Cache 401
Editing rciusergroup Attributes for User Members 401

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:

rciusergroup	attribute type: string

This may require a schema extension on your LDAP/LDAPS server. Consult your authentication server administrator to enable this attribute.

In addition, for Microsoft® Active Directory®, the standard LDAP memberOf is used.

From Microsoft Active Directory

Note: This should be attempted only by an experienced Active Directory® administrator.

Returning user role information from Microsoft's® Active Directory for Windows 2000® operating system server requires updating the LDAP/LDAPS schema. See your Microsoft documentation for details.

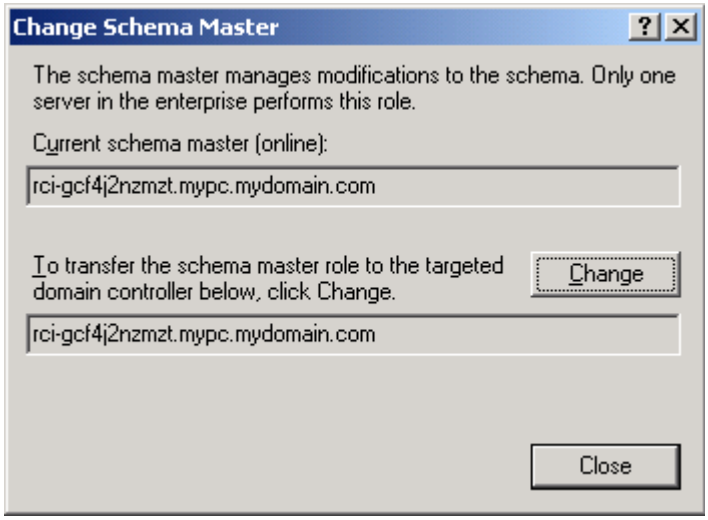
1. Install the schema plug-in for Active Directory. See Microsoft Active Directory documentation for instructions.
2. Run Active Directory Console and select Active Directory Schema.

Setting the Registry to Permit Write Operations to the Schema

To allow a domain controller to write to the schema, you must set a registry entry that permits schema updates.

To permit write operations to the schema:

1. Right-click the Active Directory® Schema root node in the left pane of the window and then click Operations Master. The Change Schema Master dialog appears.



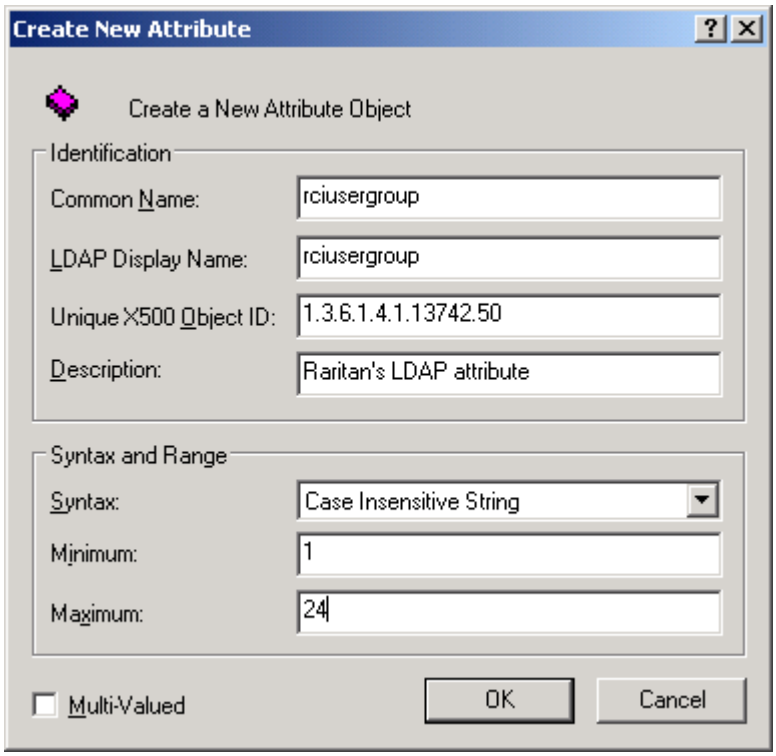
2. Select the "Schema can be modified on this Domain Controller" checkbox. **Optional**
3. Click OK.

Creating a New Attribute

To create new attributes for the rciusergroup class:

1. Click the + symbol before Active Directory® Schema in the left pane of the window.
2. Right-click Attributes in the left pane.

3. Click New and then choose Attribute. When the warning message appears, click Continue and the Create New Attribute dialog appears.



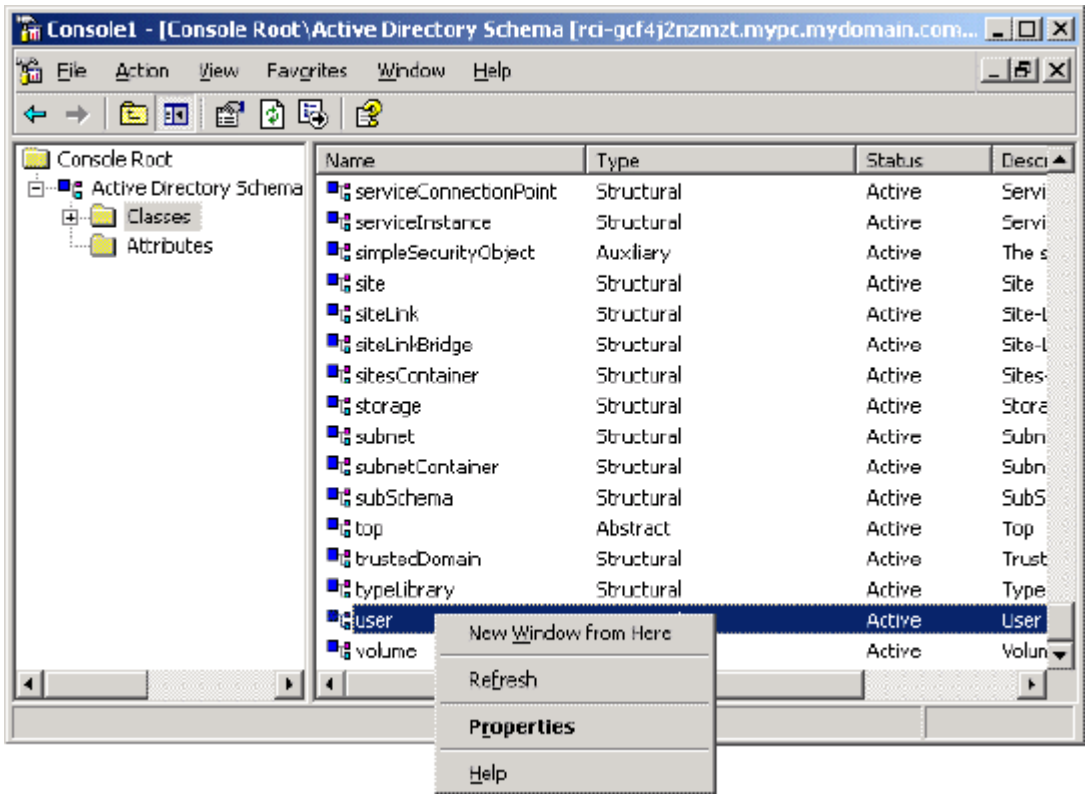
4. Type *rciusergroup* in the Common Name field.
5. Type *rciusergroup* in the LDAP Display Name field.
6. Type *1.3.6.1.4.1.13742.50* in the Unique x5000 Object ID field.
7. Type a meaningful description in the Description field.
8. Click the Syntax drop-down arrow and choose Case Insensitive String from the list.
9. Type *1* in the Minimum field.
10. Type *24* in the Maximum field.
11. Click OK to create the new attribute.

Adding Attributes to the Class

▶ **To add attributes to the class:**

1. Click Classes in the left pane of the window.

2. Scroll to the user class in the right pane and right-click it.



3. Choose Properties from the menu. The user Properties dialog appears.
4. Click the Attributes tab to open it.
5. Click Add.

6. Choose rciusergroup from the Select Schema Object list.

7. Click OK in the Select Schema Object dialog.
8. Click OK in the User Properties dialog.

Updating the Schema Cache

To update the schema cache:

1. Right-click Active Directory® Schema in the left pane of the window and select Reload the Schema.
2. Minimize the Active Directory Schema MMC (Microsoft® Management Console) console.

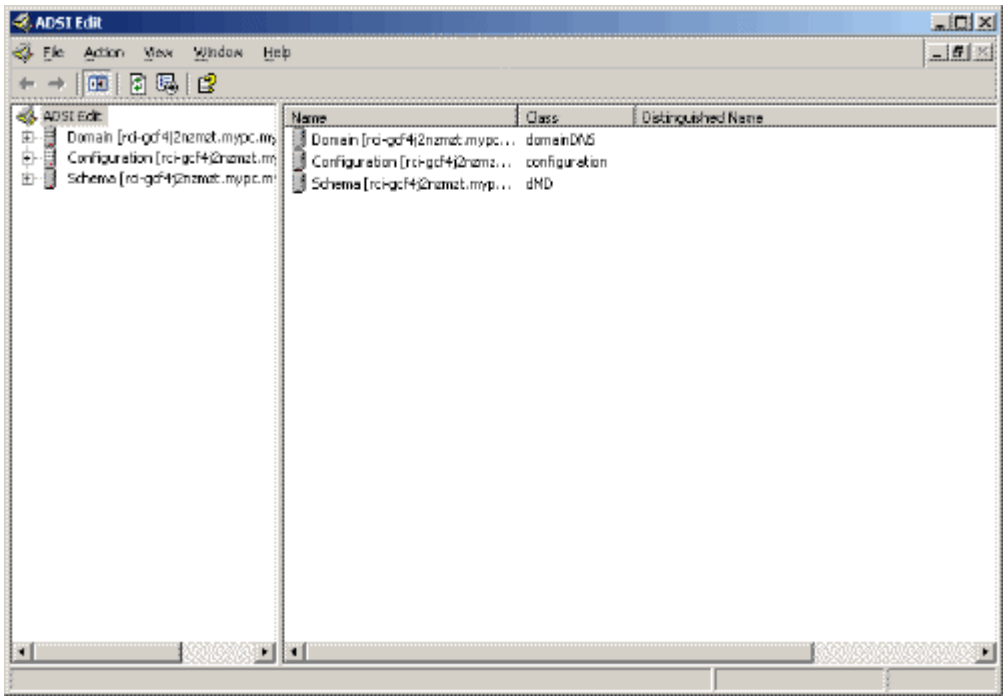
Editing rciusergroup Attributes for User Members

To run the Active Directory® script on a Windows 2003® server, use the script provided by Microsoft® (available on the Windows 2003 server installation CD). These scripts are loaded onto your system with a Microsoft® Windows 2003 installation. ADSI (Active Directory Service Interface) acts as a low-level editor for Active Directory, allowing you to perform common administrative tasks such as adding, deleting, and moving objects with a directory service.

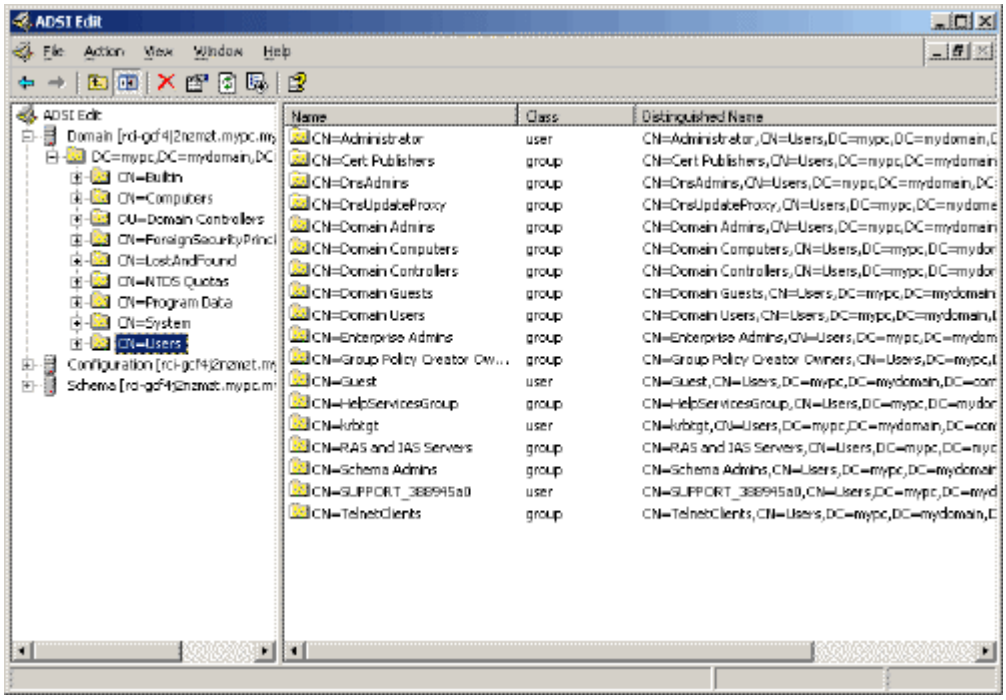
To edit the individual user attributes within the group rciusergroup:

1. From the installation CD, choose Support > Tools.
2. Double-click SUPTOOLS.MSI to install the support tools.

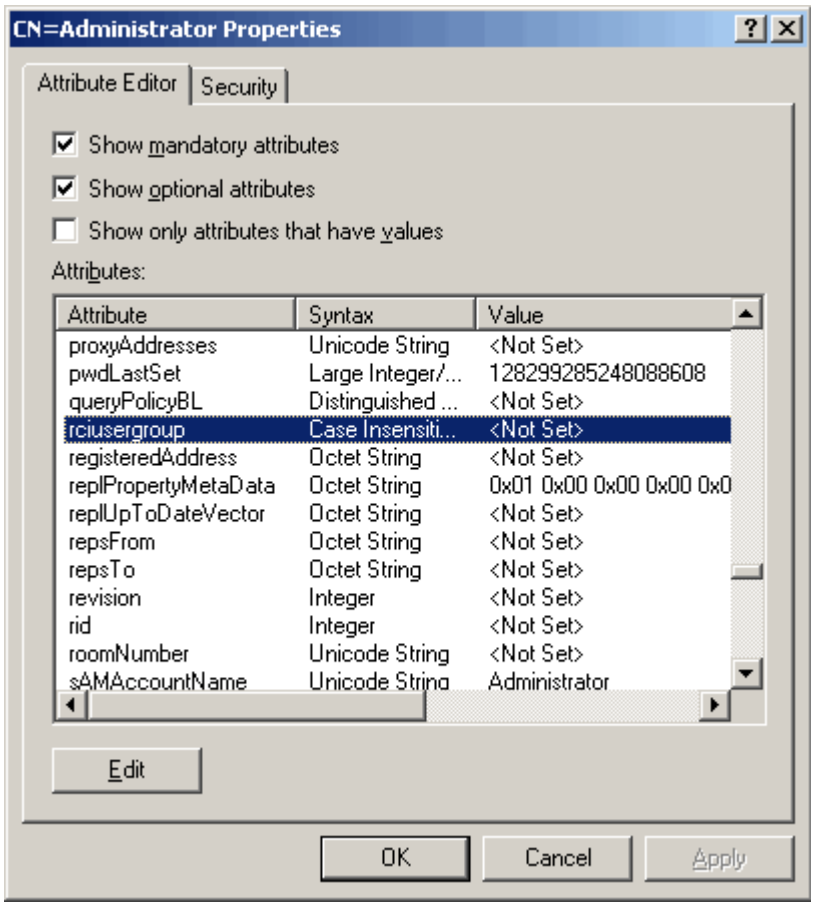
3. Go to the directory where the support tools were installed. Run adsiedit.msc. The ADSI Edit window opens.



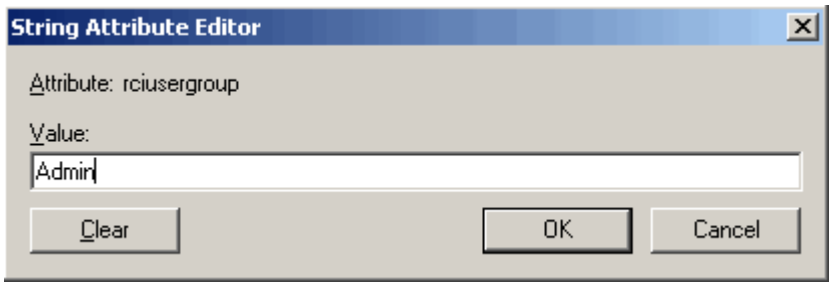
4. Open the Domain.
5. In the left pane of the window, select the CN=Users folder.



6. Locate the user name whose properties you want to adjust in the right pane. Right-click the user name and select Properties.
7. Click the Attribute Editor tab if it is not already open. Choose rciusergroup from the Attributes list.



8. Click Edit. The String Attribute Editor dialog appears.
9. Type the user role (created in the PXE) in the Edit Attribute field. Click OK.



Appendix G RADIUS Configuration Illustration

This section provides illustrations for configuring RADIUS authentication. One illustration is based on the Microsoft® Network Policy Server (NPS), and the other is based on a FreeRADIUS server.

The following steps are required for any RADIUS authentication:

1. Configure RADIUS authentication on the PXE. See *Adding Radius Servers* (on page 137).
2. Configure roles on the PXE. See *Creating Roles* (on page 99).
3. Configure PXE user credentials and roles on your RADIUS server.
   - To configure using standard attributes, see *Standard Attributes* (on page 404).
   - To configure using vendor-specific attributes, see *Vendor-Specific Attributes* (on page 423).

Note that we assume that the NPS is running on a Windows 2008 system in the NPS illustrations.

In This Chapter

Standard Attributes 404
Vendor-Specific Attributes 423
AD-Related Configuration 436

Standard Attributes

The RADIUS standard attribute "Filter-ID" is used to convey the group membership, that is, roles.

- If a user has multiple roles, configure multiple standard attributes for this user.
- The syntax of a standard attribute is:
  `Raritan:G{role-name}`

For configuration on NPS, see *NPS Standard Attribute Illustration* (on page 404).

For configuration on FreeRADIUS, see *FreeRADIUS Standard Attribute Illustration* (on page 422).

NPS Standard Attribute Illustration

To configure Windows 2008 NPS with the *standard attribute*, you must:

a. Add your PXE to NPS. See *Step A: Add Your PXE as a RADIUS Client* (on page 405).

b. On the NPS, configure Connection Request Policies and the standard attribute. See ***Step B: Configure Connection Policies and Standard Attributes*** (on page 409).

Some configuration associated with Microsoft Active Directory (AD) is also required for RADIUS authentication. See ***AD-Related Configuration*** (on page 436).

Step A: Add Your PXE as a RADIUS Client

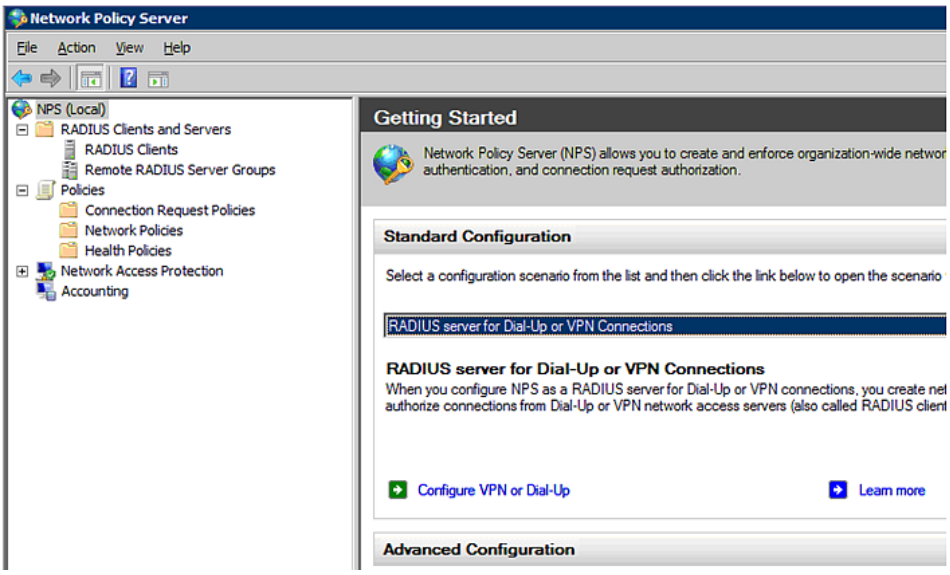
The RADIUS implementation on a PXE follows the standard RADIUS Internet Engineering Task Force (IETF) specification so you must select "RADIUS Standard" as its vendor name when configuring the NPS server.

Presumptions in the illustration:

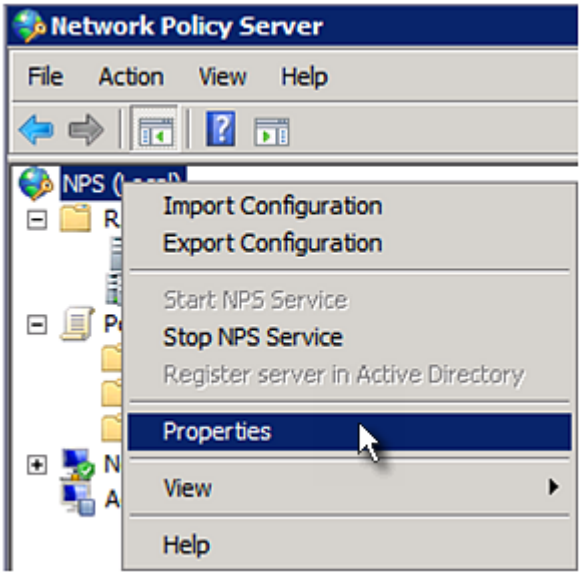
- IP address of your PXE = `192.168.56.29`
- RADIUS authentication port specified for PXE: *1812*
- RADIUS accounting port specified for PXE: *1813*

To add your PXE to the RADIUS NPS:

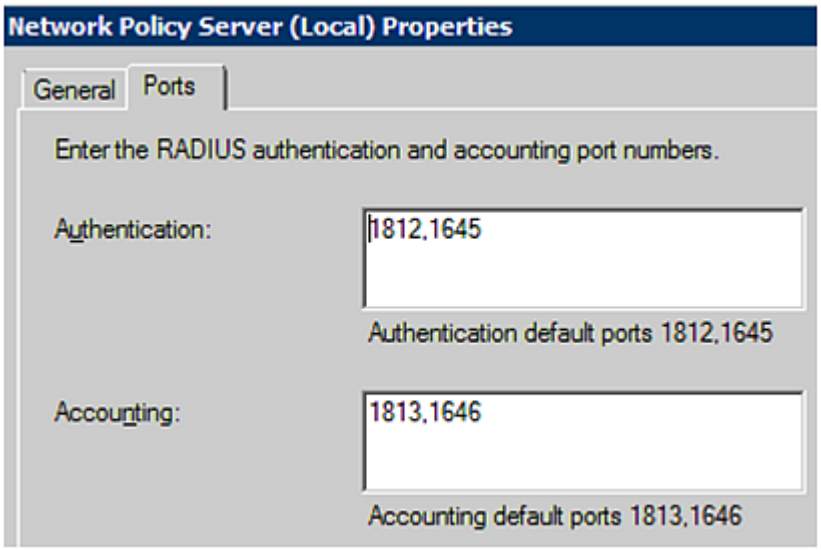
1. Choose Start > Administrative Tools > Network Policy Server. The Network Policy Server console window opens.



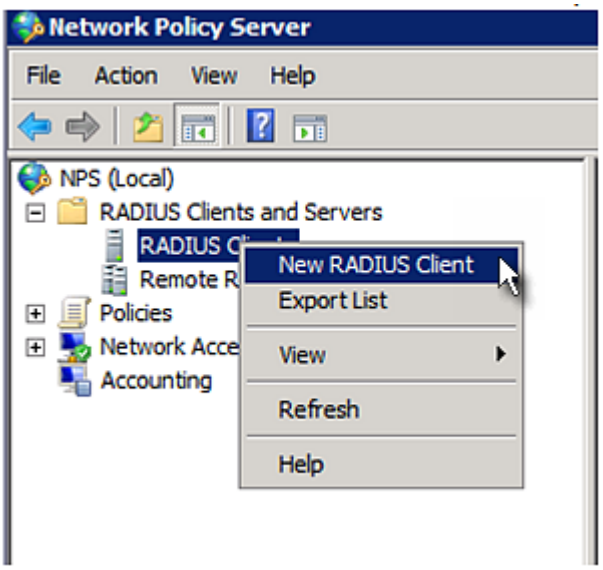
2. Right-click NPS (Local), and select Properties.



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.

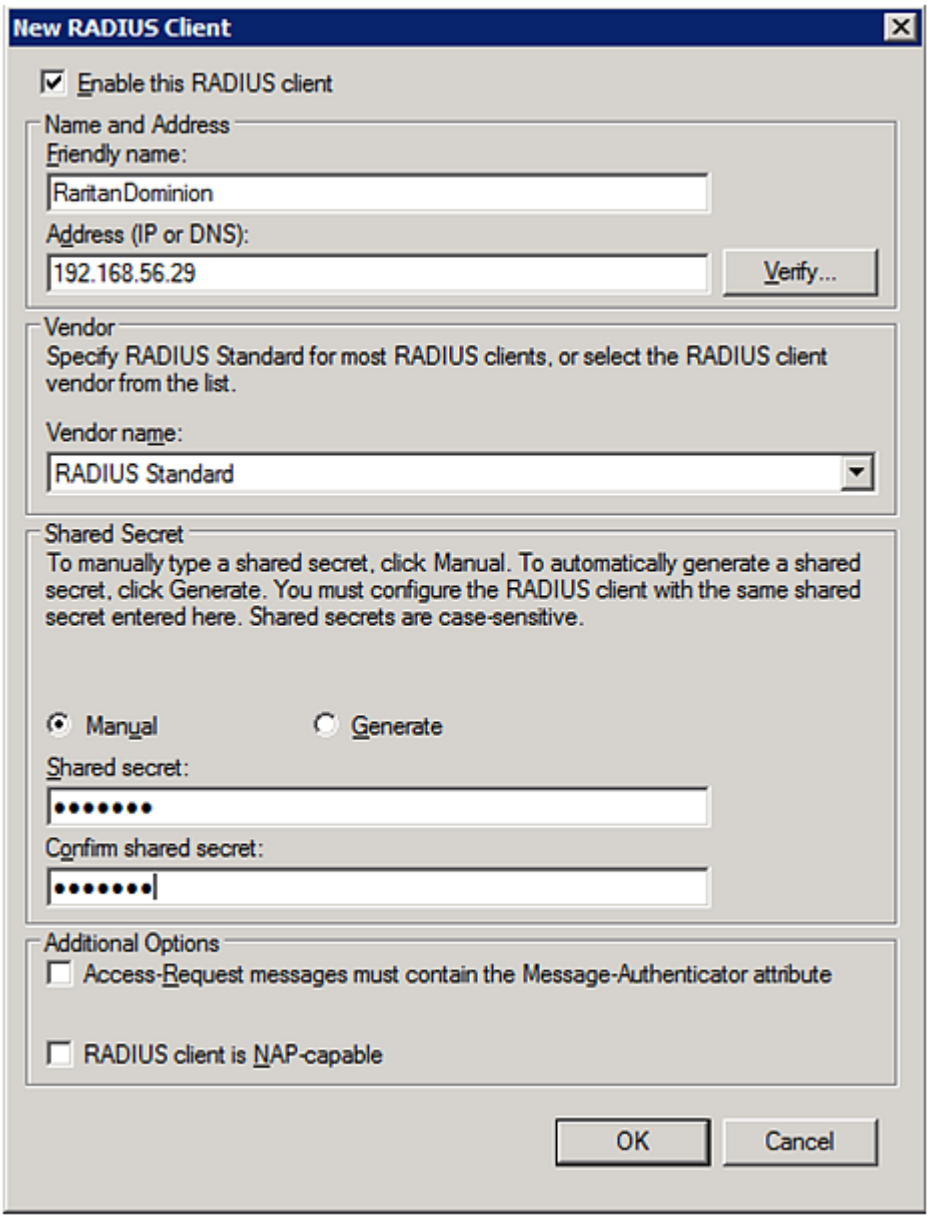


3. Under "RADIUS Clients and Servers," right-click RADIUS Client and select New RADIUS Client. The New RADIUS Client dialog appears.



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.



5. Click OK.

Step B: Configure Connection Policies and Standard Attributes

You need to configure the following for connection request policies:

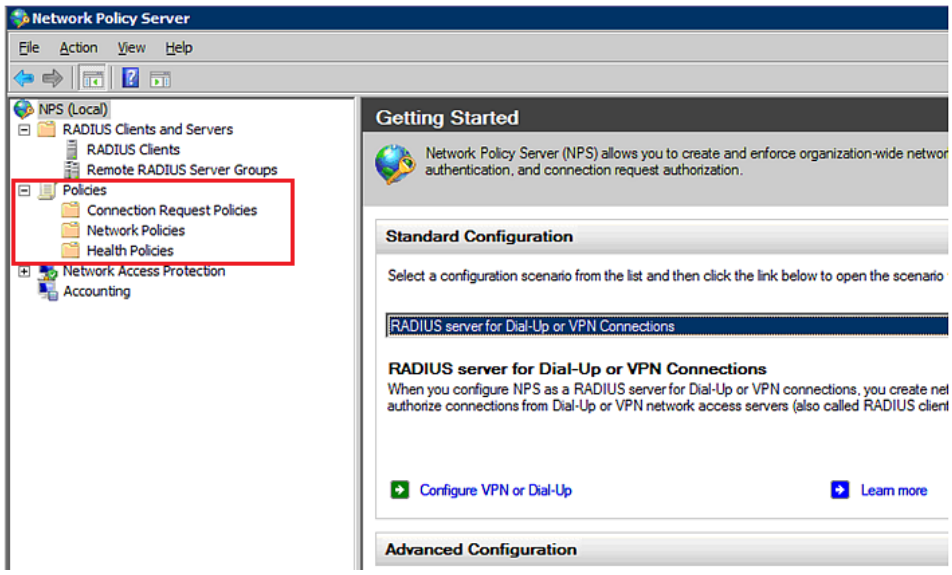
- IP address or host name of the PXE
- Connection request forwarding method
- Authentication method(s)
- Standard RADIUS attributes

Presumptions in the illustration:

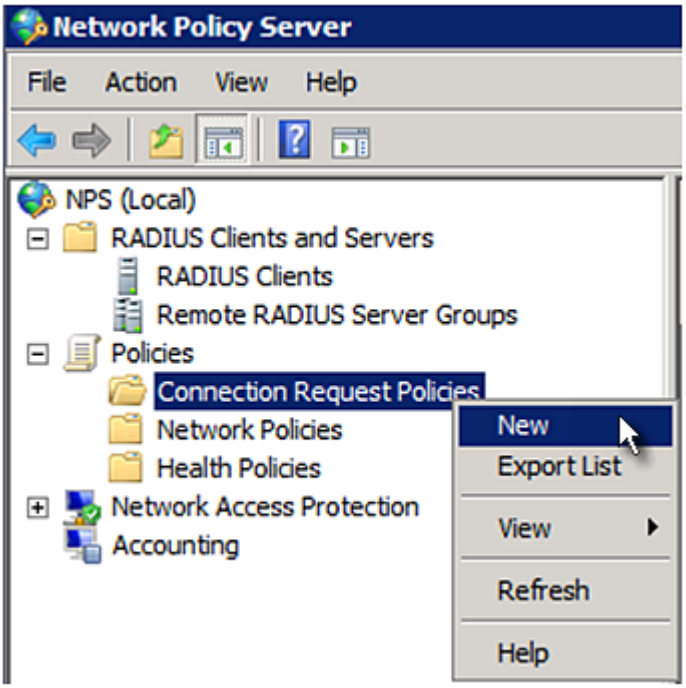
- IP address of your PXE = `192.168.56.29`
- *Local* NPS server is used
- RADIUS protocol selected on your PXE = `CHAP`
- Existing role of your PXE = `Admin`

Illustration:

1. Open the NPS console, and expand the Policies folder.

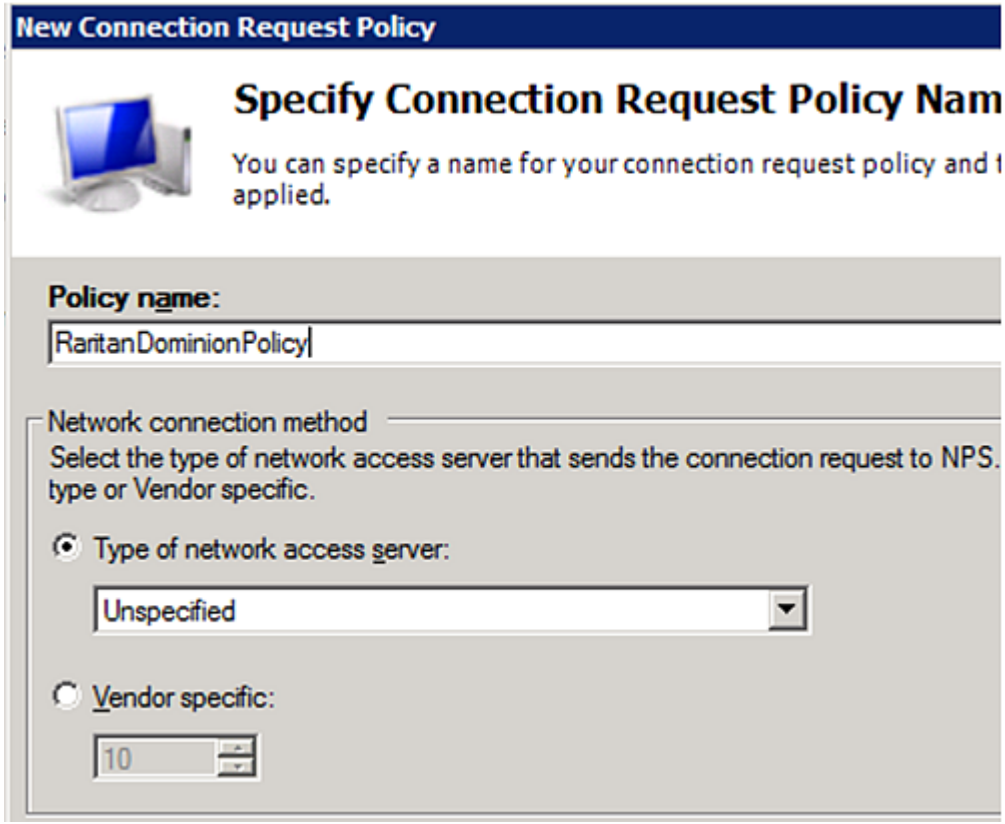


2. Right-click Connection Request Policies and select New. The New Connection Request Policy dialog appears.

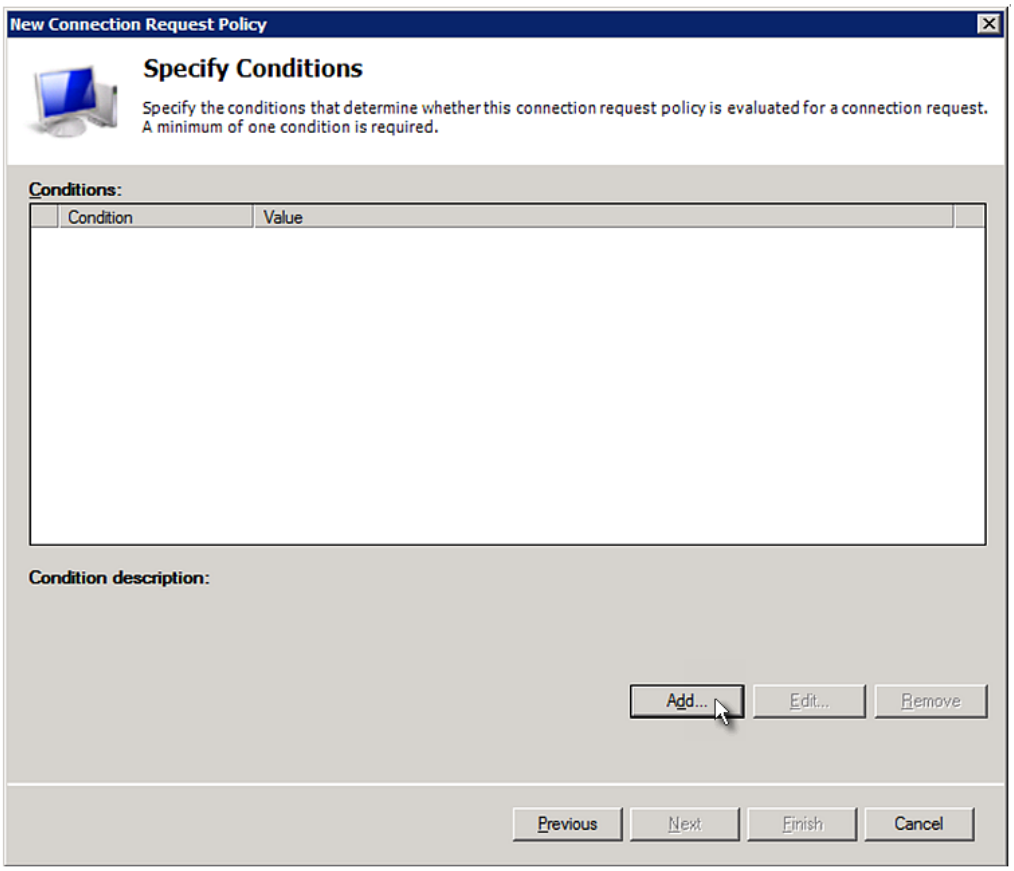


3. Type a descriptive name for identifying this policy in the "Policy name" field.

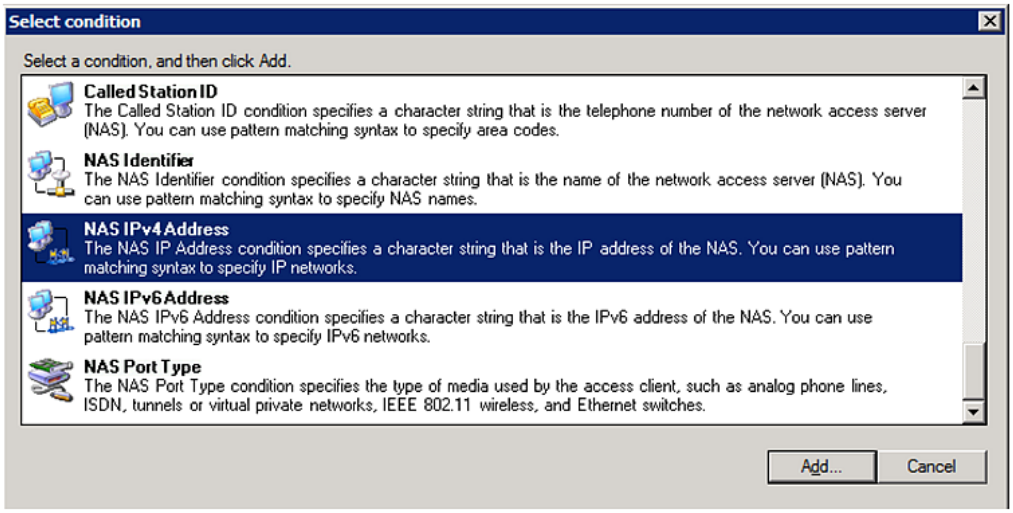
- You can leave the "Type of network access server" field to the default -- Unspecified.



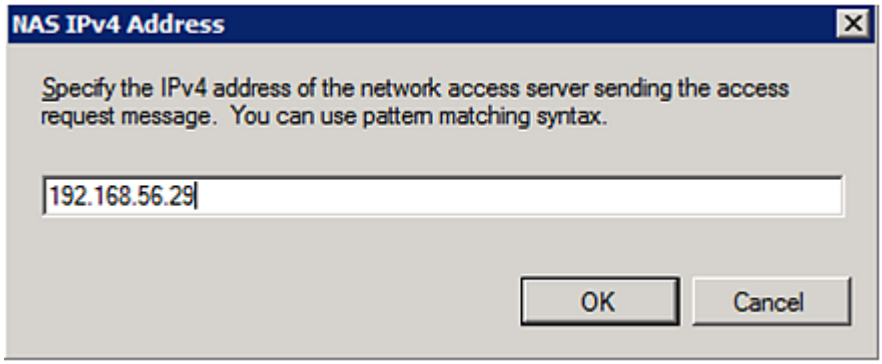
4. Click Next to show the "Specify Conditions" screen. Click Add.



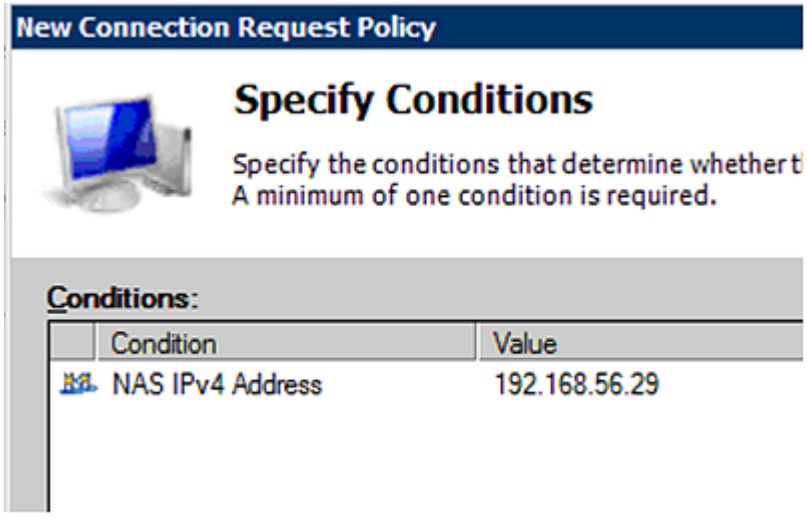
5. The "Select condition" dialog appears. Click Add.



6. The NAS IPv4 Address dialog appears. Type the PXE IP address -- *192.168.56.29*, and click OK.

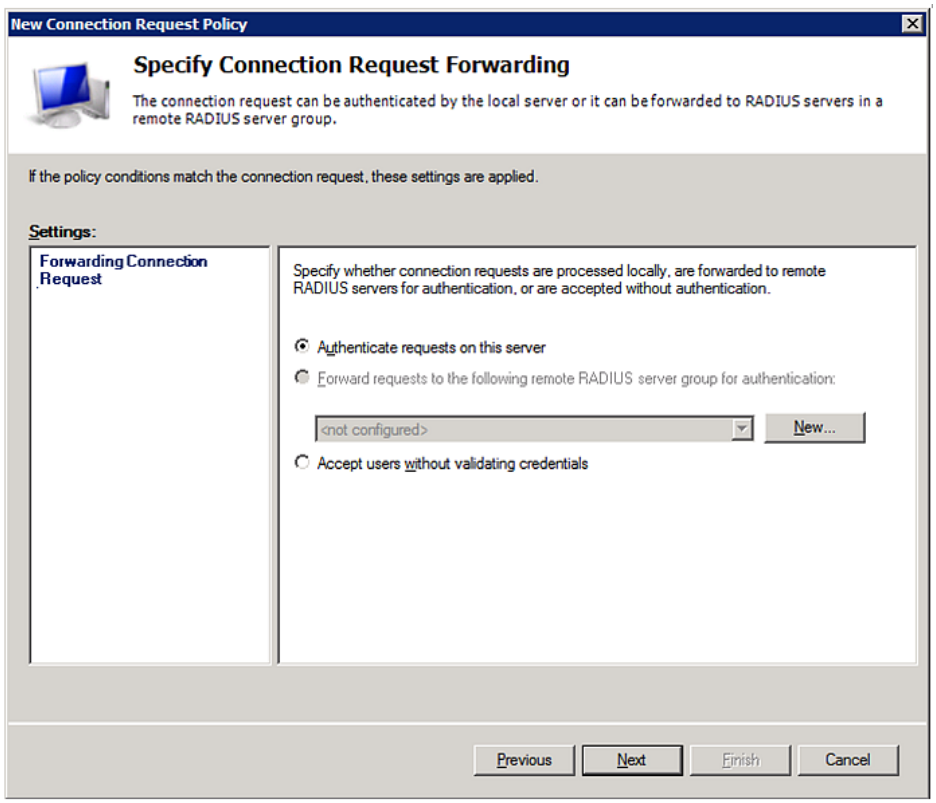


7. Click Next in the New Connection Request Policy dialog.



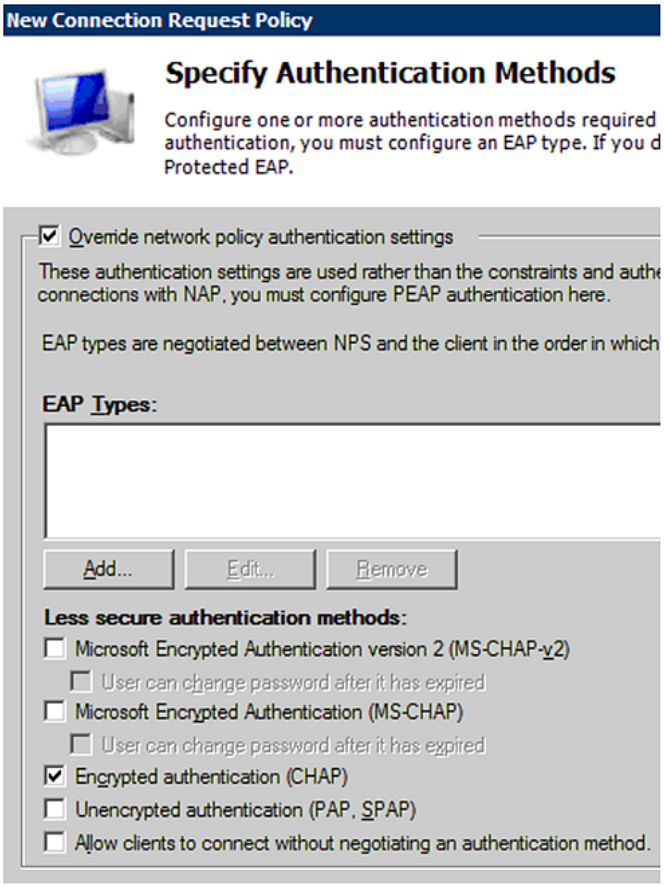
8. Select "Authenticate requests on this server" because a local NPS server is used in this example. Then click Next.

Note: Connection Request Forwarding options must match your environment.

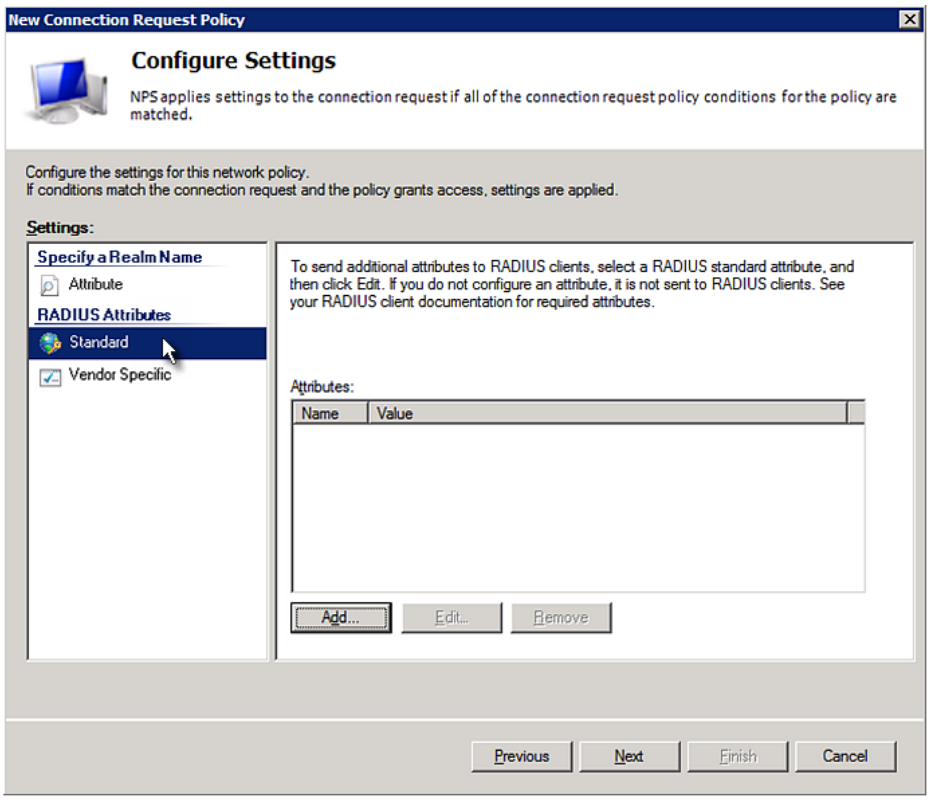


9. When the system prompts you to select the authentication method, select the following two options:
   - Override network policy authentication settings
   - CHAP -- the PXE uses "CHAP" in this example

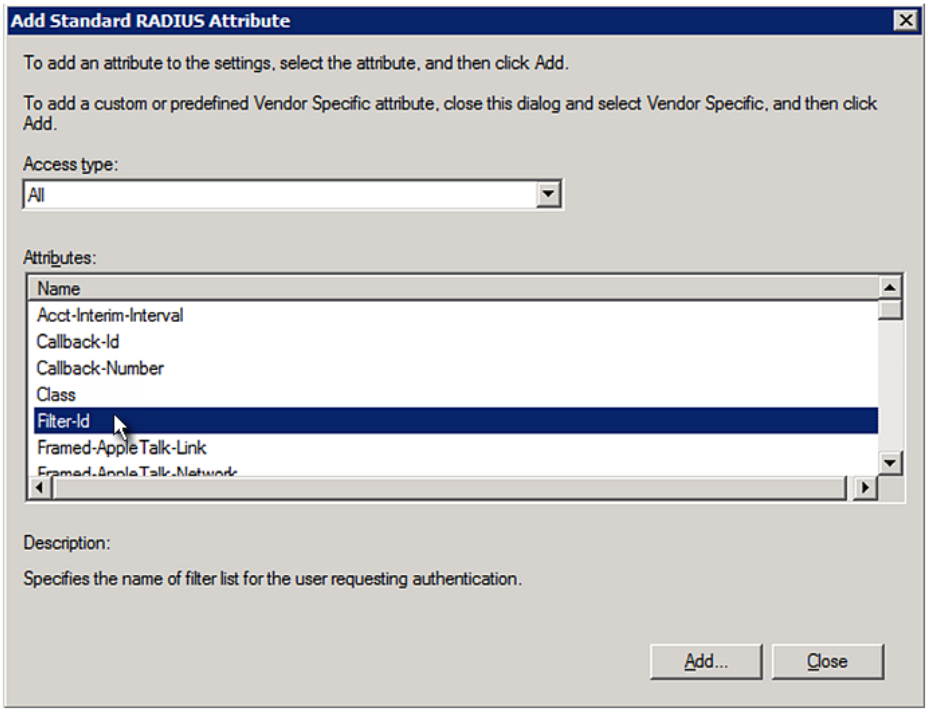
Note: If your PXE uses PAP, then select "PAP."



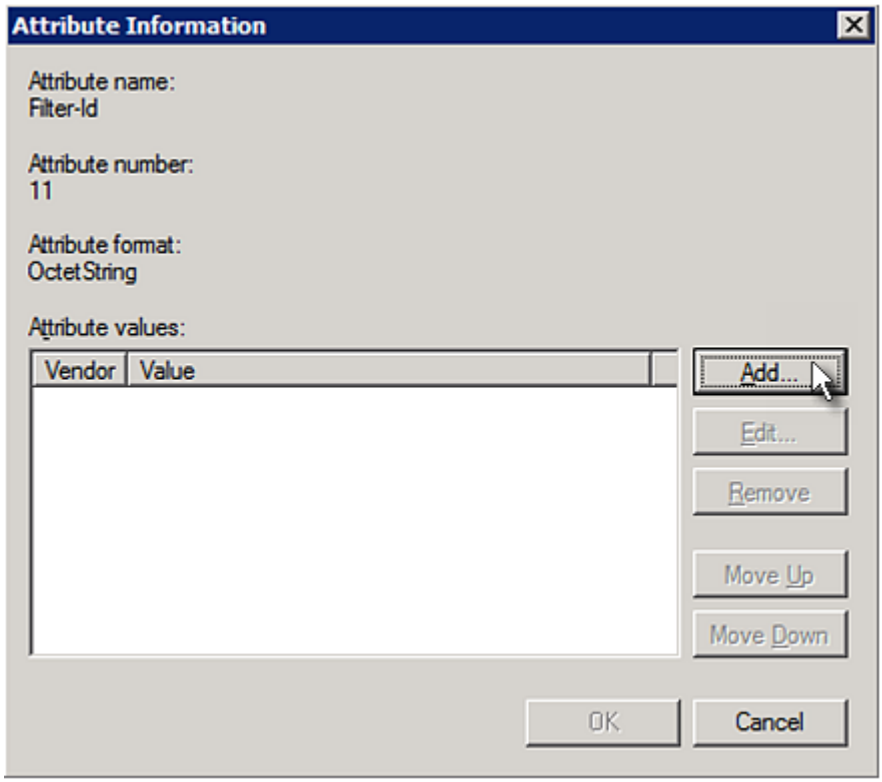
10. Select Standard to the left of the dialog and then click Add.



11. Select Filter-Id from the list of attributes and click Add.

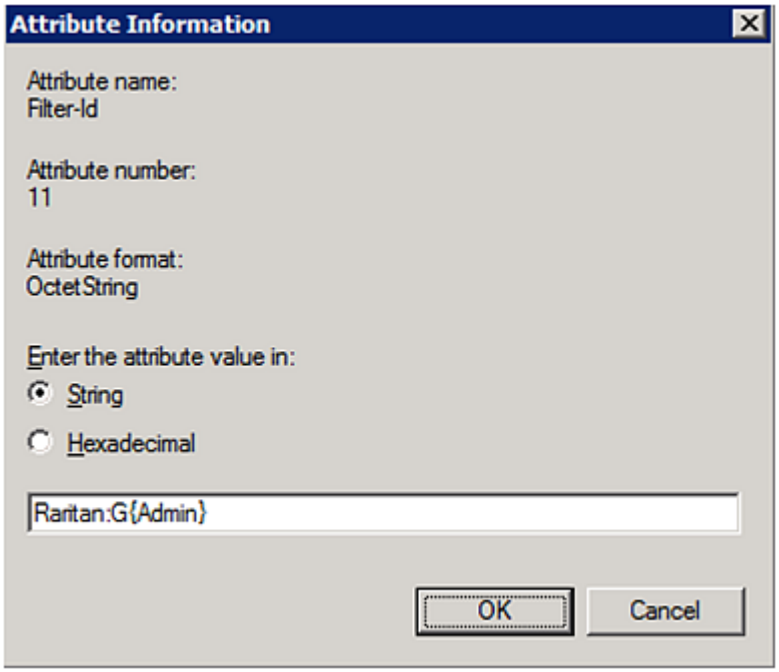


12. In the Attribute Information dialog, click Add.

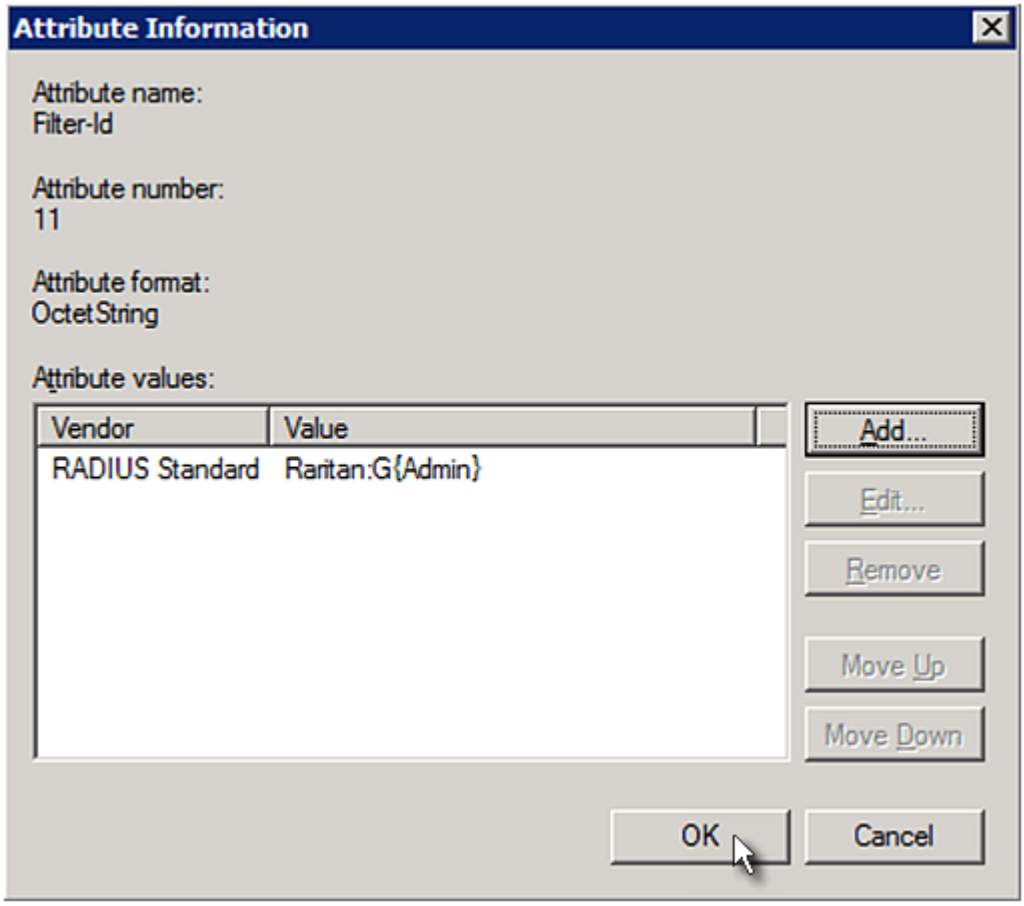


13. Select String, type *Raritan:G{Admin}* in the text box, and then click OK.

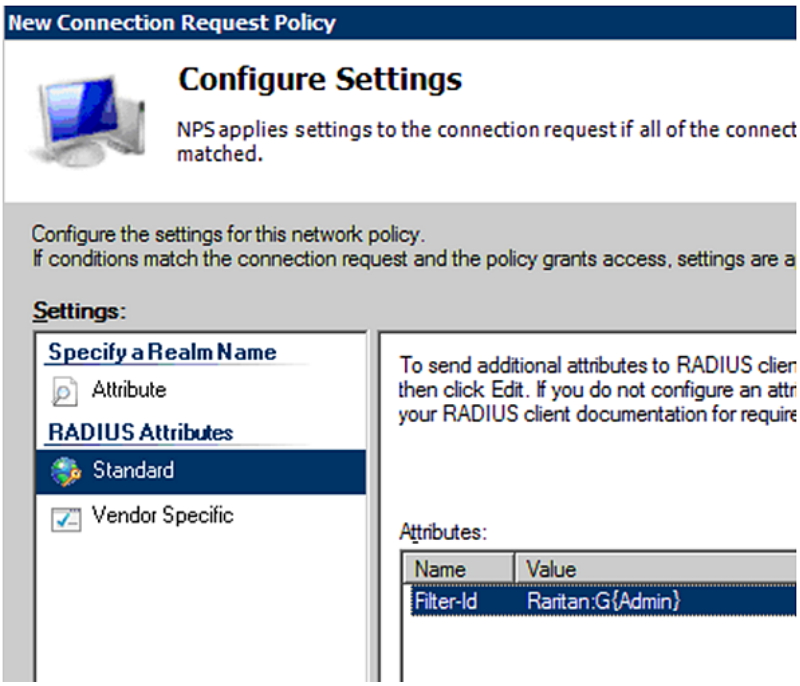
Admin inside the curved brackets {} is the existing role on the PXE. It is recommended to use the Admin role to test this configuration. The role name is case sensitive.



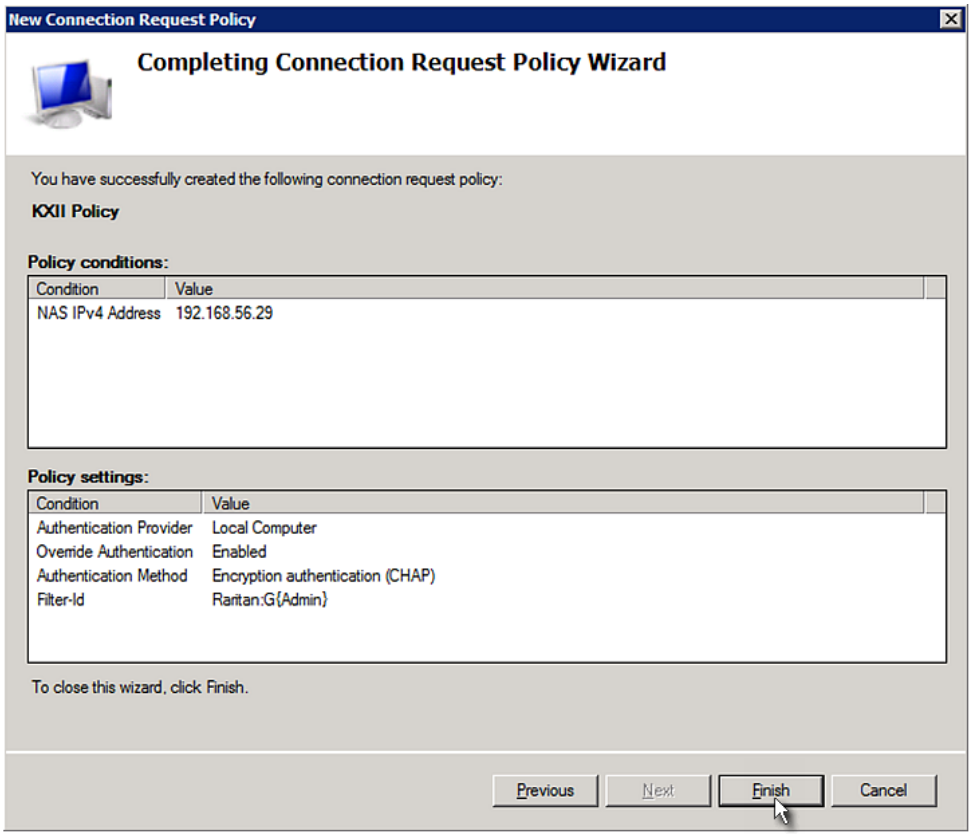
14. The new attribute is added. Click OK.



15. Click Next to continue.



16. A summary showing connection request policy settings is displayed. Click Finish to close the dialog.



FreeRADIUS Standard Attribute Illustration

With standard attributes, NO dictionary files are required. You simply add all user data, including user names, passwords, and roles, in the following FreeRADIUS path.

`/etc/raddb/users`

Presumptions in the illustration:

- User name = `steve`
- Steve's password = `test123`
- Steve's roles = `Admin` and `SystemTester`

To create a user profile for "steve" in FreeRADIUS:

1. Go to this location: `/etc/raddb/users`.
2. Add the data of the user "steve" by typing the following. Note that the values after the equal sign (=) must be enclosed in double quotes (").

```
steve Cleartext-Password := "test123"
Filter-ID = "Raritan:G{Admin}",
Filter-ID = "Raritan:G{SystemTester}"
```

Vendor-Specific Attributes

You must specify the following properties when using a RADIUS vendor-specific attribute (VSA).

- Vendor code = `13742`
- Vendor-assigned attribute number = `26`
- Attribute format = `String`

The syntax of the vendor-specific attribute for specifying one or multiple roles is:

`Raritan:G{role-name1 role-name2 role-name3}`

For configuration on NPS, see ***NPS VSA Illustration*** (on page 423).

For configuration on FreeRADIUS, see ***FreeRADIUS VSA Illustration*** (on page 435).

NPS VSA Illustration

To configure Windows 2008 NPS with the *vendor-specific attribute*, you must:

a. Add your PXE to NPS. See ***Step A: Add Your PXE as a RADIUS Client*** (on page 405).

b. On the NPS, configure connection request policies and the vendor-specific attribute. See ***Step B: Configure Connection Policies and Vendor-Specific Attributes*** (on page 428).

Some configuration associated with Microsoft Active Directory (AD) is also required for RADIUS authentication. See ***AD-Related Configuration*** (on page 436).

Step A: Add Your PXE as a RADIUS Client

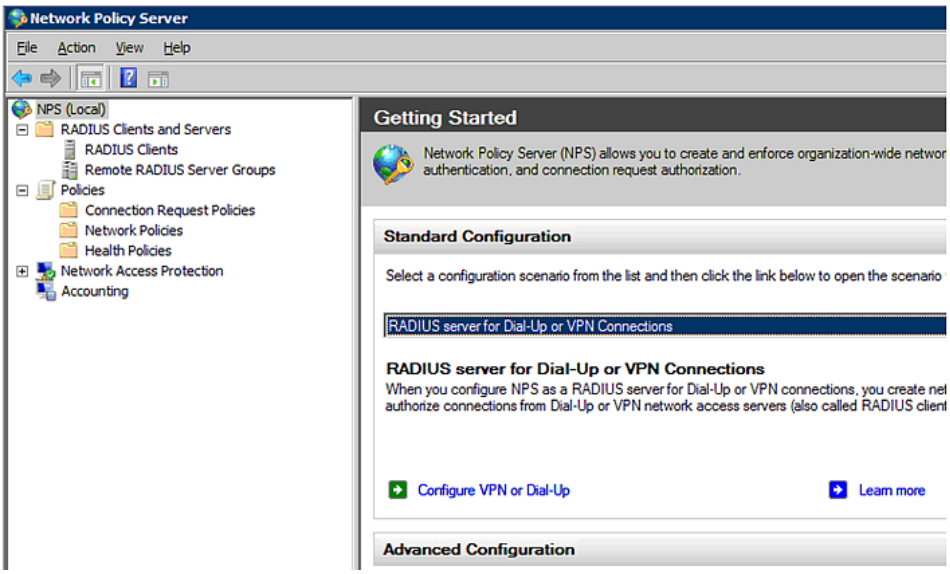
The RADIUS implementation on a PXE follows the standard RADIUS Internet Engineering Task Force (IETF) specification so you must select "RADIUS Standard" as its vendor name when configuring the NPS server.

Presumptions in the illustration:

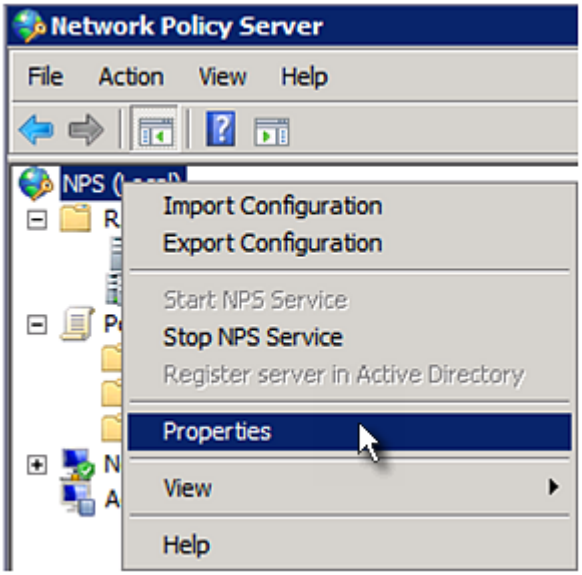
- IP address of your PXE = `192.168.56.29`
- RADIUS authentication port specified for PXE: *1812*
- RADIUS accounting port specified for PXE: *1813*

To add your PXE to the RADIUS NPS:

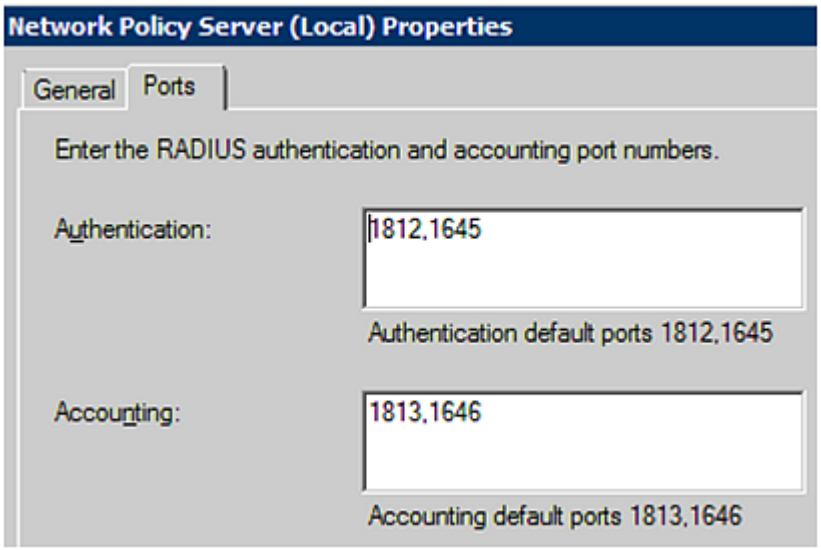
1. Choose Start > Administrative Tools > Network Policy Server. The Network Policy Server console window opens.



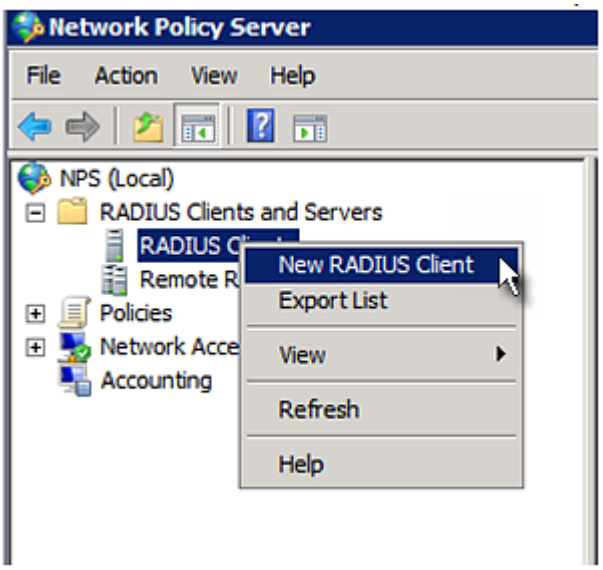
2. Right-click NPS (Local), and select Properties.



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.

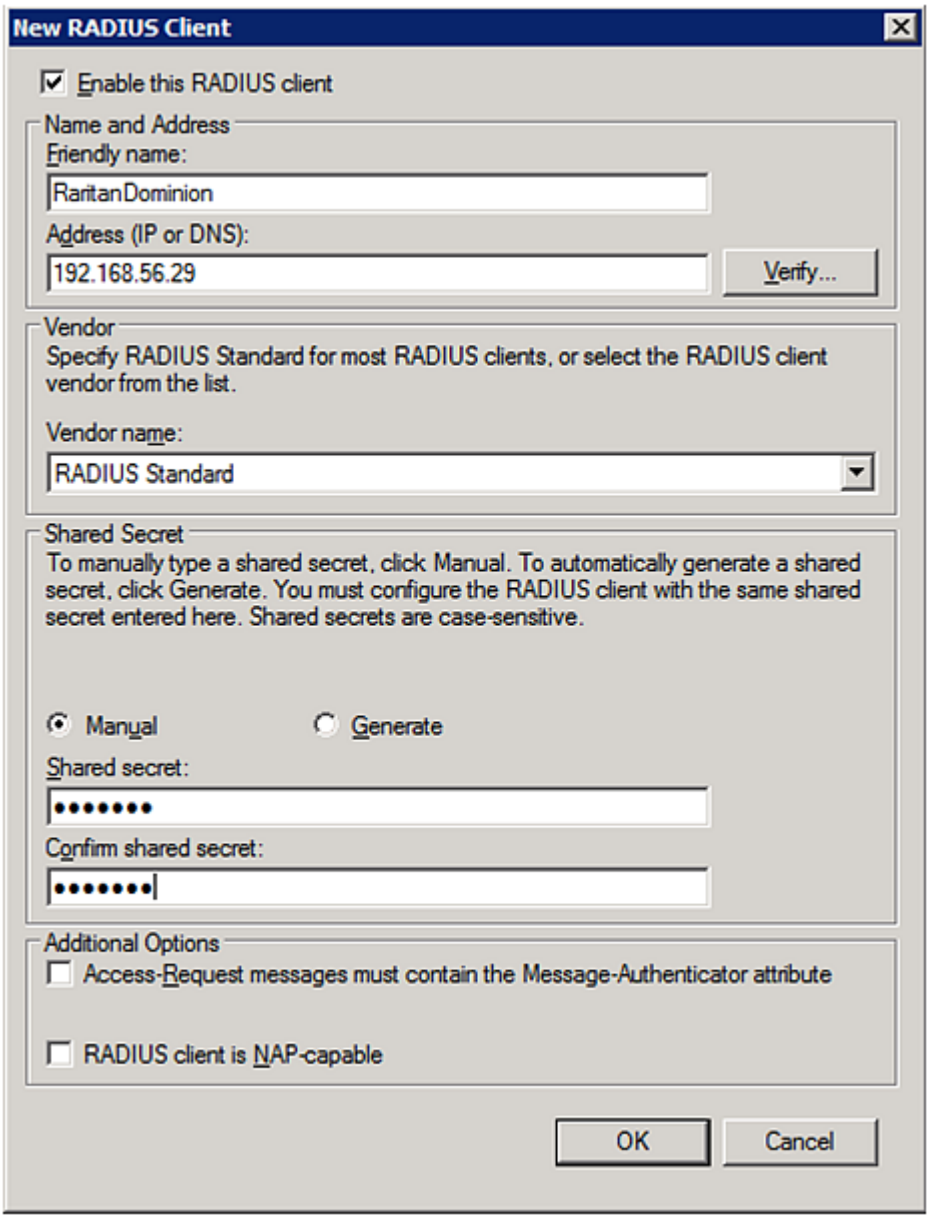


3. Under "RADIUS Clients and Servers," right-click RADIUS Client and select New RADIUS Client. The New RADIUS Client dialog appears.



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.



5. Click OK.

Step B: Configure Connection Policies and Vendor-Specific Attributes

You need to configure the following for connection request policies:

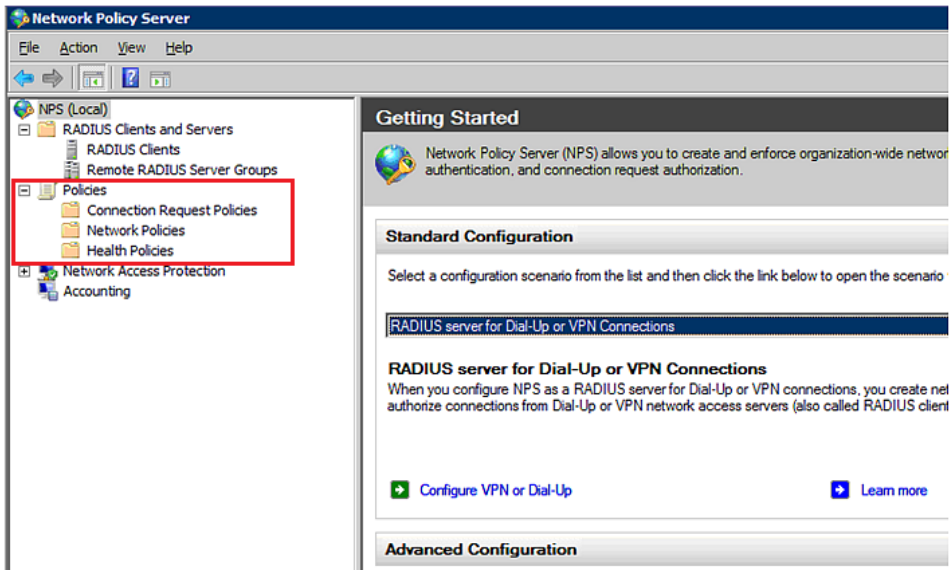
- IP address or host name of the PXE
- Connection request forwarding method
- Authentication method(s)
- Standard RADIUS attributes

Presumptions in the illustration:

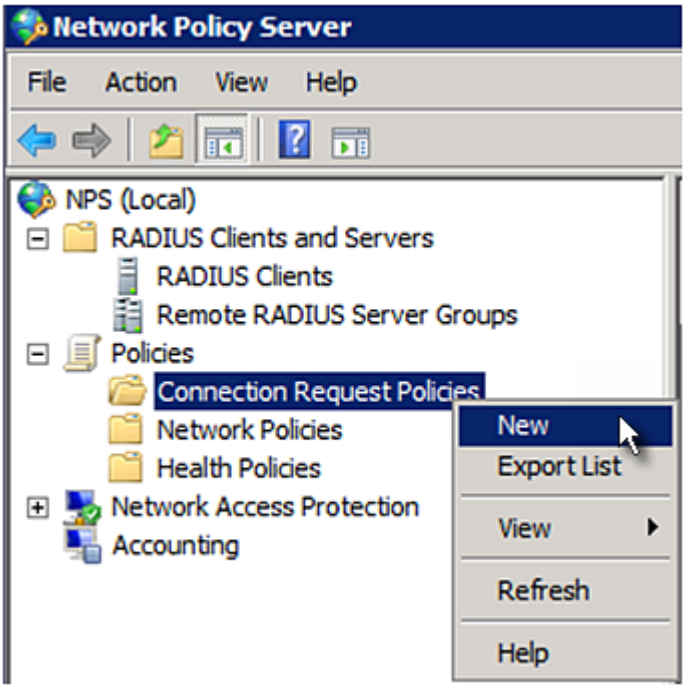
- IP address of your PXE = `192.168.56.29`
- *Local* NPS server is used
- RADIUS protocol selected on your PXE = `CHAP`
- Existing roles of your PXE = `Admin`, `User` and `SystemTester`

Illustration:

1. Open the NPS console, and expand the Policies folder.

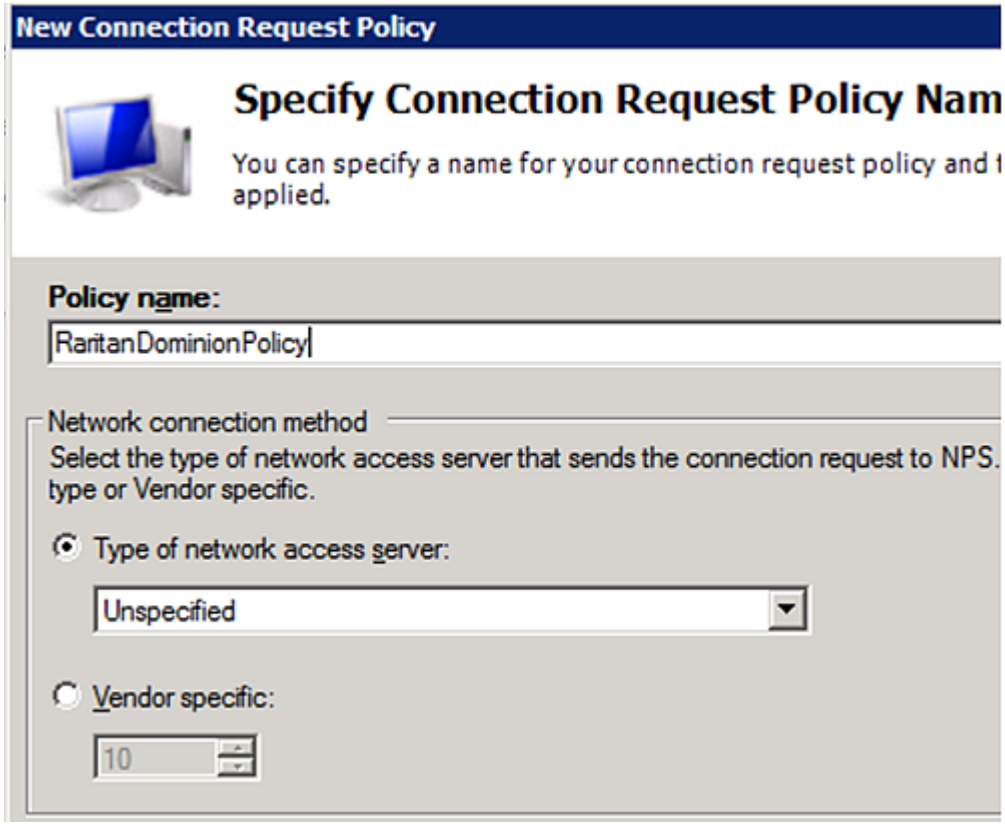


2. Right-click Connection Request Policies and select New. The New Connection Request Policy dialog appears.

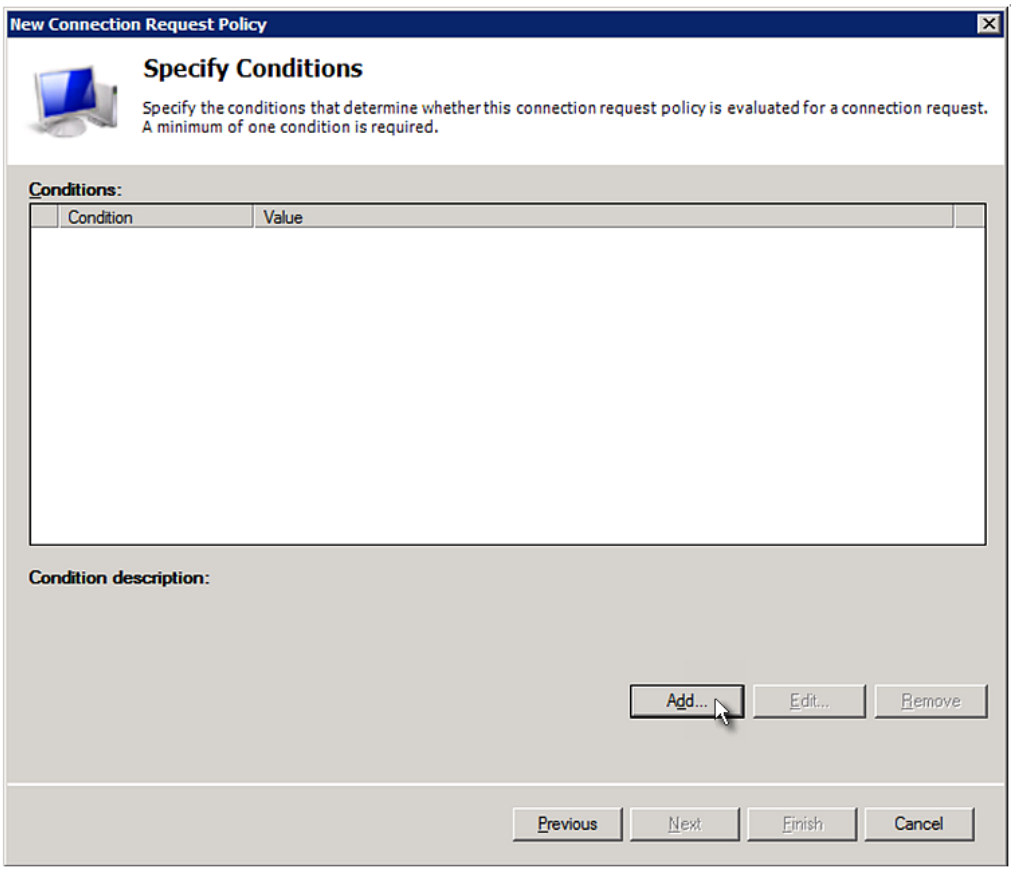


3. Type a descriptive name for identifying this policy in the "Policy name" field.

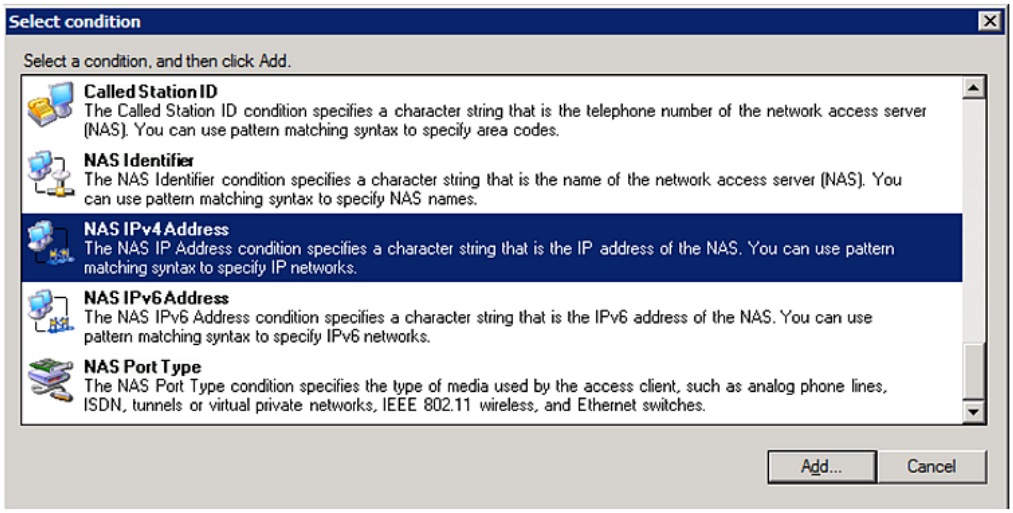
- You can leave the "Type of network access server" field to the default -- Unspecified.



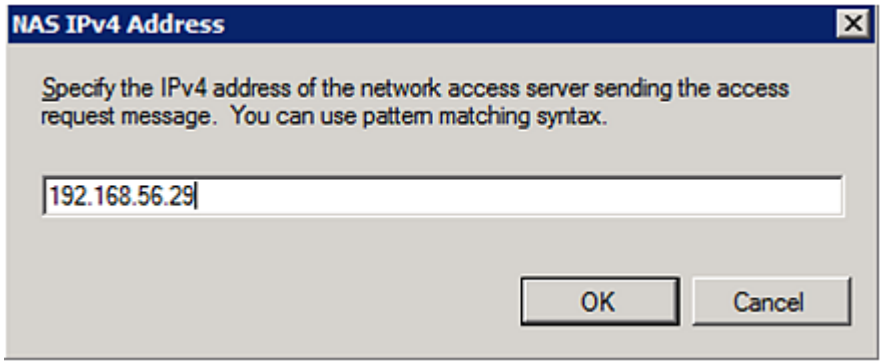
4. Click Next to show the "Specify Conditions" screen. Click Add.



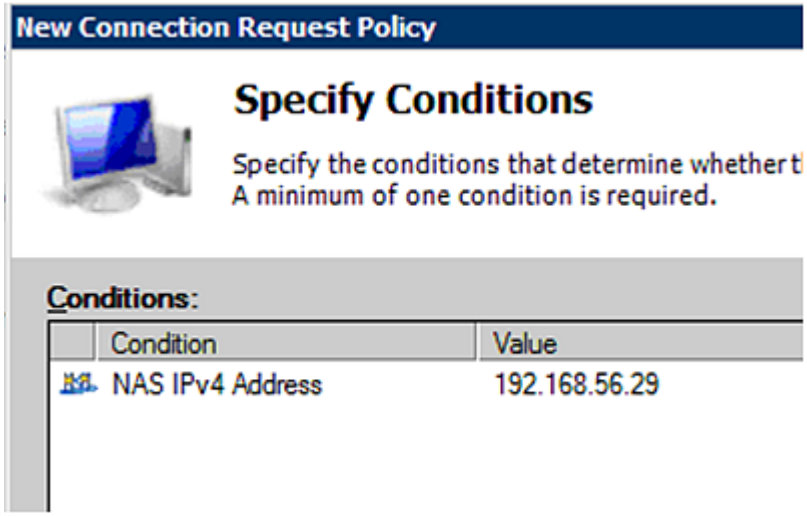
5. The "Select condition" dialog appears. Click Add.



6. The NAS IPv4 Address dialog appears. Type the PXE IP address -- *192.168.56.29*, and click OK.

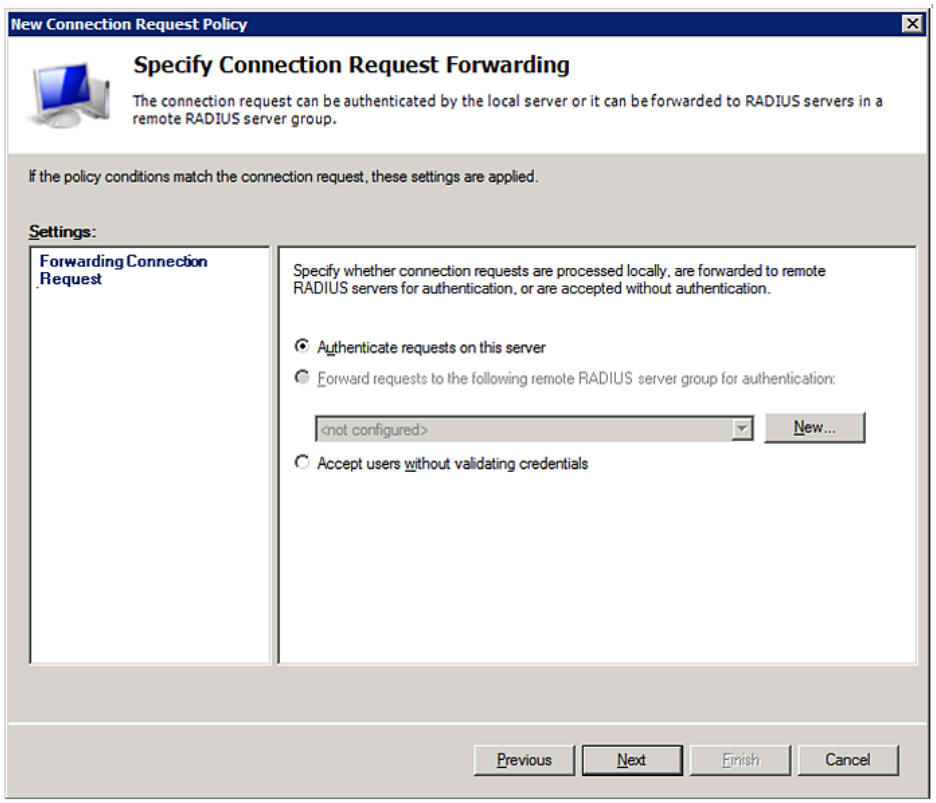


7. Click Next in the New Connection Request Policy dialog.



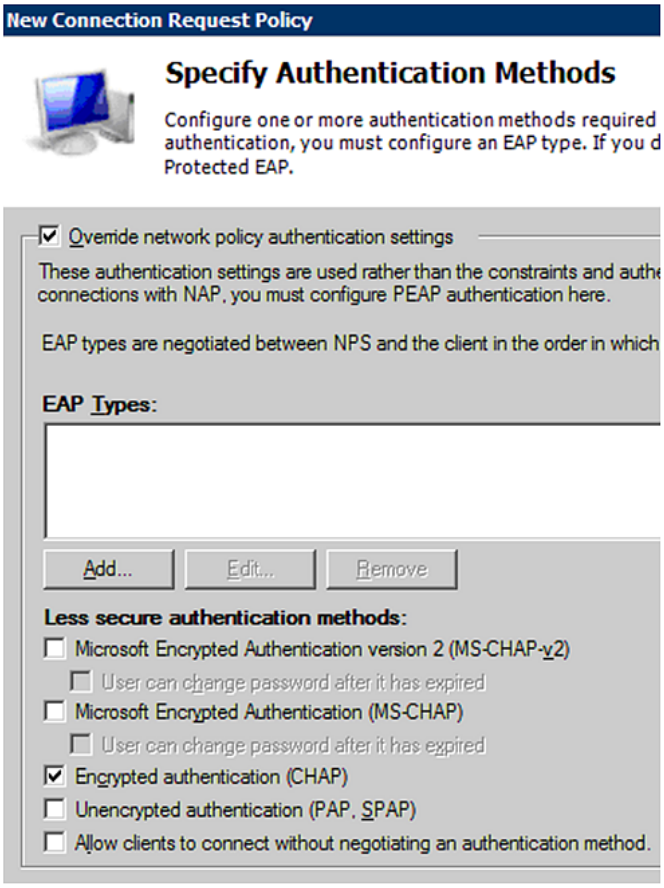
8. Select "Authenticate requests on this server" because a local NPS server is used in this example. Then click Next.

Note: Connection Request Forwarding options must match your environment.



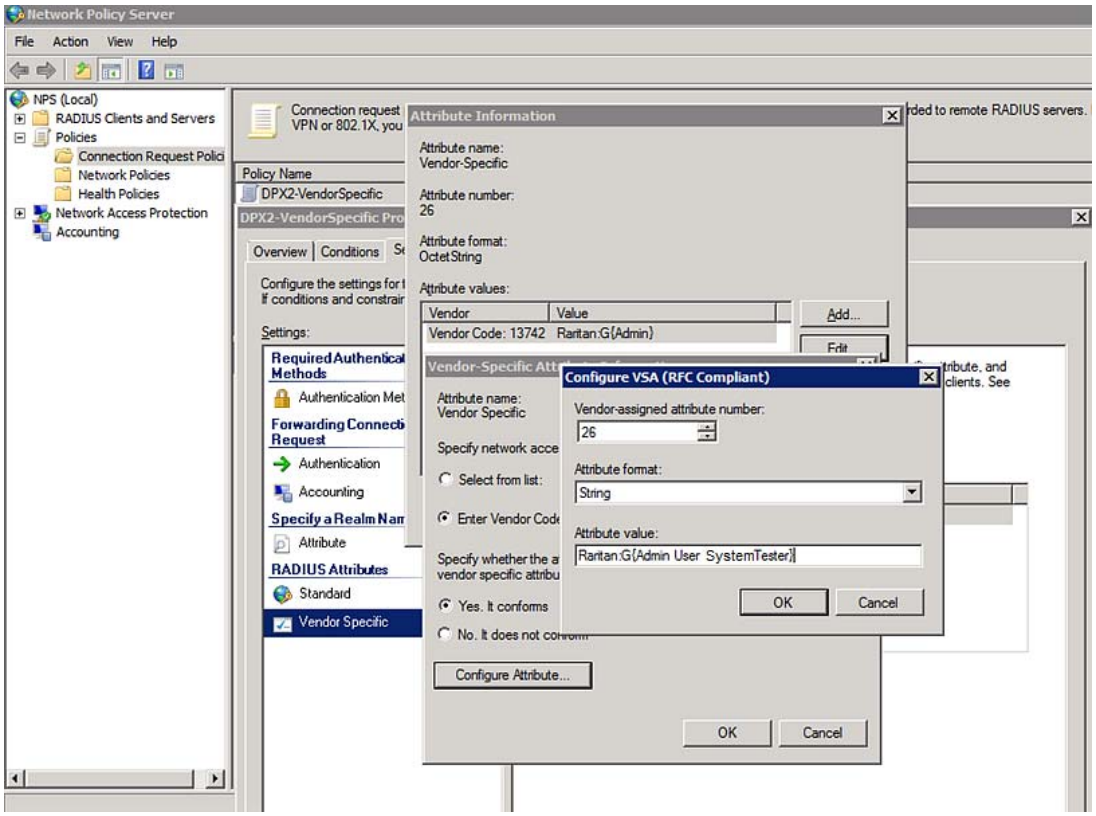
9. When the system prompts you to select the authentication method, select the following two options:
   - Override network policy authentication settings
   - CHAP -- the PXE uses "CHAP" in this example

Note: If your PXE uses PAP, then select "PAP."



10. Select Vendor Specific to the left of the dialog, and click Add. The Add Vendor Specific Attribute dialog appears.
11. Select Custom in the Vendor field, and click Add. The Attribute Information dialog appears.
12. Click Add, and the Vendor-Specific Attribute Information dialog appears.
13. Click "Enter Vendor Code" and type *13742*.
14. Select "Yes, it conforms" to indicate that the custom attribute conforms to the RADIUS Request For Comment (RFC).
15. Click Configure Attribute, and then:
    a. Type *26* in the "Vendor-assigned attribute number" field.
    b. Select String in the "Attribute format" field.
    c. Type *Raritan:G{Admin User SystemTester}* in the "Attribute value" field. In this example, three roles 'Admin,' 'User' and 'SystemTester' are specified inside the curved brackets {}.

Note that multiple roles are separated with a space.



16. Click OK.

FreeRADIUS VSA Illustration

A vendor-specific dictionary file is required for the vendor-specific-attribute configuration on FreeRADIUS. Therefore, there are two major configuration steps.

a. Use a dictionary to define the Raritan vendor-specific attribute

b. Add all user data, including user names, passwords, and roles

Presumptions in the illustration:

- Raritan attribute = `Raritan-User-Roles`
- User name = `steve`
- Steve's password = `test123`
- Steve's roles = `Admin`, `User` and `SystemTester`

Step A -- define the vendor-specific attribute in FreeRADIUS:

1. Go to this location: `/etc/raddb/dictionary`.
2. Type the following in the Raritan dictionary file.

```
VENDOR Raritan 13742
BEGIN-VENDOR Raritan
ATTRIBUTE Raritan-User-Roles 26 string
END-VENDOR Raritan
```

Step B -- create a user profile for "steve" in FreeRADIUS:

1. Go to this location: `/etc/raddb/users`.
2. Add the data of the user "steve" by typing the following. Note that the values after the equal sign (=) must be enclosed in double quotes (").

```
steve Cleartext-Password := "test123"
Raritan-PDU-User-Roles = "Raritan:G{Admin User SystemTester}"
```

AD-Related Configuration

When RADIUS authentication is intended, make sure you also configure the following settings related to Microsoft Active Directory (AD):

- Register the NPS server in AD
- Configure remote access permission for users in AD

The NPS server is registered in AD only when NPS is configured for the FIRST time and user accounts are created in AD.

If CHAP authentication is used, you must enable the following feature for user accounts created in AD:

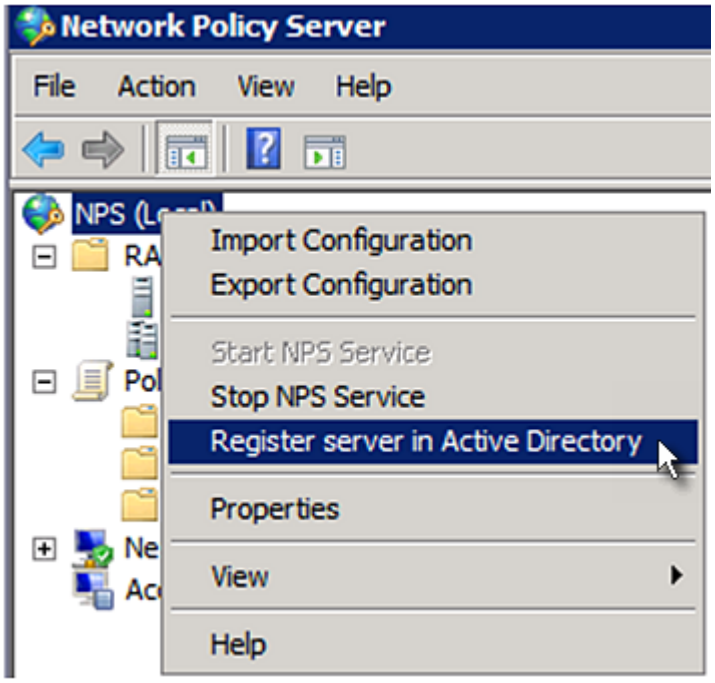
- Store password using reversible encryption

Important: Reset the user password if the password is set before you enable the "Store password using reversible encryption" feature.

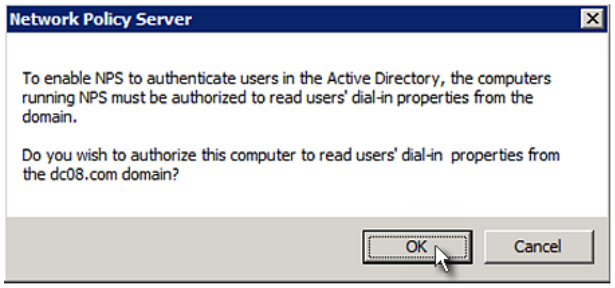
To register NPS:

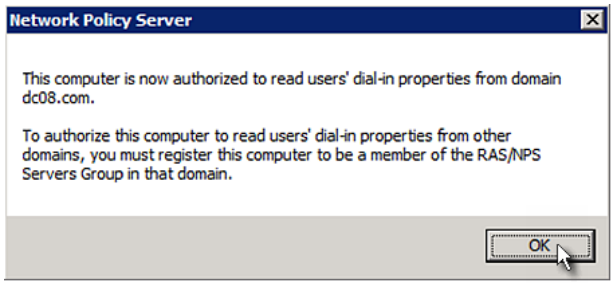
1. Open the NPS console.

2. Right-click NPS (Local) and select "Register server in Active Directory."



3. Click OK, and then OK again.

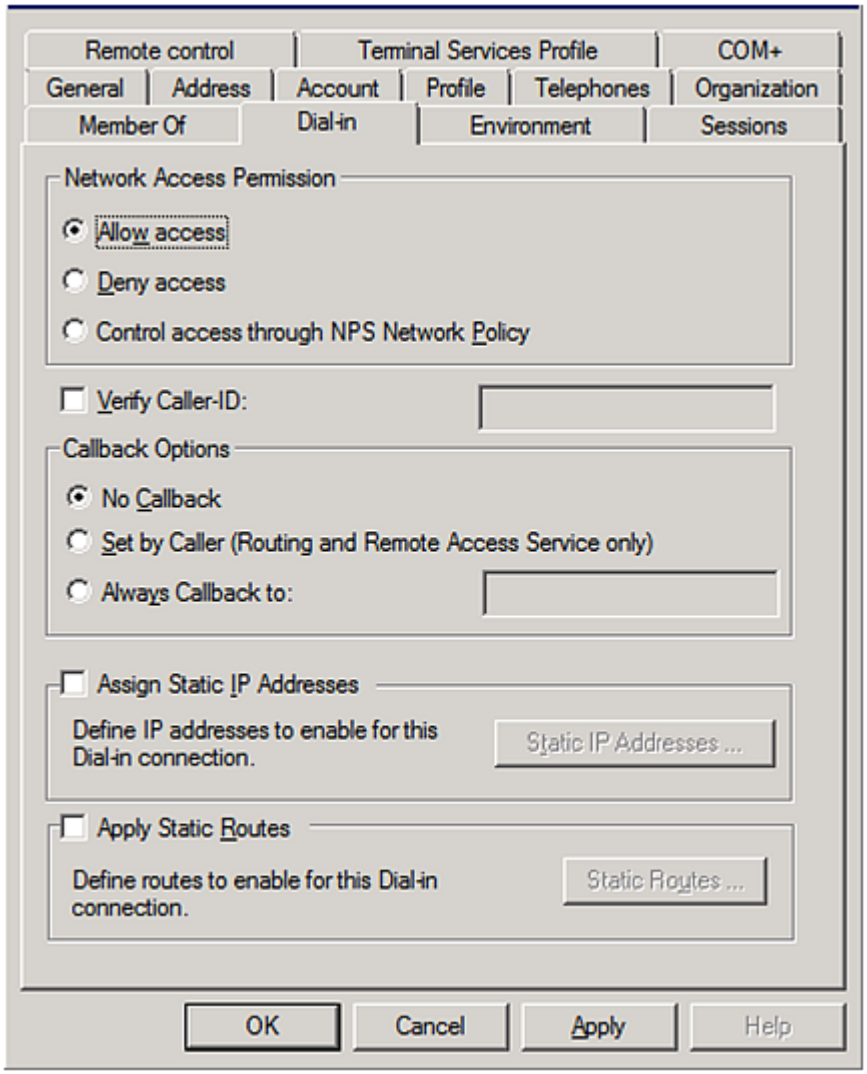




▶ To grant PXE users remote access permission:

1. Open Active Directory Users and Computers.

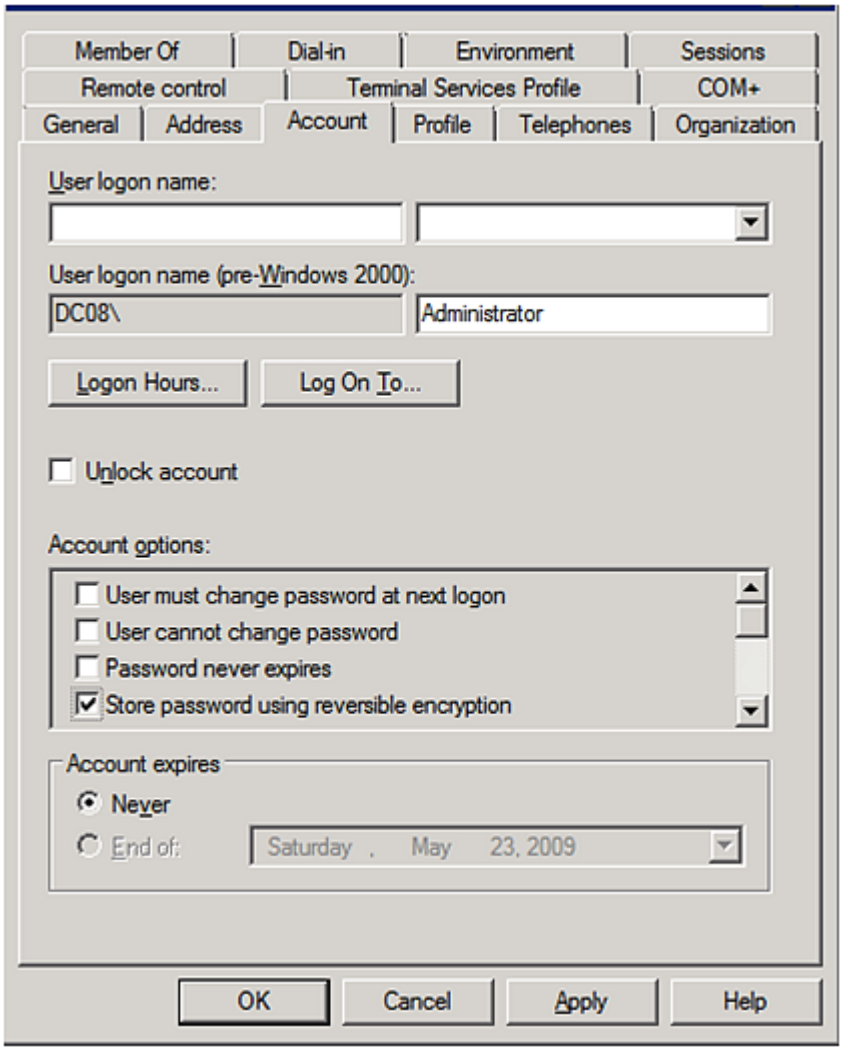
2. Open the properties dialog of the user whom you want to grant the access permission.
3. Click the Dial-in tab and select the "Allow access" checkbox.



To enable reversible encryption for CHAP authentication:

1. Open Active Directory Users and Computers.
2. Open the properties dialog of the user that you want to configure.

3. Click the Account tab and select the "Store password using reversible encryption" checkbox.



Appendix H Additional PXE Information

In This Chapter

Locking Outlets and Cords 440
MAC Address 442
Reserving IP Addresses in DHCP Servers 443
Sensor Threshold Settings 446
PDView App for Viewing the PXE 453
Altitude Correction Factors 455
Unbalanced Current Calculation 456
Ways to Probe Existing User Profiles 457
Raritan Training Website 458
Browsing through the Online Help 458

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:

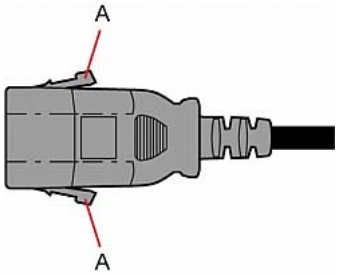
- SecureLock™ outlets and cords
- Button-type locking outlets

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.

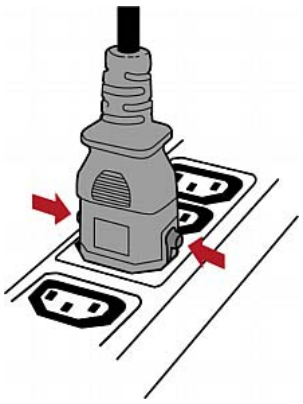
Tip: The SecureLock™ outlets can accept regular power cords for power distribution but the SecureLock™ mechanism does not take effect.

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.



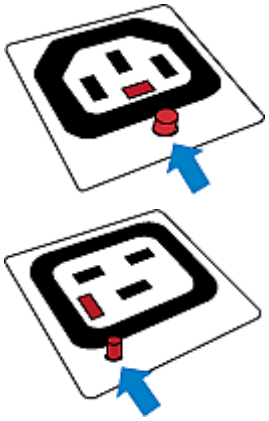
2. Unplug the cord now.

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.

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.

Reserving IP Addresses in 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 DHCP server, use the PXE device's serial number as the unique ID instead of the MAC address.

Interface	Client Identifier
ETHERNET	serial number
BRIDGE	serial number

You can reserve the IP addresses of more than one interfaces in the DHCP server if preferred. Note that you must choose/configure the bridge interface if your PXE is set to the bridging mode. This is because only the IP parameters of the BRIDGE interface functions in the bridging mode, and the IP parameters of the ETHERNET interface do NOT function.

Reserving IP in Windows

To reserve the IP address of any network interface in the Windows DHCP server, you must convert that interface's client identifier into *hexadecimal* ASCII codes.

For each interface's client identifier, see ***Reserving IP Addresses in DHCP Servers*** (on page 443).

In the following illustration, it is assumed that the PXE serial number is PEG1A00003.

▶ **Windows IP address reservation illustration:**

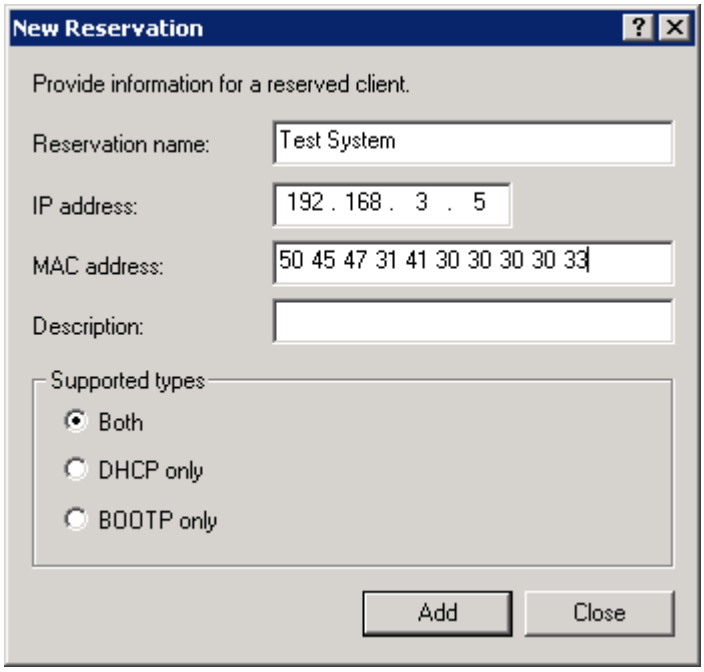
1. Convert the client identifier of the desired network interface into ASCII codes (*hexadecimal*).

Interface	Client identifier conversion
ETHERNET	PEG1A00003 = 50 45 47 31 41 30 30 30 30 33
BRIDGE	PEG1A00003 = 50 45 47 31 41 30 30 30 30 33

2. In your DHCP server, bring up the New Reservation dialog, and separate the converted ASCII codes with spaces.

   For example, to reserve the IP address of the ETHERNET interface, enter the following data in the dialog.

Field	Data entered
IP address	The IP address you want to reserve.
MAC address	The following ASCII codes. `50 45 47 31 41 30 30 30 30 33`
Other fields	Configure as needed.



Reserving IP in Linux

There are two methods to reserve the IP address of any network interface in the standard Linux DHCP server (ISC DHCP server):

- Convert an interface's client identifier into *hexadecimal* ASCII codes.
- Use an interface's original client identifier without converting it into ASCII codes.

For each interface's client identifier, see ***Reserving IP Addresses in DHCP Servers*** (on page 443).

In the following illustrations, it is assumed that the PXE serial number is PEG1A00003, and the IP address you want to reserve is 192.168.20.1.

Illustration with ASCII code conversion:

1. Convert the client identifier of the desired network interface into ASCII codes (*hexadecimal*).

Interface	Client identifier conversion
ETHERNET	PEG1A00003 = 50 45 47 31 41 30 30 30 30 33
BRIDGE	PEG1A00003 = 50 45 47 31 41 30 30 30 30 33

2. Separate the converted ASCII codes with a colon, and a prefix "00:" must be added to the beginning of the converted codes.

   For example, the *converted* client identifier of the ETHERNET interface looks like the following:

   `00:50:45:47:31:41:30:30:30:30:33`

3. Now enter the converted client identifier with the following syntax.

```
host mypx {
option dhcp-client-identifier = 00:50:45:47:31:41:30:30:30:30:33;
fixed-address 192.168.20.1;
}
```

Illustration without ASCII code conversion:

1. Use the original client identifier of the desired network interface. DO NOT convert them into ASCII codes.
2. A prefix "\000" must be added to the beginning of the client identifier.

   For example, the client identifier of the ETHERNET interface looks like the following:

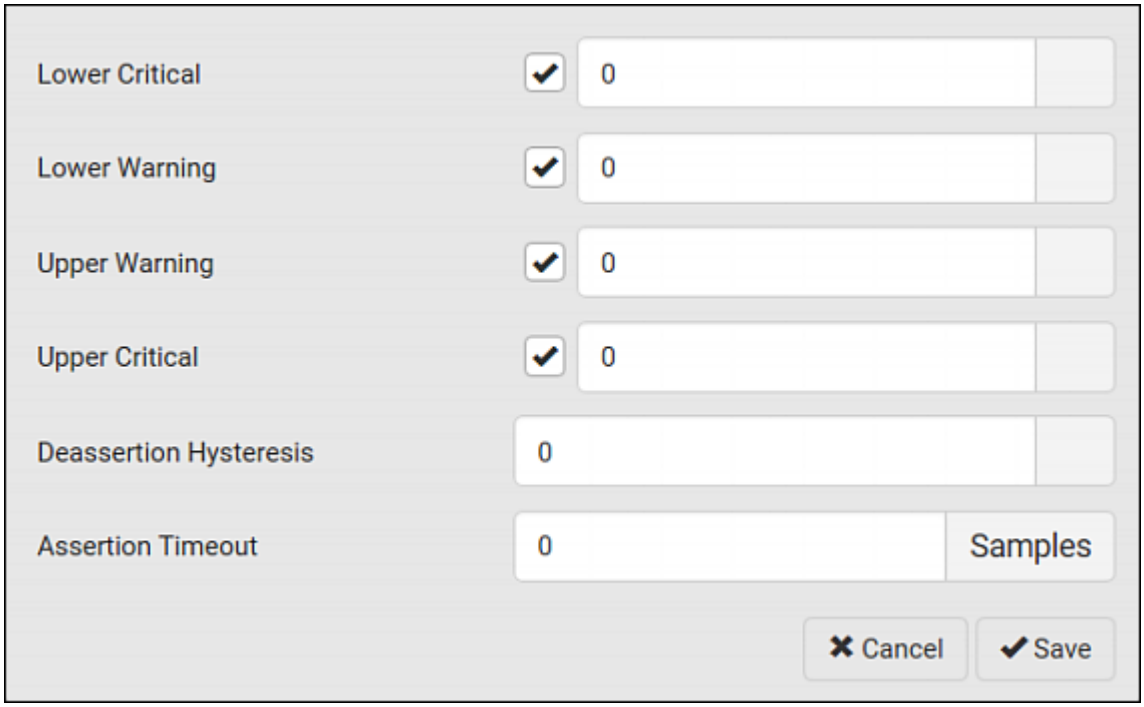
   `\000`PEG1A00003

3. Now enter the original client identifier with the following syntax. The client identifier is enclosed in quotation marks.

```
host mypx {
option dhcp-client-identifier = "\000PEG1A00003";
fixed-address 192.168.20.1;
}
```

Sensor Threshold Settings

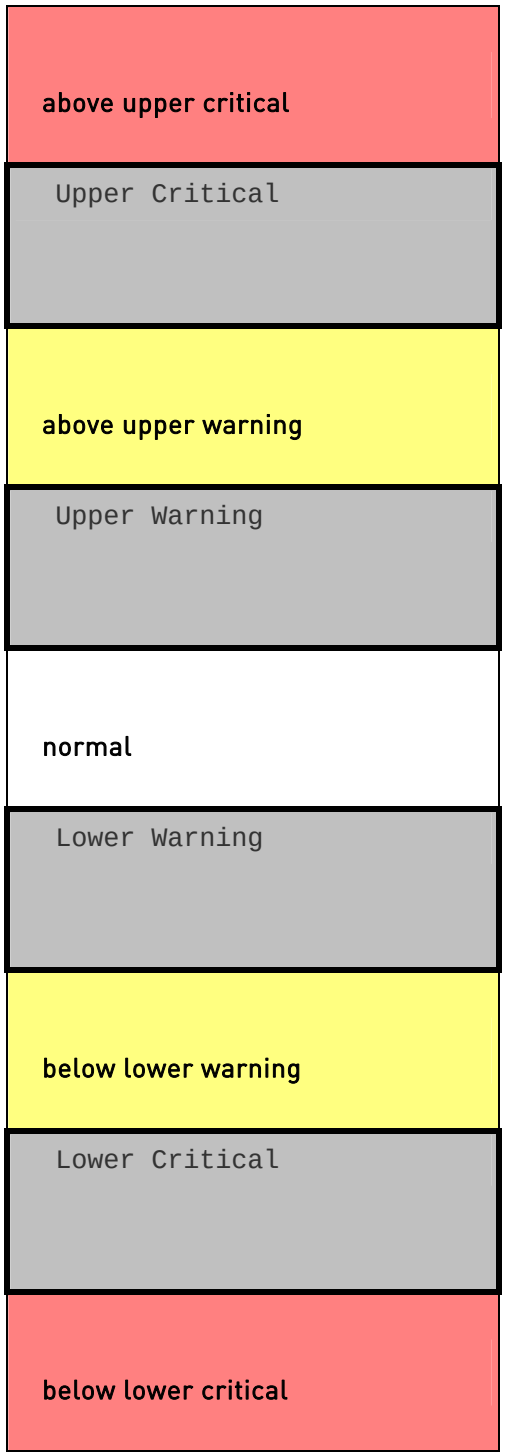
This section explains the thresholds settings for a numeric sensor.



Thresholds and Sensor States

A numeric sensor has four thresholds: Lower Critical, Lower Warning, Upper Warning and Upper Critical.

The threshold settings determine how many sensor states are available for a certain sensor and the range of each sensor state. The diagram below shows how each threshold relates to each state.



▶ Available sensor states:

The more thresholds are enabled for a sensor, the more sensor states are available for it. The "normal' state is always available regardless of whether any threshold is enabled.

For example:

- When a sensor only has the Upper Critical threshold enabled, it has two sensor states: normal and above upper critical.
- When a sensor has both the Upper Critical and Upper Warning thresholds enabled, it has three sensor states: normal, above upper warning, and above upper critical.

States of "above upper warning" and "below lower warning" are warning states to call for your attention.

States of "above upper critical" and "below lower critical" are critical states that require you to immediately handle.

Range of each available sensor state:

The value of each enabled threshold determines the reading range of each available sensor state. For details, see *Yellow- or Red-Highlighted Sensors* (on page 81).

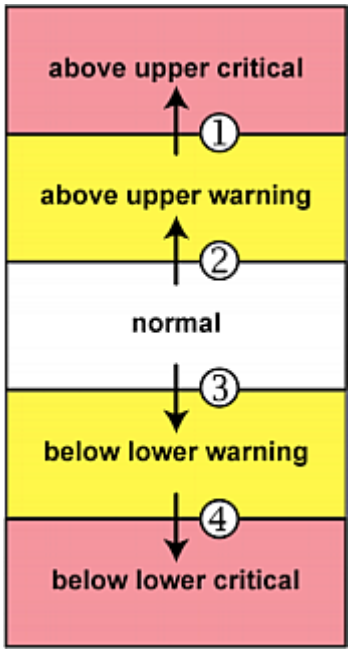
"To Assert" and Assertion Timeout

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:

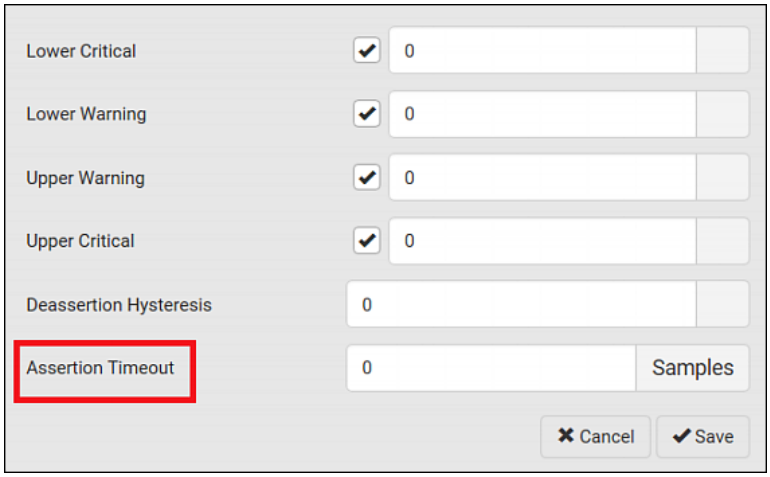
To assert a state is to announce a new, "worse" state.

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 settings, the Assertion Timeout field postpones or even cancels the "assertion" action. It determines how long a sensor must be in the "worse" new state before the PXE triggers 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. Sensors are measured every second, so the timing of a sample is equal to a second. BCM2 is an exception to this, with a sample of 3 seconds.

How "Assertion Timeout" is helpful:

If you have created an event rule that instructs the 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 readings fluctuate around a certain threshold.

Assertion Timeout Example for Temperature Sensors

Assumption:

```
Upper Warning threshold is enabled.
Upper Warning = 25 (degrees Celsius)
Assertion Timeout = 5 samples (that is, 5 seconds)
```

When a temperature sensor's reading exceeds 25 degrees Celsius, moving from the "normal" range to the "above upper warning" range, the 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 performs 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 perform the "assertion" action.

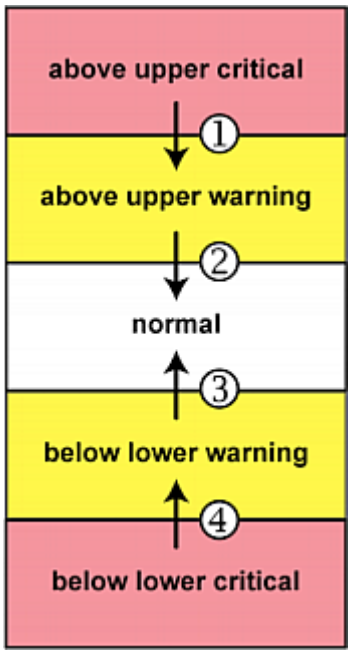
"To De-assert" and Deassertion Hysteresis

After the PXE asserts a worse state for a sensor, it may de-assert that state later on if the readings improve.

To de-assert a state:

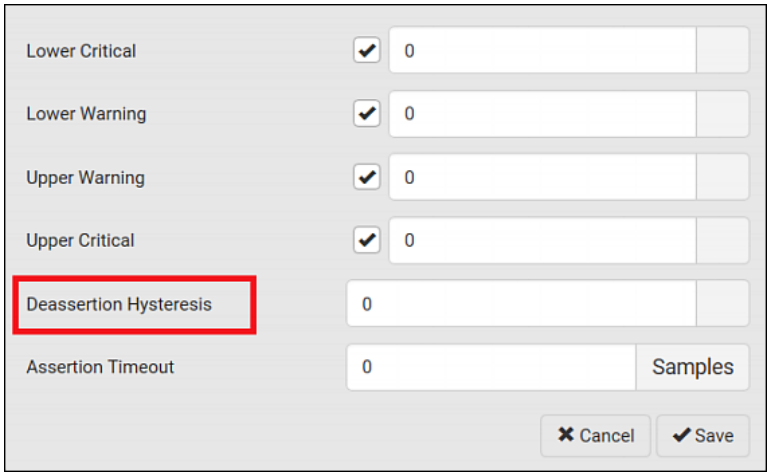
To de-assert a state is to announce the end of the previously-asserted worse state.

Below are good state changes that cause the 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, the Deassertion Hysteresis field determines a new level to trigger the "deassertion" action.

This function is similar to a thermostat, which instructs the air conditioner to turn on the cooling system when the temperature exceeds a pre-determined level. "Deassertion Hysteresis" instructs the PXE to de-assert the worse state for a sensor only when that sensor's reading reaches the pre-determined "deassertion" level.

For upper thresholds, this "deassertion" level is a decrease against each threshold. For lower thresholds, this level is an increase to each threshold. The absolute value of the decrease/increase is exactly the hysteresis value.

For example, if Deassertion Hysteresis = 2, then:

- 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 readings fluctuate around a certain threshold.

Deassertion Hysteresis Example for Temperature Sensors

Assumption:

```
Upper Warning threshold is enabled.
Upper Warning = 20 (degrees Celsius)
Deassertion Hysteresis = 3 (degrees Celsius)
"Deassertion"  level = 20-3 = 17 (degrees Celsius)
```

When the 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 perform the "deassertion" action.
- If the temperature drops to 17 degrees Celsius or lower, the PXE performs the "deassertion" action to announce the end of the "above upper warning" state.

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.

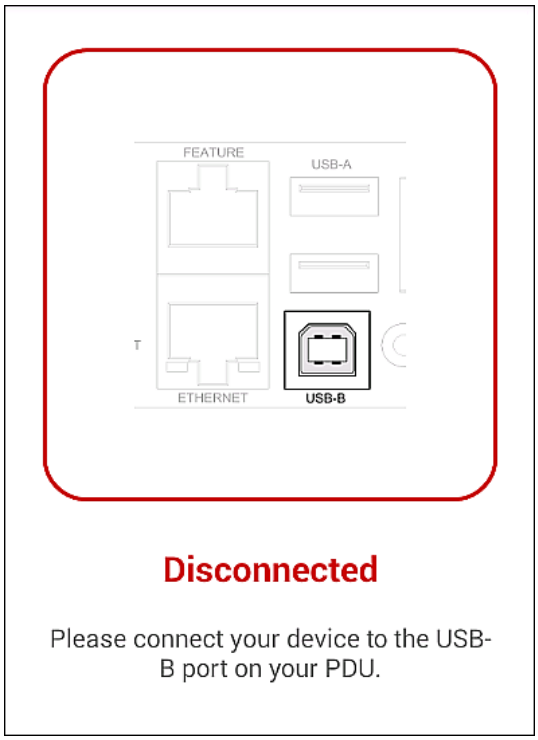
Requirements for using PDView:

- 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:

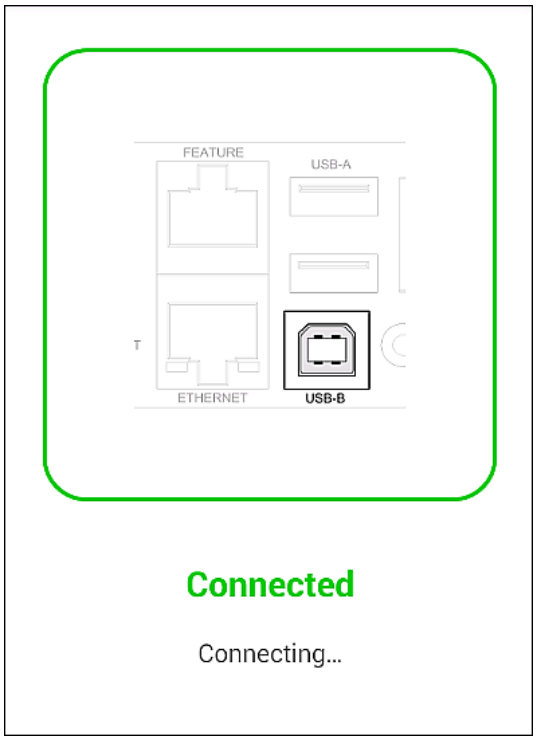
1. Use your mobile device to download the PDView app from the Google Play.

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

Altitude (meters)	Altitude (feet)	Correction factor
425	1394	1.00
500	1640	1.01
740	2428	1.04
1500	4921	1.15
2250	7382	1.26
3000	9842	1.38

Unbalanced Current Calculation

Unbalanced current information is available on 3-phase models only. This section explains how the PXE calculates the unbalanced current percentage.

Calculation:

1. Calculate the average current of all 3 lines.

   `Average current = (L1+L2+L3) / 3`

2. Calculate each line's current unbalance by having each line current subtracted and divided with the average current.

   `L1 current unbalance = (L1 - average current) / average current`

   `L2 current unbalance = (L2 - average current) / average current`

   `L3 current unbalance = (L3 - average current) / average current`

3. Determine the maximum absolute value among three lines' current unbalance values.

   `Maximum (|L1 current unbalance|, |L2 current unbalance|, |L3 current unbalance|)`

4. Convert the maximum value to a percentage.

   `Unbalanced load percent = 100 * maximum current unbalance`

Example:

- Each line's current:

  L1 = 5.5 amps

L2 = 5.2 amps
L3 = 4.0 amps

- Average current: (5.5+5.2+4.0) / 3 = 4.9 amps

- L1 current unbalance: (5.5 - 4.9) / 4.9 = 0.1224
- L2 current unbalance: (5.2 - 4.9) / 4.9 = 0.0612
- L3 current unbalance: (4.0 - 4.9) / 4.9 = -0.1837

- Maximum current unbalance:
  Maximum (|0.1224|, |0.0612|, |-0.1837|) = 0.1837

- Current unbalance converted to a percentage:
  100 * (0.1837) = 18%

Ways to Probe Existing User Profiles

This section indicates available ways to query existing user accounts on the 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.

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.

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 Scriplets. Consult your browser help for information on enabling these features.

To use the PXE online help:

1. Click Online Documentation. See *Web Interface Overview* (on page 51).
2. The online help opens in the default web browser.
3. To view the content of any topic, click the topic in the left pane. Then its content is displayed in the right pane.
4. To select a different topic, do any of the following:
   - To view the next topic, click the Next icon in the toolbar.
   - To view the previous topic, click the Previous icon .
   - To view the first topic, click the Home icon .
5. To expand or collapse a topic that contains sub-topics, do the following:
   - To expand any topic, click the white arrow prior to the topic, or double-click that topic. The arrow turns into a black, gradient arrow , and sub-topics appear below the topic.

- To collapse any expanded topic, click the black, gradient arrow ◢ prior to the topic, or double-click the expanded topic. The arrow then turns into a white arrow ▷, and all sub-topics below that topic disappear.

6. To search for specific information, type the key word(s) or string(s) in the Search text box, and press Enter or click the Search icon to start the search.
   - If necessary, select the "Match partial words" checkbox to include information matching part of the words entered in the Search text box.

   The search results are displayed in the left pane.
7. To have the left pane show the list of topics, click the Contents tab at the bottom.
8. To show the Index page, click the Index tab.
9. To email any URL link to the currently selected topic to any person, click the "Email this page" icon in the toolbar.
10. To email your comments or suggestions regarding the online help to Raritan, click the "Send feedback" icon .
11. To print the currently selected topic, click the "Print this page" icon .

Appendix I Integration

The PXE device can work with certain Sunbird's products to provide diverse power solutions.

In This Chapter

Power IQ Configuration 460
dcTrack 460

Power IQ Configuration

Sunbird's Power IQ is a software application that collects and manages the data from different PDUs installed in your server room or data center. With this software, you can:

- Do bulk configuration for multiple PDUs
- Name outlets on different PDUs
- Switch on/off outlets on outlet-switching capable PDUs

For more information on Power IQ, refer to the Power IQ online help on the Sunbird website: *http://support.sunbirddcim.com.*

dcTrack

Sunbird's dcTrack® is a product that allows you to manage the data center. The 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.sunbirddcim.com*.

dcTrack Overview

dcTrack® is a powerful and intelligent data center management and automation application.

It has been designed by data center and IT professionals to provide broad and deep visibility into the data center. It empowers data center managers to plan for growth and change by optimizing their current operations, assets, and infrastructure.

With dcTrack, you can view everything in the data center from servers, blades, virtual servers and applications to data networks, IP addressing space and cabling. dcTrack also allows you to track real-time power consumption and manage raised floor space and rack elevations.

Use dcTrack to build your floor map data center map directly in the application, or import an existing floor map into the dcTrack. Further, dcTrack allows you to import AutoCAD® 2012 (and earlier) objects to build a data center map.

If you currently maintain data center information in spreadsheet format, that data can be imported into dcTrack using the Import wizard.

Isolate potential problems with end-to-end power and data circuits by visually tracing them. This allows you to identify all intermediate circuit points and locate problems.

By using dcTrack's workflow and change management feature, data center managers are better able to enforce best practices across the enterprise and meet ITIL framework guidelines. You can also opt to skip the Change Control workflow process and work in Request Bypass so requests are processed immediately.

dcTrack® can be used as a standalone product or integrated with Power IQ® for power and environmental monitoring.

Index

1

1U Products • 1

A

A Note about Enabling Thresholds • 214
A Note about Firmware Upgrade Time • 198
A Note about Infinite Loop • 179
A Note about Untriggered Rules • 179
About the Interface • 215
Action Group • 159, 162
Actuator Configuration Commands • 313, 314, 327
Actuator Control Operations • 335
Actuator Information • 230
Adding a Firewall Rule • 276
Adding a Monitored Device • 328
Adding a Role-Based Access Control Rule • 288
Adding Attributes to the Class • 399
Adding LDAP/LDAPS Servers • 132, 134, 139
Adding Radius Servers • 132, 137, 139, 404
Additional PXE Information • 440
AD-Related Configuration • 405, 423, 436
Alarm • 159, 160
All Privileges • 303, 309, 312
Altitude Correction Factors • 66, 248, 455
APIPA and Link-Local Addressing • 2, 12, 49, 120
Assertion Timeout Example for Temperature Sensors • 450
Automatic Mode • 43
Automatically Completing a Command • 342
Available Actions • 116, 146, 158, 162, 164, 170, 176, 208
Available Data of the Outlets Overview Page • 70, 71

B

Backup and Restore of Device Settings • 193, 199, 202, 360
Backup and Restore via SCP • 203, 346
Before You Begin • 3
Browsing through the Online Help • 53, 458
Built-in Rules and Rule Configuration • 146, 147, 176
Bulk Configuration • 18, 193, 199, 202, 345, 360
Bulk Configuration Methods • 13, 18
Bulk Configuration or Firmware Upgrade via DHCP/TFTP • 18, 198, 200, 355
Bulk Configuration Restrictions • 199, 201
Bulk Configuration via SCP • 200, 345
Bulk Configuration/Upgrade Procedure • 355, 366, 367
Button-Type Locking Outlets • 442

C

Calendar • 144, 145
Changing a User's Password • 296
Changing HTTP(S) Settings • 103, 114, 121
Changing Measurement Units • 303, 306
Changing Modbus Settings • 103, 114, 119
Changing SSH Settings • 95, 103, 114, 118
Changing Telnet Settings • 103, 114, 119, 215
Changing the Inlet Name • 294
Changing the LAN Duplex Mode • xiv, 261
Changing the LAN Interface Speed • xiv, 260
Changing the Modbus Configuration • 267
Changing the Modbus Port • 268
Changing the Outlet Name • 293
Changing the Overcurrent Protector Name • 295
Changing the PDU Name • 247
Changing the Role(s) • 303
Changing the Sensor Description • 316
Changing the Sensor Name • 314
Changing the SSH Configuration • 264
Changing the SSH Port • 264
Changing the Telnet Configuration • 263
Changing the Telnet Port • 264
Changing the UDP Port • 333
Changing Your Own Password • 305
Changing Your Password • 50, 94, 95
Checking Lua Scripts States • 189, 190, 191

Checking the Accessibility of NTP Servers • 273
Checking the Branch Circuit Rating • 4
Circuit Breaker Orientation Limitation • 5, 7, 9
Circuit Breakers • 45
Clearing Event Log • 245
Clearing Information • 245
Closing a Local Connection • 218
Command History • 242
Commands for Environmental Sensors • 324
Commands for Inlet Pole Sensors • 322
Commands for Inlet Sensors • 320
Common Network Settings • 104, 107
config.txt • 356, 359, 362
Configuration Files • 355, 356
Configuring Data Push Settings • 104, 162, 181
Configuring DNS Parameters • xiv, 259
Configuring Environmental Sensors' Default Thresholds • 318
Configuring IPv4 Parameters • xiv, 250
Configuring IPv6 Parameters • 254
Configuring Login Settings • 104, 121, 140
Configuring Network Services • 114, 217
Configuring Network Settings • 2, 15, 103, 104
Configuring NTP Server Settings • 213
Configuring Password Policy • 104, 121, 142
Configuring Security Settings • 121
Configuring SMTP Settings • 103, 114, 116, 163
Configuring SNMP Settings • 95, 103, 114, 115, 158, 207
Configuring the PXE • 12
Configuring the PXE Device and Network • 246
Connecting a DPX2 Sensor Package to DPX3 • 30, 39
Connecting a DPX2 Sensor Package to DX • 29, 32, 33, 39
Connecting Environmental Sensor Packages • 20, 76
Connecting the PDU to a Power Source • 11
Connecting the PXE to a Computer • 2, 12, 14, 389
Connecting the PXE to Your Network • 11, 12, 104
Connection Ports • 41
Creating a CSR • 126, 127, 128
Creating a New Attribute • 398
Creating a Role • 309
Creating a Self-Signed Certificate • 126, 129
Creating a User Profile • 296
Creating Configuration Files via Mass Deployment Utility • 357, 365, 366
Creating IP Access Control Rules • 104, 121, 123
Creating Role Access Control Rules • 104, 121, 124, 125
Creating Roles • 50, 94, 98, 99, 404
Creating Users • 48, 50, 94, 99, 100, 102, 103, 118, 132, 207
Customizing the Date and Time • 272

D

Dashboard • 53, 56, 160
Dashboard - Alarms • 57, 63, 159
Dashboard - Alerted Sensors • 57, 60
Dashboard - Inlet History • 57, 62, 68
Dashboard - Inlet I1 • 57, 58, 68
Data Encryption in 'config.txt' • 362, 366
Date and Time Settings • 228
dcTrack • 460
dcTrack Overview • 461
Deassertion Hysteresis Example for Temperature Sensors • 452
Default Log Messages • 143, 147, 152, 162, 163
Default Measurement Units • 228
Deleting a Firewall Rule • 279
Deleting a Monitored Device • 329
Deleting a Role • 313
Deleting a Role-Based Access Control Rule • 291
Deleting a User Profile • 305
Deleting an NTP Server • xiv, 271
Detailed Information on Outlet Pages • 71, 72
Determining the SSH Authentication Method • 265
Determining the Time Setup Method • 269, 272
Device Information • 193, 194
Device Settings • 54, 103
devices.csv • 357, 359, 363, 364

Device-Specific Settings NOT Included • 199, 201
DHCP IPv4 Configuration in Linux • 356, 385
DHCP IPv4 Configuration in Windows • 356, 368
DHCP IPv6 Configuration in Linux • 356, 387
DHCP IPv6 Configuration in Windows • 356, 378
Diagnostic Commands • 340
Different CLI Modes and Prompts • 217, 218, 220, 245, 246, 247, 273, 335, 340
Downloading Diagnostic Data via SCP • xiv, 347
Downloading Diagnostic Information • 193, 204
Downloading SNMP MIB • 116, 207, 210
DPX Sensor Packages • 20, 21
DPX2 Sensor Packages • 20, 27
DPX3 Sensor Packages • 20, 29
DX Sensor Packages • 20, 31, 168

E

Editing or Deleting a Rule/Action • 158, 176, 187
Editing or Deleting IP Access Control Rules • 123
Editing or Deleting Ping Monitoring Settings • 185
Editing or Deleting Role Access Control Rules • 125
Editing or Deleting Roles • 101
Editing or Deleting Users • 50, 98, 100, 102
Editing rciusergroup Attributes for User Members • 401
Email and SMS Message Placeholders • 163, 165, 173
Enabling and Configuring SNMP • 177, 180, 207
Enabling or Disabling a User Profile • 299
Enabling or Disabling an Inlet (for Multi-Inlet PDUs) • 294
Enabling or Disabling Data Logging • 247
Enabling or Disabling EnergyWise • 332
Enabling or Disabling Modbus • 267
Enabling or Disabling Peripheral Device Auto Management • 249
Enabling or Disabling Service Advertising • 268
Enabling or Disabling SNMP v1/v2c • 265
Enabling or Disabling SNMP v3 • 266
Enabling or Disabling SSH • 264
Enabling or Disabling Strong Passwords • 284
Enabling or Disabling Telnet • 263
Enabling or Disabling the LAN Interface • xiv, 260
Enabling or Disabling the Read-Only Mode • 268
Enabling or Disabling the Restricted Service Agreement • 280
Enabling Service Advertising • 103, 114, 120, 268
Enabling the Restricted Service Agreement • 49, 104, 121, 143
EnergyWise Configuration Commands • 332
EnergyWise Settings • 239
Entering Configuration Mode • 218, 246, 297, 305
Entering Diagnostic Mode • 218, 339
Environmental Sensor Configuration Commands • 313
Environmental Sensor Default Thresholds • 236
Environmental Sensor Information • 229
Environmental Sensor Package Information • 231
Environmental Sensor Threshold Information • 235
Equipment Setup Worksheet • 4, 351
Ethernet Interface Settings • 105, 108
Event Log • 240
Event Rules and Actions • 63, 68, 89, 104, 115, 116, 146, 160, 181, 183, 189
Example • 271, 281, 297, 305
  Ping Monitoring and SNMP Notifications • 183, 185
Example - Actuator Naming • 328
Example - Creating a Role • 313
Example - Default Upper Thresholds for Temperature • 320
Example - Inlet Naming • 295
Example - OCP Naming • 295
Example - Outlet Naming • 293

Example - Ping Command • 342
Example - Server Settings Changed • 331
Example - Setting Up EnergyWise • 334
Example - Turning On a Specific Actuator • 337
Example 1 • 179
Example 1 - Basic Security Information • 243
Example 1 - Combination of IP, Subnet Mask and Gateway Parameters • 334
Example 1 - Creating a User Profile • 308
Example 1 - Environmental Sensor Naming • 318
Example 1 - IPv4 Firewall Control Configuration • 291
Example 1 - Networking Mode • 269
Example 1 - PDU Naming • 250
Example 1 - Time Setup Method • 273
Example 1 - Upper Critical Threshold for a Temperature Sensor • 326
Example 2 • 179
Example 2 - Adding an IPv4 Firewall Rule • 292
Example 2 - Combination of Upper Critical and Upper Warning Settings • 335
Example 2 - Data Logging Enabled • 250
Example 2 - Enabling Both IP Protocols • 269
Example 2 - In-Depth Security Information • 244
Example 2 - Modifying a User's Roles • 308
Example 2 - Primary NTP Server • 273
Example 2 - Sensor Threshold Selection • 318
Example 2 - Warning Thresholds for Inlet Sensors • 326
Example 3 - Basic PDU Information • 244
Example 3 - Default Measurement Units • 308
Example 3 - Static IPv4 Configuration • 269
Example 3 - User Blocking • 292
Example 4 - Adding an IPv4 Role-based Access Control Rule • 292
Example 4 - In-Depth PDU Information • 245
Examples • 243, 250, 269, 273, 291, 307, 317, 326
Existing Roles • 239
Existing User Profiles • 228, 238

F

Filling Out the Equipment Setup Worksheet • 4
Finding the Sensor's Serial Number • 78, 85
Firewall Control • 274
Firmware Update via SCP • 198, 344
Forcing a Password Change • 299
FreeRADIUS Standard Attribute Illustration • 404, 422
FreeRADIUS VSA Illustration • 423, 435
From LDAP/LDAPS • 397
From Microsoft Active Directory • 397
Full Disaster Recovery • 198
fwupdate.cfg • 356, 358, 362, 364

G

Gathering LDAP/Radius Information • 132, 133

H

Help Command • 219
History Buffer Length • 242
How the Automatic Management Function Works • 66, 67, 249

I

Identifying the Sensor Position and Channel • 78, 86
Idle Timeout • 283
Individual OCP Pages • 74
Individual Outlet Pages • 70, 71
Individual Sensor/Actuator Pages • 60, 65, 67, 77, 79, 80, 89, 93
Initial Installation and Configuration • 11
Initial Network Configuration via CLI • xiv, 2, 12, 15, 389
Inlet • 54, 58, 59, 66, 68
Inlet Configuration Commands • 293
Inlet Information • 226
Inlet Pole Sensor Threshold Information • 233
Inlet Sensor Threshold Information • 232
Installing a CA-Signed Certificate • 126, 128
Installing Cable Retention Clips on Outlets (Optional) • 18

Installing or Downloading Existing Certificate and Key • 126, 130
Installing the USB-to-Serial Driver (Optional) • 13, 14
Integration • 460
Interface Names • 110, 113
Internal Beeper State • 66
Introduction • 1
IP Configuration • xiv, 221, 222
IPv4-Only or IPv6-Only Configuration • xiv, 221, 222

L

Layout • 212
LDAP Configuration Illustration • 132, 391
LED Display • 42
LEDs for Measurement Units • 43, 44
Locking Outlets and Cords • 19, 440
Log an Event Message • 159, 162
Logging in to CLI • 216, 366, 389
Logging out of CLI • 218
Login • 12, 13, 15, 49
Login Limitation • 281
Login, Logout and Password Change • 48
Logout • 51
Lowercase Character Requirement • 285
Lua Scripts • 104, 167, 187

M

MAC Address • 12, 442
Maintenance • 54, 193
Managed vs Unmanaged Sensors/Actuators • 76, 81, 82
Managing External Authentication Settings • 132, 136, 138, 139
Managing Firewall Rules • 275
Managing One Sensor or Actuator • 78, 79, 87
Managing Role-Based Access Control Rules • 288
Manual Mode • 44
Manually Starting or Stopping a Script • 188, 189
Maximum Ambient Operating Temperature • 3, 349
Maximum Password History • 286
Maximum Password Length • 284
Menu • 52, 53, 65, 68, 70, 73, 76, 94, 103, 189, 193
Minimum Password Length • 284
Miscellaneous • 104, 192, 194, 211
Mixing Diverse Sensor Types • 34, 36
Modifying a Firewall Rule • 277
Modifying a Monitored Device's Settings • 329
Modifying a Role • 311
Modifying a Role-Based Access Control Rule • 289
Modifying a User Profile • 296
Modifying a User's Personal Data • 298
Modifying Firewall Control Parameters • 274
Modifying or Deleting a Script • 187, 191
Modifying Role-Based Access Control Parameters • 287
Modifying SNMPv3 Settings • 300
Monitoring Server Accessibility • 104, 183, 185
Mounting 1U Models Using L-Brackets and Buttons • 6
Mounting Zero U Models Using L-Brackets and Buttons • 9
Mounting Zero U Models Using Two Rear Buttons • 7
Multi-Command Syntax • 275, 281, 283, 284, 288, 296, 298, 300, 303, 306, 318, 320, 322, 324, 327, 329, 334

N

Network Configuration • xiv, 221
Network Configuration Commands • 250
Network Diagnostics • 193, 203
Network Interface Settings • xiv, 223
Network Service Settings • 224
Network Troubleshooting • 203, 339
NPS Standard Attribute Illustration • 404
NPS VSA Illustration • 423
Numeric Character Requirement • 285

O

OCPs • 54, 73, 74
Outlet Configuration Commands • 293
Outlet Information • 225
Outlets • 40, 54, 70, 71

Overcurrent Protector Configuration Commands • 295
Overcurrent Protector Information • 227
Overriding DHCP-Assigned NTP Servers • 270, 273

P

Package Contents • 1, 3
Panel Components • 40
Password Aging • 282
Password Aging Interval • 282
PDU • 52, 54, 65, 67, 69, 76, 91, 93
PDU Configuration • 225
PDU Configuration Commands • 247
PDView App for Viewing the PXE • 453
Peripherals • 31, 54, 67, 76, 82, 84, 87, 89, 90, 178
Power Cord • 40
Power IQ Configuration • 460
Preparing the Installation Site • 3
Product Models • 1
Push Out Sensor Readings • 159, 162

Q

Querying Available Parameters for a Command • 219, 220
Querying DNS Servers • 340
Quick Access to a Specific Page • 49, 55
Quitting Configuration Mode • 246, 281
Quitting Diagnostic Mode • 339

R

Rackmount Safety Guidelines • 5
Rack-Mounting the PDU • 5
RADIUS Configuration Illustration • 132, 404
Raritan Training Website • 458
Rebooting the PXE Device • 193, 205
Reliability Data • 242
Reliability Error Log • 243
Remembering User Names and Passwords • 50
Reserving IP Addresses in DHCP Servers • xiv, 443, 444
Reserving IP in Linux • xiv, 444
Reserving IP in Windows • xiv, 443
Reset Button • 45
Resetting Active Energy Readings • 338
Resetting All Settings to Factory Defaults • 193, 205
Resetting the Button-Type Circuit Breaker • 45
Resetting the Handle-Type Circuit Breaker • 46
Resetting the PXE • 337
Resetting to Factory Defaults • 206, 339, 389
Restarting the PDU • 338
Restricted Service Agreement • 280
Retrieving Previous Commands • 342
Retrieving Software Packages Information • 193, 206
Returning User Group Information • 397
Role Configuration Commands • 309
Role-Based Access Control • 286
RS-485 Port Pinouts • 349

S

Safety Guidelines • ii
Safety Instructions • iii, 3
Sample Event Rules • 149, 177
Sample Inlet-Level Event Rule • 177
Sample PDU-Level Event Rule • 177
Sample Sensor-Level Event Rule • 178
Scheduling an Action • 147, 162, 170, 172
SecureLock™ Outlets and Cords • 440
Security Configuration Commands • 274
Security Settings • 237
Send an SNMP Notification • 116, 160, 165
Send Email • 152, 159, 163, 172, 173
Send Sensor Report • 103, 160, 164, 172
Send Sensor Report Example • 164, 172
Sensor RJ-12 Port Pinouts • 349
Sensor Threshold Configuration Commands • 320
Sensor Threshold Settings • 69, 80, 81, 90, 213, 446
Sensor/Actuator Location Example • 67, 91, 93
Sensor/Actuator States • 61, 77, 78, 83
Server Reachability Configuration Commands • 328
Server Reachability Information • 241

Server Reachability Information for a Specific Server • 241
Setting Data Logging • 104, 180, 182, 247, 248
Setting Data Logging Measurements Per Entry • 248
Setting Default Measurement Units • 66, 94, 102, 303, 306
Setting IPv4 Static Routes • xiv, 253
Setting IPv6 Static Routes • xiv, 257
Setting LAN Interface Parameters • xiv, 259
Setting Network Service Parameters • 261
Setting NTP Parameters • 270, 273
Setting the Alarmed to Normal Delay for DX-PIR • 317
Setting the Automatic Daylight Savings Time • 272
Setting the Date and Time • 104, 143, 213
Setting the History Buffer Length • 334
Setting the HTTP Port • 262
Setting the HTTPS Port • 263
Setting the IPv4 Address • xiv, 252
Setting the IPv4 Configuration Mode • xiv, 250
Setting the IPv4 Gateway • xiv, 253
Setting the IPv4 Preferred Host Name • xiv, 251
Setting the IPv6 Address • xiv, 256
Setting the IPv6 Configuration Mode • xiv, 254
Setting the IPv6 Gateway • xiv, 257
Setting the IPv6 Preferred Host Name • xiv, 255
Setting the Polling Interval • 333
Setting the Registry to Permit Write Operations to the Schema • 398
Setting the SNMP Configuration • 265
Setting the SNMP Read Community • 266
Setting the SNMP Write Community • 266
Setting the sysContact Value • 266
Setting the sysLocation Value • 267
Setting the sysName Value • 267
Setting the Time Zone • 213, 271
Setting the X Coordinate • 315
Setting the Y Coordinate • 315
Setting the Z Coordinate • 249, 316
Setting the Z Coordinate Format for Environmental Sensors • 249, 316, 328
Setting Up an SSL/TLS Certificate • 104, 121, 126
Setting Up External Authentication • 104, 121, 131
Setting Your Preferred Measurement Units • 66, 94, 98, 102
Showing Information • 220
Showing Network Connections • 340
Single Login Limitation • 282
SNMP Gets and Sets • 211
SNMP Sets and Thresholds • 213
SNMPv2c Notifications • 116, 208
SNMPv3 Notifications • 116, 208, 209
Sorting a List • 55, 60, 70, 73, 77, 98, 101, 173, 195, 196, 199
Special Character Requirement • 286
Specifications • 5, 349
Specifying the Agreement Contents • 280
Specifying the CC Sensor Type • 314
Specifying the Device Altitude • 248
Specifying the EnergyWise Domain • 332
Specifying the EnergyWise Secret • 333
Specifying the Primary NTP Server • 270
Specifying the Secondary NTP Server • 270
Specifying the SSH Public Key • 265, 304
Standard Attributes • 404
Start or Stop a Lua Script • 160, 167, 188, 189
Static Route Examples • 105, 108, 110, 253, 257
Step A
  Add Your PXE as a RADIUS Client • 404, 405, 423, 424
Step A. Determine User Accounts and Roles • 391
Step B
  Configure Connection Policies and Standard Attributes • 405, 409
  Configure Connection Policies and Vendor-Specific Attributes • 423, 428
Step B. Configure User Groups on the AD Server • 392
Step C. Configure LDAP Authentication on the PXE Device • xiv, 393
Step D. Configure Roles on the PXE Device • 394
Strong Passwords • 284

Supported Maximum DPX Sensor Distances • 21, 26
Supported Web Browsers • 48
Switch Peripheral Actuator • 160, 168
Switching Off an Actuator • 336
Switching On an Actuator • 336
Syslog Message • 160, 169

T

Testing the Network Connectivity • 341
TFTP Requirements • 356, 367
The PXE MIB • 211
Three-Digit Row • 42, 197
Thresholds and Sensor States • 446
Time Configuration Commands • 269
Time Units • 140, 141, 142
Tracing the Route • 342
Two-Digit Row • 43

U

Unbalanced Current Calculation • 456
Unblocking a User • 141, 337
Unpacking the Product and Components • 3
Updating the LDAP Schema • 397
Updating the PXE Firmware • 193, 197, 344
Updating the Schema Cache • 401
Uppercase Character Requirement • 285
User Blocking • 283
User Configuration Commands • 295
User Interfaces Showing Default Units • 102, 103
User Management • 54, 94
Using an Optional DPX3-ENVHUB4 Sensor Hub • 22, 34
Using an Optional DPX-ENVHUB2 cable • 24
Using an Optional DPX-ENVHUB4 Sensor Hub • 22
Using Default Thresholds • 317
Using SCP Commands • 344
Using SNMP • 198, 207
Using the CLI Command • 339, 389
Using the Command Line Interface • 114, 215, 389
Using the PDU • 40
Using the Web Interface • xiv, 48

V

Vendor-Specific Attributes • 404, 423
Viewing Connected Users • 193, 195
Viewing Firmware Update History • 193, 199
Viewing or Clearing the Local Event Log • 116, 132, 169, 193, 196

W

Ways to Probe Existing User Profiles • 457
Web Interface Overview • 51, 458
What's New in the PXE User Guide • xiv
Windows NTP Server Synchronization Solution • 144, 145
Wired Network Settings • 105, 106, 120, 393
With HyperTerminal • 216, 337
With SSH or Telnet • 217
Writing or Loading a Lua Script • 187, 191

Y

Yellow- or Red-Highlighted Sensors • 68, 77, 81, 83, 89, 448

Z

Z Coordinate Format • 65, 67
Zero U Products • 1