



Dominion PX

User Guide
Release 1.5.5

Copyright © 2014 Raritan, Inc.

DPX-0S-v1.5.5-E

February 2014

255-80-6080-00

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 2014 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、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラス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。

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.



Contents

Safety Guidelines	ii
<hr/>	
Safety Instructions	iii
<hr/>	
Applicable Models	xiii
<hr/>	
What's New in the Dominion PX User Guide	xiv
<hr/>	
Chapter 1 Introduction	1
<hr/>	
Product Models	1
Product Photos	1
Zero U Size	2
1U Size	2
2U Size	2
Product Features	3
Package Contents.....	5
Zero U Products.....	5
1U Products	5
2U Products	5
<hr/>	
Chapter 2 Rack-Mounting the PDU	6
<hr/>	
Rackmount Safety Guidelines	6
Circuit Breaker Orientation Limitation	6
Standard Rackmount	7
Mounting Zero U Models Using L-Brackets	8
For Zero U Models Using Tool-less Button Mounting.....	9
Before You Begin Tool-less Mounting:	9
Mounting Zero U Models Using Button Mount	10

Contents

Mounting Zero U Models Using Claw-Foot Brackets.....	12
Mounting 1U or 2U Models	13

Chapter 3 Installation and Configuration 15

Before You Begin.....	15
Unpacking the Product and Components.....	15
Preparing the Installation Site.....	15
Filling Out the Equipment Setup Worksheet	16
Connecting the Dominion PX to a Power Source.....	16
Configuring the Dominion PX	17
Connecting the Dominion PX to a Computer	17
Connecting the Dominion PX to Your Network	18
Initial Network and Time Configuration	19
Connecting Environmental Sensors (Optional)	25
About Contact Closure Sensors	27
How to Connect Differential Air Pressure Sensors.....	30

Chapter 4 Using the PDU 31

Panel Components	31
Blue LED.....	31
Power Cord.....	31
Outlets	32
Connection Ports	32
LED Display	33
Reset Button.....	36
Circuit Breaker	36
Resetting the Button-Type Circuit Breaker.....	37
Resetting the Handle-Type Circuit Breaker.....	37
Beeper	38
A Note about the Non-Critical Temperature Threshold Alarm	38

Chapter 5 Using the Web Interface 39

Logging in to the Web Interface.....	39
Login.....	39
Changing Your Password.....	42
Web Interface Elements	42
Menus.....	42
Navigation Path	44
Status Panel	45
Status Messages.....	47
Unavailable Options	47
Reset to Defaults	47
Refresh	48
Using the Home Page.....	48
Line Loads Display	48

Circuit Breaker Status.....	49
Outlets List.....	50
All Outlets Control.....	51
Measurement Accuracy	52
Managing the Dominion PX	52
Displaying Basic Device Information	52
Displaying Model Configuration Information.....	53
Naming the Dominion PX Device	55
Modifying the Network Settings.....	56
Modifying the Network Service Settings.....	58
Modifying the LAN Interface Settings	59
Setting the Date and Time.....	59
Specifying the Device Altitude.....	61
Configuring the SMTP Settings	62
Configuring the SNMP Settings.....	63
Enabling Data Retrieval.....	64
Resetting the Dominion PX Device	66
Updating the Firmware	67
Copying Configurations with Bulk Configuration	72
Setting Up User Profiles	75
Creating a User Profile	75
Copying a User Profile.....	77
Modifying a User Profile	78
Deleting a User Profile.....	78
Setting User Permissions Individually	79
Setting Up User Groups.....	80
Creating a User Group	80
Setting the System Permissions.....	80
Setting the Outlet Permissions	82
Copying a User Group.....	83
Modifying a User Group.....	83
Deleting a User Group.....	84
Setting Up and Managing Outlets.....	84
Setting the Global Default Outlet State	85
Setting the Global Power Cycling Delay.....	86
Setting the Outlet Power-On Sequence	87
Naming and Configuring Outlets	88
Viewing Outlet Details	89
Power Cycling an Outlet.....	90
Turning an Outlet On or Off.....	90
Setting Up Power Thresholds and Hysteresis.....	91
Setting PDU Thresholds and Hysteresis	91
Setting Outlet Thresholds and Hysteresis	92
Monitoring Line and Circuit Breaker Status	93
Monitoring Unbalanced Loads.....	94
Line Details Page	96
Circuit Breaker Details Page	96
Access Security Control.....	97
Forcing HTTPS Encryption.....	97
Configuring the Firewall.....	98
Creating Group Based Access Control Rules	101
Setting Up User Login Controls.....	104

Disabling the PDU's Ping Response	108
Setting Up a Digital Certificate	108
Creating a Certificate Signing Request	109
Installing a Certificate	111
Setting Up External User Authentication	112
Gathering Information for LDAP Configuration.....	113
Setting Up LDAP Authentication.....	114
Setting Up RADIUS Authentication	117
Environmental Sensors.....	118
Identifying Environmental Sensors	119
Managing Environmental Sensors.....	121
Configuring Environmental Sensors	122
Viewing Sensor Readings and States	127
Unmanaging Environmental Sensors.....	130
Assigning or Changing the ID Number.....	131
Configuring and Using Alert Notifications	131
Components of an Alert.....	132
How to Configure an Alert	132
Sample Alerts	140
A Note about Untriggered Alerts.....	142
Setting Up Event Logging	144
Configuring the Local Event Log	145
Configuring the NFS Logging	148
Configuring the SMTP Logging	149
Configuring the SNMP Logging.....	150
Configuring the Syslog Forwarding	150
Outlet Grouping.....	151
Identifying Other Dominion PX Devices	152
Grouping Outlets Together	153
Viewing and Controlling Outlet Groups	154
Editing or Deleting Outlet Groups.....	155
Deleting Outlet Group Devices	155
Setting the FIPS Mode.....	156
FIPS Limitations	156
Configuring the FIPS Mode	157
Diagnostics	158
Network Interface Page	159
Network Statistics Page.....	159
Ping Host Page.....	161
Trace Route to Host Page	161
Saving a Device Diagnostics File	162
Using Online Help	163

Chapter 6 Using SNMP **165**

Enabling SNMP.....	165
Configuring Users for Encrypted SNMP v3	167
Restarting the SNMP Agent after Adding Users	168
Configuring the SNMP Traps.....	169
Suggestion for SNMP Trap Configuration	170

A False Circuit Breaker Trip Trap	170
SNMP Gets and Sets.....	171
The Dominion PX MIB	171
SNMP Sets and Configurable Objects	172
Configuring the Hysteresis	173
Disabling Outlet Switching.....	173
Setting Data Retrieval.....	173
Retrieving Energy Usage.....	173
Configuring the FIPS Mode	174
Changing ID Numbers of Environmental Sensors.....	174
A Note about Measurement Units	176
Retrieving and Interpreting Sensor Readings	176

Chapter 7 Using the CLP Interface 180

About the CLP Interface	180
Logging in to the CLP interface	180
With HyperTerminal.....	181
With SSH or Telnet.....	182
Closing a Serial Connection	183
Showing Outlet Information	183
Syntax.....	184
Attributes.....	184
Examples	184
Showing In-Depth Outlet Information.....	185
Outlet Sensor Properties	186
Examples of Showing In-Depth Outlet Information	186
Switching an Outlet.....	187
Turning an Outlet On	187
Turning an Outlet Off	187
Querying an Outlet Sensor	188
Setting the Sequence Delay	188
Showing Environmental Sensor Information	188
Identifying Sensor Types	189
Example 1 - No Attributes.....	189
Example 2 - Name Attribute	190
Example 3 - CurrentReading Attribute	190
Configuring the Thresholds for Environmental Sensors.....	191
Querying the PDU's Serial Number	192
Resetting the Dominion PX Device.....	192
Using the Help Command.....	192
Example 1 - Help Information for the Show Command	192
Example 2 - Getting In-Depth Help Information	193

Chapter 8 In-line Monitors 194

Overview	194
Models with Power Sockets.....	195
Models with Cable Glands.....	195

Contents

Flexible Cord Installation Instructions	196
Flexible Cord Selection.....	197
Plug Selection.....	197
Receptacle Selection.....	197
Derating a Raritan Product.....	197
Wiring of 3-Phase In-Line Monitors	198
In-Line Monitor Unused Channels.....	198
Step by Step Flexible Cord Installation	199
In-line Monitor's LED Display.....	204
Automatic Mode.....	204
Manual Mode.....	205
In-line Monitor's Web Interface	205
Menus.....	206
Home Page.....	207
SNMP and CLP Interfaces.....	208

Appendix A Specifications **209**

Maximum Ambient Operating Temperature	209
Dominion PX Serial RJ-45 Port Pinouts	209
Dominion PX Feature RJ-12 Port Pinouts	209

Appendix B Equipment Setup Worksheet **211**

Appendix C Enabling or Disabling the Power CIM **215**

Appendix D Integration **216**

Power IQ Configuration	218
Adding PDUs to Power IQ Management.....	218
Dominion KX II Power Strip Configuration.....	220
Configuring Rack PDU (Power Strip) Targets.....	220
Dominion KX I Power Strip Configuration.....	224
Setup Preparation.....	224
Connecting the Power Strip.....	224
Configuring the Power Strip.....	225
KX Manager Application	226
Associating Outlets with a Target Server	226
Controlling a Target Server's Power.....	228
Paragon II	229
Adding a Dominion PX in Paragon II.....	230
Associating Outlets with a Target Server	230
Controlling a Target Server's Power.....	231
Controlling an Outlet's Power	231
Paragon Manager Application	232

Dominion SX	232
Configuring a Dominion PX on Dominion SX	232
Power Control	234
Checking Power Strip Status	235
Dominion KSX	235
CommandCenter Secure Gateway	236
Direct Control from CC-SG 4.0 or Later	236

Appendix E Using the IPMI Tool Set 237

Channel Commands	237
authcap <channel number> <max priv>	237
info [channel number]	238
getaccess <channel number> [userid]	238
setaccess <channel number> <userid>[callin=on off] [ipmi=on off] [link=on off] [privilege=level]	238
getciphers <all supported> <ipmi sol> [channel]	238
Event Commands	238
<predefined event number>	239
file <filename>	239
LAN Commands	239
print <channel>	239
set <channel> <parameter>	240
Sensor Commands	241
list	241
get <id> ... [<id>]	241
thresh <id> <threshold> <setting>	241
OEM Commands	242
A Note about Group Commands	243
A Note about Outlet Numbers	243
Set Power On Delay Command	244
Get Power On Delay Command	245
Set Receptacle State Command	245
Get Receptacle State Command	245
Get Receptacle State and Data Command	246
Set Group State Command	246
Set Group Membership Command	247
Get Group Membership Command	247
Set Group Power On Delay Command	248
Get Group Power On Delay Command	248
Set Receptacle ACL	248
Get Receptacle ACL	249
Test Actors	249
Test Sensors	249
Set Power Cycle Delay Command	249
Get Power Cycle Delay Command	250

Contents

IPMI Privilege Levels	250
IPMI in the FIPS Mode.....	251
Appendix F Additional PDU Information	253
<hr/>	
Default Hysteresis Values for Thresholds.....	253
Event Types	253
MAC Address.....	255
Altitude Correction Factors	255
Data for BTU Calculation	256
Appendix G LDAP Configuration Illustration	257
<hr/>	
Step A. Determine User Accounts and Groups.....	257
Step B. Configure User Groups on the AD Server	258
Step C. Configure LDAP Authentication on the Dominion PX Device.....	259
Step D. Configure User Groups on the Dominion PX Device.....	262
Appendix H Resetting the PDU Settings	267
<hr/>	
Resetting to Factory Defaults	267
Resetting the Administrator Password.....	268
Index	269
<hr/>	

Applicable Models

This user guide is applicable to the Raritan PDUs whose model names begin with DPXS, DPXR, DPCS, DPCR, or PX.

*Note: For information on PDUs whose model names begin with PX2, see the "PX2-1000/2000 Series" or "PX2-3000/4000/5000 Series" User Guide or online help on the **Raritan website** (<http://www.raritan.com>).*

What's New in the Dominion PX User Guide

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

Product Features (on page 3)

Initial Network and Time Configuration (on page 19)

Menus (on page 42)

Status Panel (on page 45)

Modifying the Network Service Settings (on page 58)

Configuring the SNMP Settings (on page 63)

Saving a Dominion PX Configuration (on page 73)

Setting Up User Profiles (on page 75)

Forcing HTTPS Encryption (on page 97)

Setting Up External User Authentication (on page 112)

Setting the FIPS Mode (on page 156)

Enabling SNMP (on page 165)

Configuring the FIPS Mode (on page 174)

Retrieving and Interpreting Sensor Readings (on page 176)

Flexible Cord Installation Instructions (on page 196)

Menus (on page 206)

Power IQ Configuration (on page 218)

Direct Control from CC-SG 4.0 or Later (on page 236)

IPMI in the FIPS Mode (on page 251)

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

Chapter 1 Introduction

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

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

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

In This Chapter

Product Models.....	1
Product Photos	1
Product Features	3
Package Contents	5

Product Models

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

Visit the **Product Selector page** (<http://www.raritan.com/resources/px-product-selector/>) on the Raritan website or contact your local reseller for a list of available models.

Product Photos

The Dominion PX comes in Zero U, 1U, and 2U sizes.

Zero U Size



1U Size



2U Size





Product Features

The Dominion PX models vary in sizes and features. In general, the Dominion PX features include:

- For units with switching, the ability to power on, power off, and reboot the devices connected to each outlet.
- The ability to group outlets from multiple Dominion PX devices as virtual outlets accessible from a single session
- The ability to monitor the following at the outlet level:

RMS Current

Power Factor

Maximum RMS Current

Voltage

Active Power

Apparent Power

Energy Consumption (Active Energy) on some models (part numbers follow PX-nnnn format, where n is a number)

- The ability to monitor the internal CPU temperature of the Dominion PX device
- The ability to display temperatures in both Celsius and Fahrenheit
- The ability to monitor environmental factors such as external temperature and humidity
- User-specified location attributes for environmental sensors
- An audible alarm (beeper) and a visual alarm (blinking LED) to indicate current overload
- An audible alarm (beeper) for circuit breaker tripping
- Configurable alarm thresholds and hysteresis
- Support for SNMP v1, v2, and v3
- The ability to send traps using the SNMP protocol
- The ability to retrieve outlet specific data using SNMP, including outlet state, current, voltage, and power
- The ability to store a history of sampled data at all levels (unit, circuit breaker, and so on) and retrieve it via SNMP

Note: Raritan's Power IQ or other external systems can retrieve the stored data (samples) from the Dominion PX.

- The ability to configure and set values through SNMP, including power threshold levels
- The ability to save one Dominion PX device's configuration settings and then deploy those settings to other Dominion PX devices
- Local overcurrent protection (OCP) via branch circuit breakers or fuses on products rated over 20A to protect connected equipment against overload and short circuits
- Support for the Federal Information Processing Standards (FIPS) that are defined in the **FIPS PUB 140-2** (<http://www.nist.gov/cmvp/>), Security Requirements for Cryptographic Modules
- Integration with Raritan's Paragon II, CommandCenter Secure Gateway (CC-SG), and Dominion access devices
- Line current and circuit breaker monitoring
- Load imbalance calculations, for 3-phase models
- A combination of outlet types (for example, C13 and C19 outlets) in select models
- A combination of outlet voltages (120 and 208 volts) in select models
- Support for high current devices (such as Blade Servers) in select models
- Full disaster recovery option in case of a catastrophic failure during a firmware upgrade

Package Contents

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

Zero U Products

- The Dominion PX device
- Screws, brackets and/or buttons for Zero U
- Null-modem cable with RJ-45 and DB9F connectors on either end
- Quick Setup Guide
- Warranty card

1U Products

- The Dominion PX device
- 1U bracket pack and screws
- Null-modem cable with RJ-45 and DB9F connectors on either end
- Quick Setup Guide
- Warranty card

2U Products

- The Dominion PX device
- 2U bracket pack and screws
- Null-modem cable with RJ-45 and DB9F connectors on either end
- Quick Setup Guide
- Warranty card

Chapter 2 Rack-Mounting the PDU

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

In This Chapter

Rackmount Safety Guidelines	6
Circuit Breaker Orientation Limitation.....	6
Standard Rackmount.....	7
Mounting Zero U Models Using L-Brackets.....	8
For Zero U Models Using Tool-less Button Mounting	9
Mounting Zero U Models Using Claw-Foot Brackets	12
Mounting 1U or 2U Models.....	13

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 209) 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.

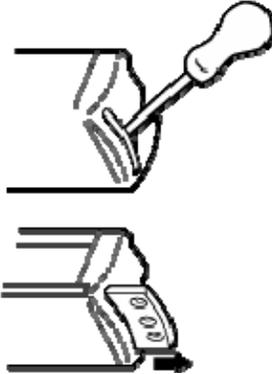
Circuit Breaker Orientation Limitation

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 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.

Standard Rackmount

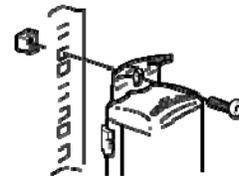
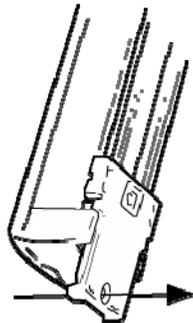
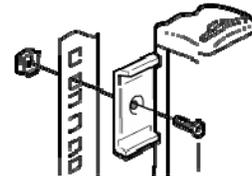
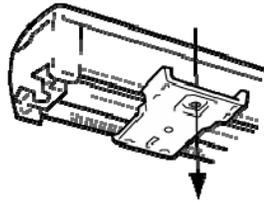


The Zero U units are provided with high grade engineering polycarbonate isolation hardware to allow fixing in a variety of positions within the rack.

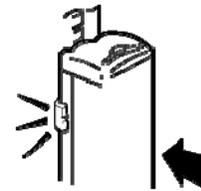
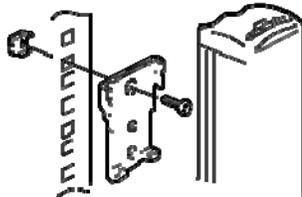
For panel/flush mount, pull out fixing brackets are available on each end cap to allow mounting on suitable rails.

See other options shown below.

Side Fixing

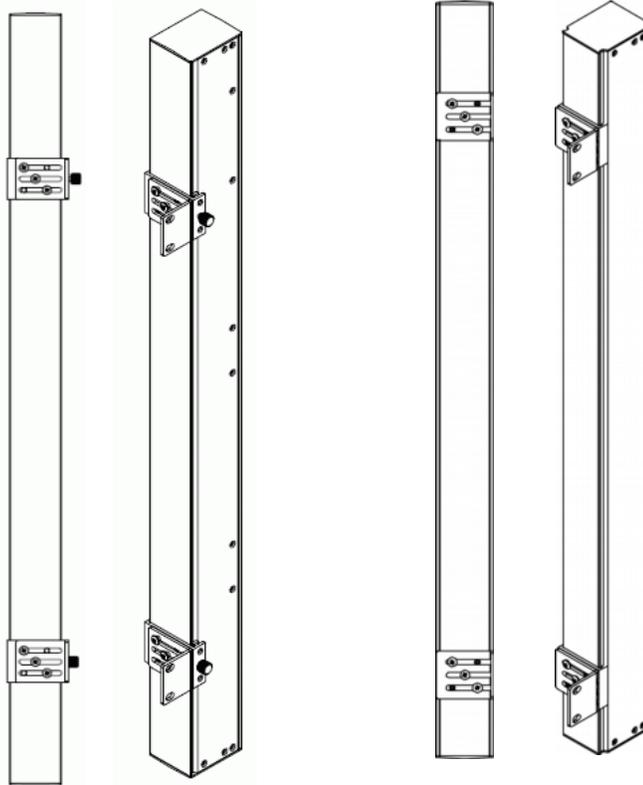


Blind Fixing



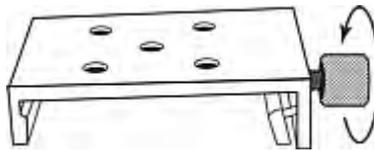
Mounting Zero U Models Using L-Brackets

If your PDU has circuit breakers implemented, read **Circuit Breaker Orientation Limitation** (on page 6) before mounting it.

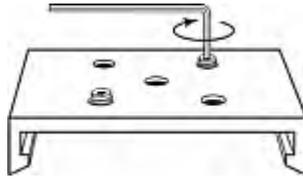


► To mount Zero U models using L-brackets:

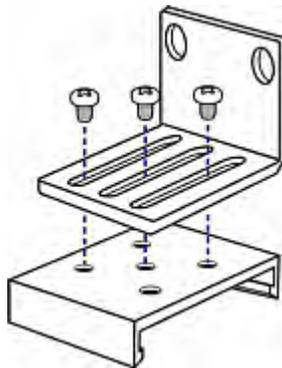
1. Align the baseplates on the rear of the Dominion PX device.
2. Secure the baseplates in place. Different models ship with different types of baseplates.
 - To secure a baseplate with the thumbscrew, turn the thumbscrew until it is tightened.



- To secure a baseplate without the thumbscrew, use the included L-shaped hex key to loosen the hex socket screws until the baseplate is fastened.



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



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

For Zero U Models Using Tool-less Button Mounting

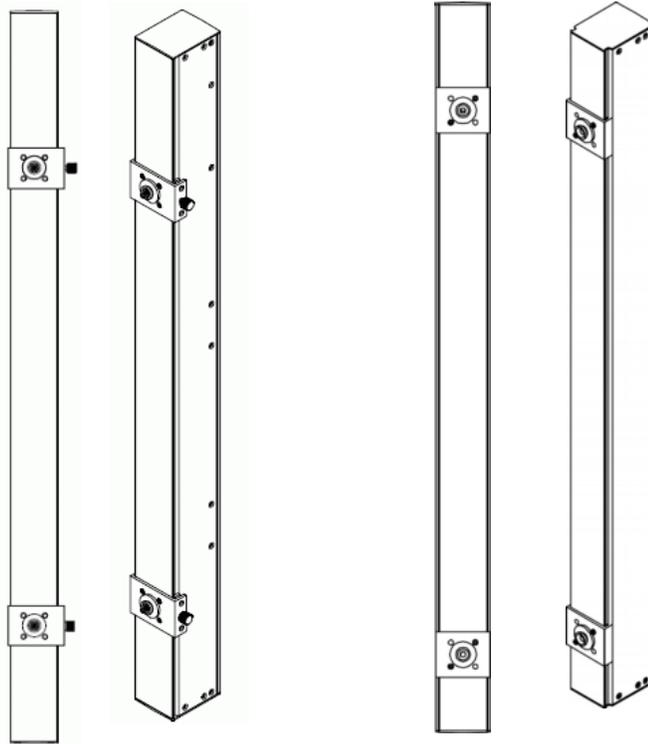
Some Zero U PDUs ship with tool-less mounting brackets consisting of an adjustable baseplate with a large button. These work by attaching to the back side of a Zero U Dominion PX device (the side opposite of the outlets) and fitting the button into the mounting holes of the cabinet. Note that not all racks may allow the option of securing the Dominion PX device in this way.

Before You Begin Tool-less Mounting:

- Ensure that you have sufficient space in the cabinet to mount the Dominion PX device. Approximately one inch of clearance is required at each end (top and bottom) of the device.
- It may help to mark the back of the Dominion PX device through the mounting holes you intend to use. You can then use this mark to assist in aligning the silver buttons properly when attaching the base-plate.

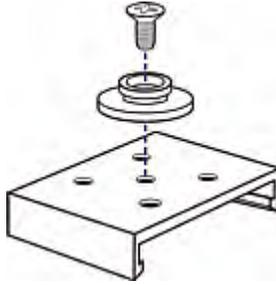
Mounting Zero U Models Using Button Mount

If your PDU has circuit breakers implemented, read **Circuit Breaker Orientation Limitation** (on page 6) before mounting it.



► **To mount Zero-U models using button mount:**

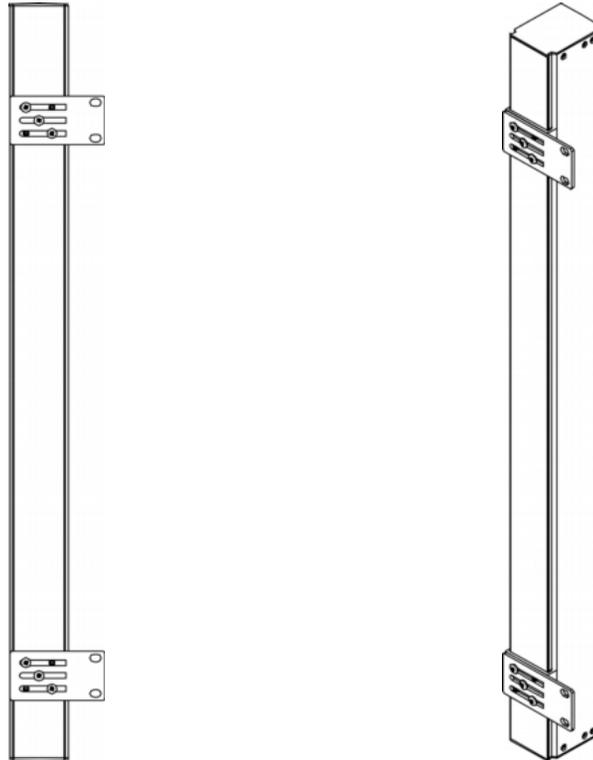
1. Align the baseplates on the rear of the Dominion PX device. Leave at least 24 inches between the baseplates for stability.
2. Make the baseplates grasp the Dominion PX device lightly.
 - For a baseplate with the thumbscrew, turn the thumbscrew until it is "slightly" tightened.
 - For a baseplate without the thumbscrew, use the included L-shaped hex key to loosen the hex socket screws until the baseplate is "slightly" fastened.
3. Screw each mounting button in the center of each baseplate. The recommended torque for the button is 1.96 N·m (20 kgf·cm).



4. Align the large mounting buttons with the mounting holes in the cabinet, fixing one in place and adjusting the other.
5. Depending on the type of your baseplates, either further tighten the thumbscrews or loosen the hex socket screws until the mounting buttons are secured in their position.
6. Ensure that both buttons can engage their mounting holes simultaneously.
7. Press the Dominion PX device forward, pushing the mounting buttons through the mounting holes, then letting the device drop about 5/8". This secures the Dominion PX device in place and completes the installation.

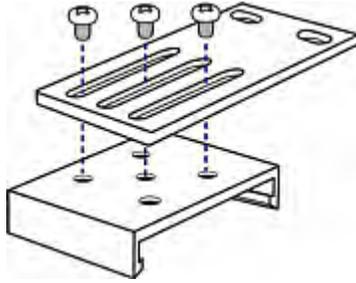
Mounting Zero U Models Using Claw-Foot Brackets

If your PDU has circuit breakers implemented, read **Circuit Breaker Orientation Limitation** (on page 6) before mounting it.



► **To mount Zero U models using claw-foot brackets:**

1. Align the baseplates on the rear of the Dominion PX device.
2. Secure the baseplates in place.
 - To secure a baseplate with the thumbscrew, turn the thumbscrew until it is tightened.
 - To secure a baseplate without the thumbscrew, use the included L-shaped hex key to loosen the hex socket screws until the baseplate is fastened.
3. Align the claw-foot brackets with the baseplates so that the five screw-holes on the baseplates line up through the bracket's slots. The rackmount side of brackets should face either the left or right side of the Dominion PX device.
4. Fasten the brackets in place with at least three screws (one through each slot). Use additional screws as desired.



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

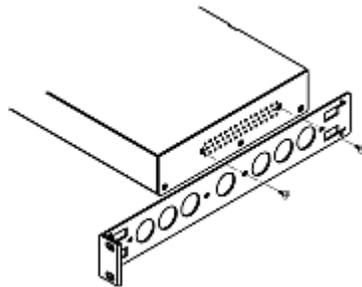
Mounting 1U or 2U Models

Using the appropriate brackets and tools, fasten the 1U or 2U Dominion PX device to the rack or cabinet. If your PDU has circuit breakers implemented, read **Circuit Breaker Orientation Limitation** (on page 6) before mounting it.

► **To mount the Dominion PX device:**

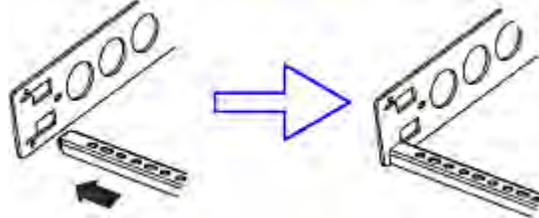
1. Attach one rackmount bracket to one side of the Dominion PX device.
 - a. Align two oval-shaped holes of the rackmount bracket with two threaded holes on one side of the Dominion PX device.
 - b. Secure the rackmount bracket with two of the Raritan-provided screws.

Note: The appropriate oval-shaped hole locations of the rackmount bracket may vary according to the threaded holes on your model.

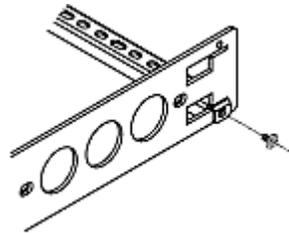


2. Repeat Step 1 for securing the other rackmount bracket to the other side of the Dominion PX.

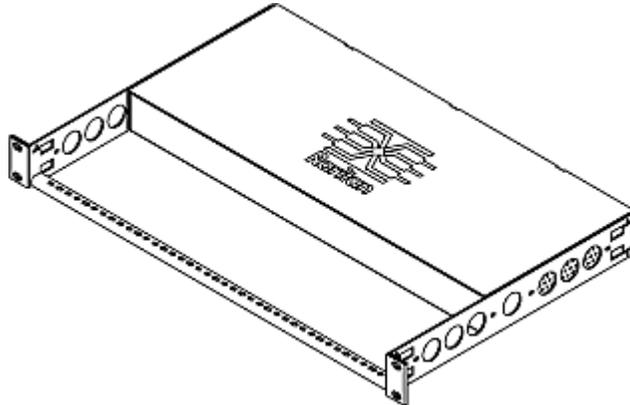
3. Insert one end of the cable-support bar into the L-shaped hole of the rackmount bracket, and align the hole on the end of the bar with the threaded hole adjacent to the L-shaped hole.



4. Secure the cable-support bar with one of the Raritan-provided cap screws.



5. Repeat Steps 3 to 4 to secure the other end of the cable-support bar to the other rackmount bracket.



6. Mount the Dominion PX device on the rack by securing the rackmount brackets' ears to the rack's front rails with your own screws, bolts, cage nuts, or the like.

Chapter 3 Installation and Configuration

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

In This Chapter

Before You Begin	15
Connecting the Dominion PX to a Power Source	16
Configuring the Dominion PX	17
Connecting Environmental Sensors (Optional)	25

Before You Begin

Before beginning the installation, perform the following activities:

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

Unpacking the Product and Components

1. Remove the Dominion PX device and other equipment from the box in which they were shipped. See **Package Contents** (on page 5) 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 Dominion PX device are set to ON. If not, turn them ON.

For a PDU with fuses, ensure that all fuses are inserted and seated properly. If there are any fuse covers, ensure that they are closed.

Note: Not all Dominion PX devices have overcurrent protection mechanisms.

Preparing the Installation Site

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

*Note: If necessary, contact Raritan Technical Support for the maximum operating temperature for your model. See **Maximum Ambient Operating Temperature** (on page 209).*

2. Allow sufficient space around the Dominion PX device for cabling and outlet connections.
3. Review the **Safety Instructions** (on page iii) listed in the beginning of this user guide.

Filling Out the Equipment Setup Worksheet

An Equipment Setup Worksheet is provided in this guide. See **Equipment Setup Worksheet** (on page 211). 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.

Connecting the Dominion PX to a Power Source

The distance between a PDU and its power source must be SHORTER than the PDU's line cord to avoid stretching out the cord. A locking connector used at the power source is highly recommended for a secure connection.

► **To connect a PDU to the power source:**

1. Verify that all circuit breakers on the Dominion PX device are set to ON. If not, turn them ON.

For a PDU with fuses, ensure that all fuses are inserted and seated properly. If there are any fuse covers, ensure that they are closed.

Note: Not all Dominion PX devices have overcurrent protection mechanisms.

2. Connect each Dominion PX device to an appropriately rated branch circuit. See the label or nameplate affixed to your Dominion PX device for appropriate input ratings or range of ratings.
3. With a 1U or 2U model, a blue power LED on the front panel is lit. A Zero U model does not have a similar power LED because it will be mounted in the back of an equipment rack.
4. When a Dominion PX device powers up, it proceeds with the power-on self test and software loading for a few moments. At this time, the outlet LEDs cycle through different colors.
5. When the software has completed loading, the outlet LEDs show a steady color and the LED display illuminates.

Configuring the Dominion PX

There are two alternatives to initially configure a Dominion PX device:

- Connect the Dominion PX device to a computer to configure it, using a serial connection between the Dominion PX and the computer.

The computer must have a communications program such as HyperTerminal or PuTTY. In addition, you need a null-modem cable with RJ-45 and DB9F connectors on either end.

- Connect the Dominion PX device to a TCP/IP network that supports DHCP.

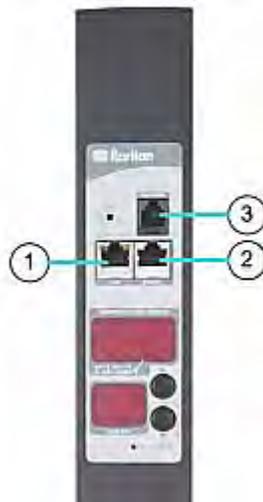
The DHCP-assigned IP address can be retrieved through the Dominion PX's MAC address. You can contact your LAN administrator for assistance. See **MAC Address** (on page 255).

A Cat5e/6 UTP cable is required.

Connecting the Dominion PX to a Computer

► **To connect the PDU to the computer:**

1. Connect the RJ-45 end of the null-modem cable to the port labeled Serial on the front of the Dominion PX device.





Item #	Description
1	LAN Port
2	Serial Port
3	Feature Port

2. Connect the DB9 end of the null-modem cable to the serial port (COM) of the computer.

Note: If you plan to use the serial connection to log in to the command line interface, leave the cable connected after the configuration is complete.

Connecting the Dominion PX to Your Network

To use the web interface to administer the Dominion PX, you must connect the Dominion PX to your local area network (LAN).

► **To connect the PDU to the network:**

1. Connect a standard Cat 5e UTP cable to the LAN port on the front of the Dominion PX device. See **Connecting the Dominion PX to a Computer** (on page 17) for the location of this port on your PDU.
2. Connect the other end of the cable to your LAN.

Initial Network and Time Configuration

After the Dominion PX device is connected to your network, you must provide it with an IP address and some additional networking information. If necessary, configure the NTP settings while determining the networking configuration.

► **To configure the networking parameters:**

1. Go to the computer that you connected to the Dominion PX and open a communications program such as HyperTerminal or PuTTY.
2. Select the appropriate COM port, and make sure the port settings are configured as follows:
 - Bits per second = 9600
 - Data bits = 8
 - Stop bits = 1
 - Parity = None
 - Flow control = None

Note: The "Flow control" parameter must be set to "None" to ensure that the communications program will work correctly with the Dominion PX.

3. Press Enter to display the opening configuration prompt.

```

Welcome!
At the prompt type one of the following commands:
- "clp"      : Enter Command Line Protocol
- "config"   : Perform initial IP configuration
- "unblock"  : Unblock currently blocked users
192.168.80.55 command:
  
```

4. Type `config` and press Enter to begin the configuration process. You are prompted to assign a name to the Dominion PX device.

```

Welcome!
At the prompt type one of the following commands:
- "clp"      : Enter Command Line Protocol
- "config"   : Perform initial IP configuration
- "unblock"  : Unblock currently blocked users
192.168.80.55 command: config
Device Name [PNM0987678]:
  
```

5. Type the name for the PDU and press Enter. The default name is the PDU's serial number.
6. You are prompted to select an IP configuration method. An IP address must be assigned to the PDU. There are two ways to do this:

- Auto configuration - Select an auto configuration method such as `dhcp` or `bootp` and let the DHCP or BOOTP server provide the IP address.
- Static IP address - Select `none` and assign the PDU a static IP address. You will be prompted for the address, network mask, and gateway.

*Note: The Dominion PX's IP address is automatically displayed in the system prompt. The default static IP address is 192.168.0.192. The default IP configuration method is DHCP. The default IP address will be replaced by the address assigned by DHCP or BOOTP, or the static IP address you entered, when the configuration process is complete. To use the factory default IP address, type in **none** as the IP autoconfiguration command, and accept the default value.*

Type your selection and press Enter. You are prompted to enable IP access control.

```
Welcome!
At the prompt type one of the following commands:
- "clp"      : Enter Command Line Protocol
- "config"   : Perform initial IP configuration
- "unblock"  : Unblock currently blocked users
192.168.80.55 command: config
Device Name [PNM0987678]: My PX
IP autoconfiguration (none/dhcp/bootp) [dhcp]: dhcp
Enable IP Access Control (yes/no) [no]:
```

7. By default, IP access control is NOT enabled. This disables the Dominion PX firewall. Leave the firewall disabled for the present. Later you can enable the firewall from the web interface and create firewall rules. See **Configuring the Firewall** (on page 98).

Note: If you ever accidentally create a rule that locks you out of the Dominion PX, you can rerun the configuration program and reset this parameter to disabled to allow you to access the Dominion PX device.

8. Press Enter. You are prompted to set the LAN interface speed.

```
Welcome!
At the prompt type one of the following commands:
- "clp"      : Enter Command Line Protocol
- "config"   : Perform initial IP configuration
- "unblock"  : Unblock currently blocked users
192.168.80.55 command: config
Device Name [PNM0987678]: My PX
IP autoconfiguration (none/dhcp/bootp) [dhcp]: dhcp
Enable IP Access Control (yes/no) [no]: no
LAN interface speed (auto/10/100) [auto]:
```

9. By default, the LAN interface speed is set to `auto`, which allows the system to select the optimum speed. To keep the default, press Enter. To set the speed to 10 or 100 Mbps, type the speed you want and press Enter. You are prompted to select the duplex mode for the LAN interface.

```

Welcome!
At the prompt type one of the following commands:
- "clp"      : Enter Command Line Protocol
- "config"   : Perform initial IP configuration
- "unblock"  : Unblock currently blocked users
192.168.80.55 command: config
Device Name [PNM0987678]: My PX
IP autoconfiguration (none/dhcp/bootp) [dhcp]: dhcp
Enable IP Access Control (yes/no) [no]: no
LAN interface speed (auto/10/100) [auto]: 100
LAN interface duplex mode (auto/half/full) [auto]:

```

10. By default, the LAN interface duplex mode is set to `auto`, which allows the system to pick the optimum mode. Half duplex allows data to be transmitted to and from the Dominion PX device, but not at the same time. Full duplex allows data to be transmitted in both directions at the same time.

To keep the default, press Enter. To specify half or full duplex, type `half` or `full` and press Enter.

11. The FIPS mode is disabled by default. Press Enter to leave it disabled, or type `yes` to enable it. Note that after enabling the FIPS mode, the Dominion PX only supports the FIPS approved algorithms, which are defined in **FIPS PUB 140-2**. See **Setting the FIPS Mode** (on page 156).

```

Welcome!
At the prompt type one of the following commands:
- "clp"      : Enter Command Line Protocol
- "config"   : Perform initial IP configuration
- "unblock"  : Unblock currently blocked users
192.168.80.55 command: config
Device Name [PNM0987678]: My PX
IP autoconfiguration (none/dhcp/bootp) [dhcp]: dhcp
Enable IP Access Control (yes/no) [no]: no
LAN interface speed (auto/10/100) [auto]: 100
LAN interface duplex mode (auto/half/full) [auto]:
Enable FIPS mode (yes/no) [no]:

```

12. The SNMP agent implemented on the Dominion PX device is enabled by default.

- To keep the default, press Enter. You are then prompted to enable or disable the SNMP v1/v2c and SNMP v3 protocols.

Note: SNMP v1/v2c is not supported and unavailable if enabling the FIPS mode.

- To disable the SNMP agent, type `no` and press Enter.

If you enable the SNMP v1/v2c protocol, the Dominion PX prompts you to specify the read and write community strings. The default read community string is "raritan_public," and the default write community string is "raritan_private."

If you enable the SNMP v3 protocol, the Dominion PX prompts you to determine whether to force the SNMP v3 encryption.

Exception: If the FIPS mode is enabled, the SNMP v3 encryption is automatically forced and cannot be configured when enabling the SNMP v3 protocol.

Then the system prompts you to specify the system location and contact person.

```
Welcome!
At the prompt type one of the following commands:
- "clp"      : Enter Command Line Protocol
- "config"   : Perform initial IP configuration
- "unblock"  : Unblock currently blocked users
192.168.80.55 command: config
Device Name [PNM0987678]: My PX
IP autoconfiguration (none/dhcp/bootp) [dhcp]: dhcp
Enable IP Access Control (yes/no) [no]: no
LAN interface speed (auto/10/100) [auto]: 100
LAN interface duplex mode (auto/half/full) [auto]:
Enable FIPS mode (yes/no) [no]:
Enable SNMP Agent (yes/no) [yes]: yes
Enable SNMP v1 / v2c Protocol (yes/no) [yes]: yes
Read Community [raritan_public]: public
Write Community [raritan_private]: private
Enable SNMP v3 Protocol (yes/no) [no]: yes
Force V3 Encryption (yes/no) [no]: yes
System Location []: TP
System Contact []:
```

13. Now determine whether to enable or disable NTP servers for the date and time setting.

- Synchronization with NTP servers: Type *y* if you want the PDU's date and time to sync up with NTP servers.
- Manual configuration: Type *n* if you want to set the date and time manually later through the Dominion PX web interface. See **Setting the Date and Time** (on page 59).

```
⋮
Read Community [raritan_public]: public
Write Community [raritan_private]: private
Enable SNMP v3 Protocol (yes/no) [no]: yes
Force V3 Encryption (yes/no) [no]: yes
System Location []: TP
System Contact []: John
Enable ntp? (y/n) [Note: 'n' will keep the current date-time setting]: y
```

14. If synchronization with NTP servers is enabled in the previous step, a list of time zones is displayed and the Dominion PX prompts you to select a time zone. Type the number or the name of the desired time zone.

```

:
Enable ntp? (y/n) [Note: 'n' will keep the current date-time setting]: y
----- Timezones available -----
(1) Africa/Abidjan
(2) Africa/Accra
(4) Africa/Algiers
(5) Africa/Asmara
(6) Africa/Bamako
(7) Africa/Bangui
(8) Africa/Banjul
(9) Africa'Bissau
:
(398) Pacific/Rarotonga
(399) Pacific/Saipan
(400) Pacific/Tahiti
(401) Pacific/Tarawa
(402) Pacific/Tongatapu
(403) Pacific/Wake
(404) Pacific/Wallis
(405) UTC
(406) WET
-----
Set Time Zone (select name or number from above list) [Europe/London]:

```

15. When prompted to enable the daylight savings time, type `yes` to enable it if the daylight savings time is applicable to the selected time zone, or type `no` to disable it.

```

:
(405) UTC
(406) WET
-----
Set Time Zone (select name or number from above list) [Europe/London]: 7
Enable Daylight Savings (yes/no) [yes]:

```

16. You must determine which NTP servers are used if the NTP synchronization is enabled in Step 13.
- Auto-assigned NTP servers:
To use the NTP servers provided by the DHCP or BOOTP server, type `yes` when prompted whether to use DHCP- or BOOTP-assigned NTP servers.
 - Manually-assigned NTP servers:

To manually specify NTP servers, type `no` when prompted whether to use DHCP- or BOOTP-assigned NTP servers. The system then prompts you to specify primary and secondary NTP servers. A secondary NTP server is optional, and you can simply press Enter if a secondary one is unavailable.

```
⋮
(405) UTC
(406) WET
-----
Set Time Zone (select name or number from above list) [Europe/London]: 7
Enable Daylight Savings (yes/no) [yes]: yes
Prefer NTP Servers provided by DHCP/BOOTP (yes/no) [yes]: no
Primary Time Server [1]: 192.168.84.123
Secondary Time Server []:
```

17. You are prompted to confirm the information you just entered.

```
⋮
Are the entered values correct? Enter y for Yes, n for No or c to Cancel
```

All the configuration parameters have been entered. All the prompts are still displayed, so you can check the information you entered. Do one of the following:

- If the information is correct, type `y` and press Enter. The system performs the configuration and displays a configuring message to indicate the configuration is being performed.
- If one or more parameters are not correct, type `n` and press Enter. You are returned to the device name prompt as shown in Step 4 to have an opportunity to re-enter each piece of information.
- If you want to terminate the configuration process, type `c` and press Enter. The configuration is thus canceled and you are returned to the opening prompt.

18. If you entered `y` to confirm the configuration, you will be returned to the opening prompt after the configuration is complete. You are now ready to begin using your Dominion PX.

```
⋮
Are the entered values correct? Enter y for Yes, n for No or c to Cancel y
Configuring device ...
```

Note: The IP address configured takes about at least 3 minutes to take effect for the PDU connected via the serial line, or even longer if configured over DHCP.

*Note: If the Dominion PX device is connected to a Raritan KVM switch, and you want to disable the connected KVM switch's capability of monitoring and controlling the PDU, you can disable the connected power CIM using the CLP command. See **Enabling or Disabling the Power CIM** (on page 215).*

Connecting Environmental Sensors (Optional)

To enable the detection of environmental factors around the Dominion PX, connect one or more Raritan environmental sensors to the Dominion PX device.

The maximum distance for all sensor cabling plugged into the product's sensor port should not exceed 30 meters/100 feet. Contact Raritan Technical Support if you have questions.

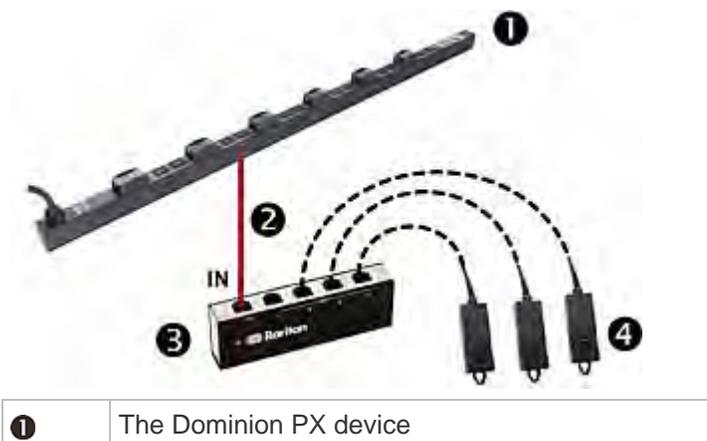
► **To directly connect an environmental sensor:**

Connect the cable of the environmental sensor to the Feature port on the Dominion PX device.

► **To connect environmental sensors via an optional PX sensor hub:**

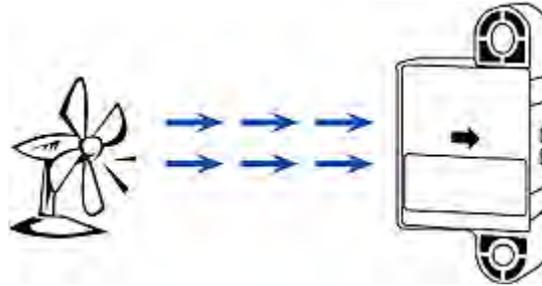
1. Connect a Raritan sensor hub to the Dominion PX device.
 - a. Plug one end of the Raritan-provided phone cable (4-wire, 6-pin, RJ-12) into the IN port (Port 1) of the hub.
 - b. Plug the other end into the Feature port of the Dominion PX device.
2. Connect Raritan environmental sensors to any of the four OUT ports on the hub.

Raritan sensor hubs CANNOT be cascaded so at most a sensor hub can be connected to each SENSOR port on the Dominion PX device. This diagram illustrates a configuration with a sensor hub connected.



②	Raritan-provided phone cable
③	Raritan PX sensor hub
④	Raritan environmental sensors

3. If there are any Raritan air flow sensors attached, make sure that sensor faces the source of the wind (such as a fan) in the appropriate orientation as indicated by the arrow on that sensor.



Note: The temperature and humidity sensors are compatible with all Dominion PX models with these prefixes: DPXS, DPXR, DPCS, DPCR, PX-5nnn, PX-4nnn, and PX-3nnn, where n is a number.

About Contact Closure Sensors

Raritan's contact closure sensor (DPX-CC2-TR) can detect the open-and-closed status of the connected detectors/switches. When an open status is detected, the Dominion PX emits an audible alarm in the form of a beep.

This feature requires the integration of at least a discrete (on/off) detector/switch to work properly. The types of discrete detectors/switches that can be plugged into DPX-CC2-TR include those for:

- Door open/closed detection
- Door lock detection
- Floor water detection
- Smoke detection
- Vibration detection

Raritan does NOT provide these discrete detectors/switches. They are third-party probes so you must test them with Raritan's DPX-CC2-TR to ensure they work properly.

Integration and testing for third-party detectors/switches is the sole responsibility of the customer. Raritan cannot assume any liability as a result of improper termination or failure (incidental or consequential) of third-party detectors/switches that customers provide and install. Failure to follow installation and configuration instructions can result in false alarms or no alarms. Raritan makes no statement or claim that all third-party detectors/switches will work with DPX-CC2-TR.

DPX-CC2-TR is compatible with all Dominion PX models with these prefixes: DPXS, DPXR, DPCS, DPCR, PX-5nnn, PX-4nnn and PX-3nnn, where n is a number.

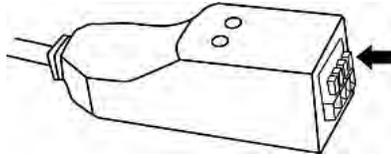
Connecting Third-Party Detectors/Switches to DPX-CC2-TR

A DPX-CC2-TR unit provides two channels for connecting two third-party detectors/switches. There are four spring-loaded termination points on the body of DPX-CC2-TR: the two to the right are associated with one channel (as indicated by the LED number), and the two to the left are associated with another channel. You must plug the third-party detectors/switches into these termination points.

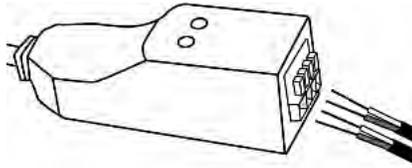
► **To connect third-party detectors/switches:**

1. Strip the insulation around 12mm from the end of each wire of two third-party detectors/switches.
2. Press and hold down the tiny rectangular buttons above the termination points on the body of DPX-CC2-TR.

Note: Each button controls the spring of each corresponding termination point.



3. Fully insert each wire of both third-party detectors/switches into each termination point.
 - Plug both wires of a detector/switch into the two termination points to the left.
 - Plug both wires of another detector/switch into the two termination points to the right.



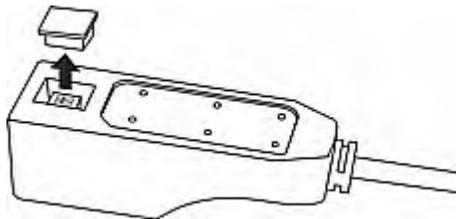
4. Release the tiny rectangular buttons after inserting the wires properly.
5. Verify that these wires are firmly fastened.

Configuring a Contact Closure Sensor

Before using DPX-CC2-TR to detect the contact closure status, water, smoke or vibration, you must determine the normal state by adjusting its dip switch, which controls the LED state on the body of DPX-CC2-TR. A dip switch is associated with a channel.

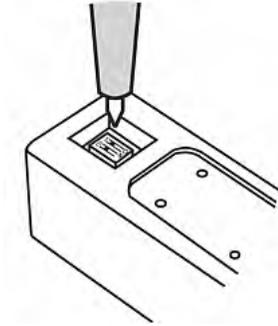
► To adjust the dip switch setting:

1. Place the detectors/switches connected to DPX-CC2-TR to the position where you want to detect a specific environmental situation.
2. Uncover the dip switch on the body of DPX-CC2-TR.



3. To set the Normal state for channel 1, locate the dip switch labeled 1.
4. Use a pointed tip such as a pen to move the slide switch to the end labeled NO (Normally Open) or NC (Normally Closed).

- Normally Open: The open status of the connected detector/switch is considered normal.
- Normally Closed: The closed status of the connected detector/switch is considered normal. This is the default.



5. To set the Normal state for channel 2, repeat Step 4 for adjusting the other dip switch's setting.
6. Install back the dip switch cover.

Note: The dip switch setting must be properly configured, or the sensor LED may be incorrectly lit in the Normal state.

Contact Closure Sensor LEDs

DPX-CC2-TR is equipped with the LEDs for showing the state of the connected detectors/switches.

The LED is lit when the associated detector/switch is in the "abnormal" state, which is the opposite of the Normal state. See **Configuring a Contact Closure Sensor** (on page 28) for how to set the Normal state.

The meaning of a lit LED varies depending on the Normal state settings.

- **When the Normal state is set to Closed:**

LED	Sensor state
Not lit	Closed
Lit	Open

- **When the Normal state is set to Open:**

LED	Sensor state
Not lit	Open
Lit	Closed

How to Connect Differential Air Pressure Sensors

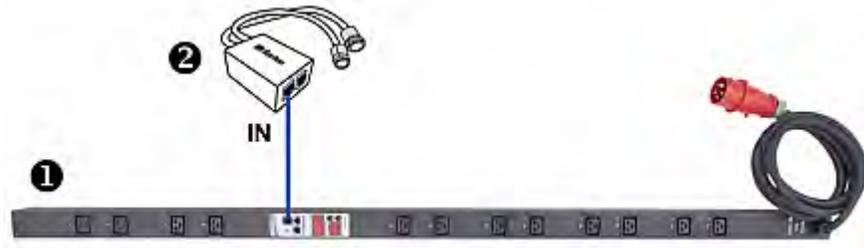
You can have a Raritan differential air pressure sensor connected to the Dominion PX device if the differential air pressure data is desired.

With this sensor, the temperature around the sensor can be also detected through a temperature sensor implemented inside it.

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

1. Plug one end of a Raritan-provided phone cable to the port labeled "Feature" on the Dominion PX device.
2. Plug the other end of this phone cable to the IN port of the differential air pressure sensor.

❶	The Dominion PX device
❷	The Raritan differential air pressure sensor



Chapter 4 Using the PDU

This chapter explains how to use the Dominion PX device. It describes the LEDs and ports on the PDU, and explains how to use the LED display panel. It also explains how the circuit breaker (overcurrent protector) works and when the beeper sounds.

In This Chapter

Panel Components	31
Circuit Breaker	36
Beeper	38

Panel Components

The Dominion PX 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
- On 1U and 2U models, there is an additional component -- a blue power LED.

Blue LED

Only 1U and 2U models have a blue power LED on the right side of the front panel. This LED is lit solid as soon as the Dominion PX device is powered on.

Power Cord

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

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

There is no power switch on the Dominion PX 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. A small LED is adjacent to each outlet to indicate the outlet or PDU state. The PDU is shipped from the factory with all outlets turned ON. The table below explains how to interpret different outlet LED states.

LED state	Outlet status	What it means
Not lit (light grey)	Powered OFF	The outlet is not connected to power, or the control circuitry's power supply is broken.
Red	ON and LIVE	LIVE power. The outlet is on and power is available.
Red flashing	ON and LIVE	The current flowing through the outlet is greater than the upper warning (non-critical) threshold.
Green	OFF and LIVE	The outlet is turned off and power is available when the outlet is turned on.
Green flashing	OFF and NOT LIVE	The outlet is turned off and power is not available because the circuit breaker has tripped.
Yellow flashing	ON and NOT LIVE	The outlet is turned on but power is not available because a circuit breaker has tripped.
Cycling through Red, Green and Yellow	n/a	The Dominion PX device has just been plugged in and its management software is loading. -- OR -- A firmware upgrade is being performed on the device.

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

Connection Ports

The three ports, from left to right, are labeled as Serial (RJ-45), Feature (RJ-12), and LAN (Ethernet, RJ-45). The table below explains what each port is used for.

Port	Used for...
Serial	Establishing a serial connection between a computer and the Dominion PX device: Take the null-modem cable that was shipped with the Dominion PX device, connect the end with the RJ-45 connector to the RS-232 serial port on the front of the Dominion PX device, and connect the end with the DB9F connector to

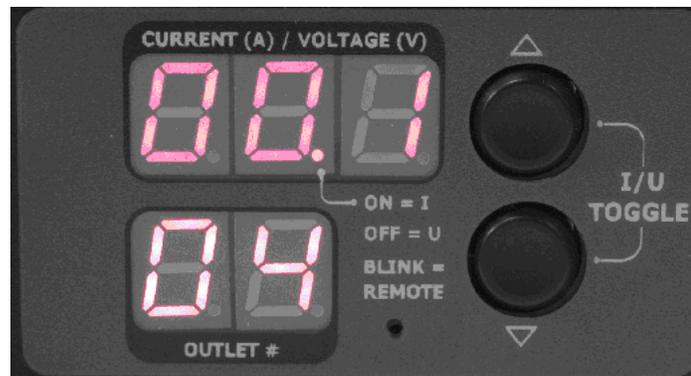
Port	Used for...
	<p>the serial (COM) port on the computer.</p> <p>The serial port is also used to interface with some Raritan access products (such as the Dominion KX) through the use of a power CIM.</p>
Feature	Connection to Raritan's environmental sensors.
LAN	<p>Connecting the Dominion PX device to your company's network:</p> <p>Connect a standard Cat5e/6 UTP cable to this port and connect the other end to your network. This connection is necessary to administer or access the Dominion PX device remotely using the web interface.</p> <p>There are two small LEDs adjacent to the port:</p> <ul style="list-style-type: none"> ▪ Green indicates a physical link and activity. ▪ Yellow indicates communications at 10/100 BaseT speeds.

Note: Connecting any power CIM except for the D2CIM-PWR (such as P2CIM-PWR) to the Dominion PX serial port causes all outlets to switch ON state, even if they were previously OFF.

LED Display

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

The following picture shows the LED display.



The LED display consists of:

- A row displaying three digits
- A row displaying two digits
- Up and Down buttons

Three-Digit Row

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

- Current, voltage, or active power of the selected outlet
- Current of the selected line or circuit breaker
- The text "FuP," which indicates that the **F**irmware **uP**grade is being performed
- The text "CbE," which indicates the circuit breaker associated with the selected outlet has tripped
- For unbalanced load on a three-phase PDU:
 - The text "nE," which indicates the unbalanced load feature is **not Enabled**.

*Note: To enable the unbalanced load detection, see **Enabling Unbalanced Load Detection** (on page 94).*

- The text "nA," which indicates the unbalanced load reading is **not Available** because there is no load connected to the selected outlet/inlet.

Two-Digit Row

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

- Two-digit numbers: This indicates the selected outlet. For example, 03 indicates outlet 3.
- C_x: This indicates the selected circuit breaker, where *x* is the circuit breaker number. For example, C1 represents Circuit Breaker 1.
- L_x: This indicates the selected line of a single-inlet PDU, where *x* is the line number. For example, L2 represents Line 2.

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

- uL: This represents the inlet's **Unbalanced Load**, which is only available for a three-phase PDU.

*Note: To enable the unbalanced load detection, see **Enabling Unbalanced Load Detection** (on page 94).*

- For a three-phase inline monitor:
 - *x*a: This indicates either the L1 current, or L1-N or L1-L2 voltage of the selected outlet/inlet, where *x* is the outlet/inlet number. For example, 3a represents the outlet/inlet 3's L1 current, or L1-N or L1-L2 voltage.

- **xb:** This indicates either the L2 current, or L2-N or L2-L3 voltage of the selected outlet/inlet, where *x* is the outlet/inlet number. For example, 1b represents the outlet/inlet 1's L2 current, or L2-N or L2-L3 voltage.
- **xc:** This indicates either the L3 current, or L3-N or L3-L1 voltage of the selected outlet/inlet, where *x* is the outlet/inlet number. For example, 2c represents the outlet/inlet 2's L3 current, or L3-N or L3-L1 voltage.
- **xU:** This indicates the unbalanced load of the selected outlet/inlet, where *x* is the outlet/inlet number. For example, 1U represents the outlet/inlet 1's unbalanced load.
- **xP:** This indicates the active power of the selected outlet/inlet, where *x* is the outlet/inlet number. For example, 1P represents the outlet/inlet 1's active power.

For information on in-line monitors, see ***In-line Monitors*** (see "***In-line Monitors***" on page 194).

Automatic Mode

When left alone, the LED display cycles through the line readings and circuit breaker readings, as available for your Dominion PX model. This is the Automatic Mode.

Manual Mode

You can press the Up or Down button to enter the Manual Mode so that a particular outlet, line or circuit breaker can be selected to show specific readings.

► **To operate the LED display:**

1. Press the Up or Down button until the desired outlet, line or circuit breaker number is selected in the two-digit row.
 - Pressing the Up button moves up one selection.
 - Pressing the Down button moves down one selection.
2. Current of the selected component is shown in the three-digit row. It appears in this format: XX.X (A).
3. If you select an outlet, you can press the Up and Down buttons simultaneously to switch between the voltage, active power and current readings.
 - The voltage appears in this format: XXX (V). It is displayed for about five seconds, after which the current reading re-appears.
 - The active power appears in this format: X.XX (W). It is displayed for about five seconds, after which the current reading re-appears.

Tip: A quick way to distinguish between voltage, current, and power is the placement of the decimal point in the display. Voltage has no decimal point, active power has a decimal point between the first and second digits, and current has a decimal point between the second and third digits.

Note: The LED display returns to the Automatic Mode after 10 seconds elapse since the last time any button was pressed.

Reset Button

The reset button is located inside the small hole near the two-digit row.

Pressing this reset button restarts the Dominion PX device's software without any loss of power to outlets. It does not reset the Dominion PX device to factory defaults.

*Tip: To reset the PDU to factory defaults, see **Resetting to Factory Defaults** (on page 267).*

Circuit Breaker

The Dominion PX models rated over 20A (North American) or 16A (international) contain branch circuit breakers. These circuit breakers automatically trip (disconnect power) when the current flowing through the circuit breaker exceeds its rating.

If the circuit breaker switches off power, the LED display shows:

- CbE, which means "circuit breaker error," in the three-digit row.
- The lowest outlet number affected by the circuit breaker error in the two-digit row.

You are still able to switch between outlets on the LED display when the circuit breaker error occurs. Outlets affected by the error show CbE. Unaffected outlets show the current and voltage readings as described in **Manual Mode** (on page 35).

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.

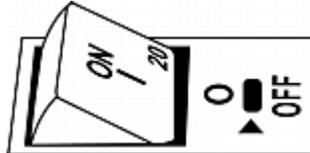
Depending on the model you purchased, the circuit breaker may use a button- or handle-reset mechanism.

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 the breaker has tripped.



2. Examine your Dominion PX device 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.

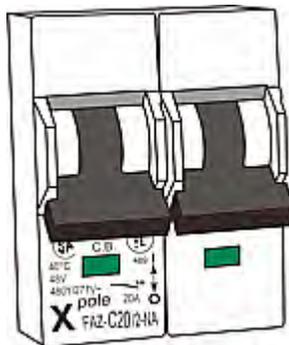


Resetting the Handle-Type Circuit Breaker

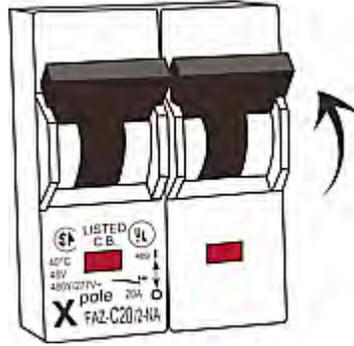
Your handle-type circuit breakers may look slightly different from the images shown in this section, but the reset procedure remains the same.

► **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 the breaker has tripped.



3. Examine your Dominion PX device 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.



Beeper

The Dominion PX includes a beeper to issue an audible alarm when a significant situation occurs.

- The beeper sounds an alarm within 3 seconds of a circuit breaker trip.
- It also sounds an alarm when the control board temperature sensor reaches the non-critical threshold -- default is 65 degrees Celsius (149 degrees Fahrenheit).

*Note: The temperature thresholds are factory defaults and can be user-configurable. See **Setting PDU Thresholds and Hysteresis** (on page 91).*

The beeper stops ringing after the significant situation disappears.

- The beeper stops as soon as all circuit breakers have been reset.
- If the alarm is caused by the control board's high temperature, it stops after the control board temperature sensor drops below the non-critical threshold.

A Note about the Non-Critical Temperature Threshold Alarm

The Dominion PX automatically shuts down its CPU when the control board temperature sensor reaches 87 degrees Celsius (188.6 degrees Fahrenheit). In order to alert you of the impending critical thermal shutdown issue for handling the situation promptly, the beeper sounds an alarm once the temperature sensor reaches the non-critical threshold.

Chapter 5 Using the Web Interface

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

In This Chapter

Logging in to the Web Interface	39
Web Interface Elements	42
Using the Home Page	48
Measurement Accuracy	52
Managing the Dominion PX.....	52
Setting Up User Profiles	75
Setting Up User Groups	80
Setting Up and Managing Outlets	84
Setting Up Power Thresholds and Hysteresis.....	91
Monitoring Line and Circuit Breaker Status.....	93
Access Security Control	97
Setting Up a Digital Certificate.....	108
Setting Up External User Authentication	112
Environmental Sensors	118
Configuring and Using Alert Notifications.....	131
Setting Up Event Logging.....	144
Outlet Grouping	151
Setting the FIPS Mode	156
Diagnostics	158
Using Online Help.....	163

Logging in to the Web Interface

To log in to the web interface, you must enter a user name and password. The first time you log in to the Dominion PX, use the default user name (admin) and password (raritan). You are then prompted to change the password for security purposes.

After successfully logging in, you can create user profiles for your other users. These profiles define their login names and passwords. See **Creating a User Profile** (on page 75).

Login

► **To log in to the web interface:**

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

http(s)://<ip address>

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

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

Please enter Username and Password

Username:

Password:

3. Type your user name and password in the Username and Password fields.

Note: Both the user name and password are case sensitive, so make sure you capitalize them correctly.

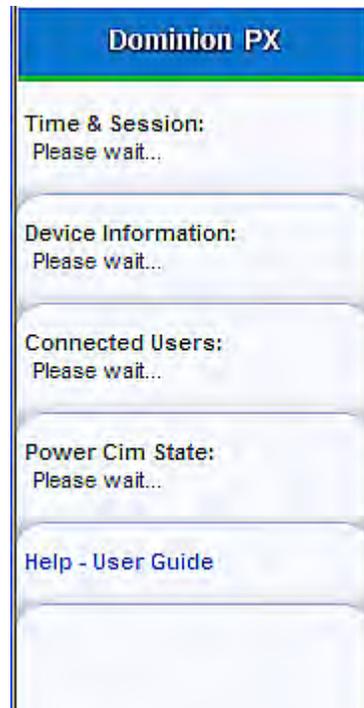
4. Click Login. The Home page opens.

Name	State	Control	RMS Current	Active Power	Group Member
Outlet 1	on	On OFF Cycle	0.00 Amps	0 Watts	no
Outlet 2	on	On OFF Cycle	0.00 Amps	0 Watts	no
Outlet 3	on	On OFF Cycle	0.00 Amps	0 Watts	no
Outlet 4	on	On OFF Cycle	0.00 Amps	0 Watts	no
Outlet 5	on	On OFF Cycle	0.00 Amps	0 Watts	no
Outlet 6	on	On OFF Cycle	0.00 Amps	0 Watts	no
Outlet 7	on	On OFF Cycle	0.00 Amps	0 Watts	no
Outlet 8	on	On OFF Cycle	0.00 Amps	0 Watts	no
Outlet 9	on	On OFF Cycle	0.00 Amps	0 Watts	no

Note: Depending on your model type and hardware configuration, elements shown on your Home page may appear differently from this image.

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

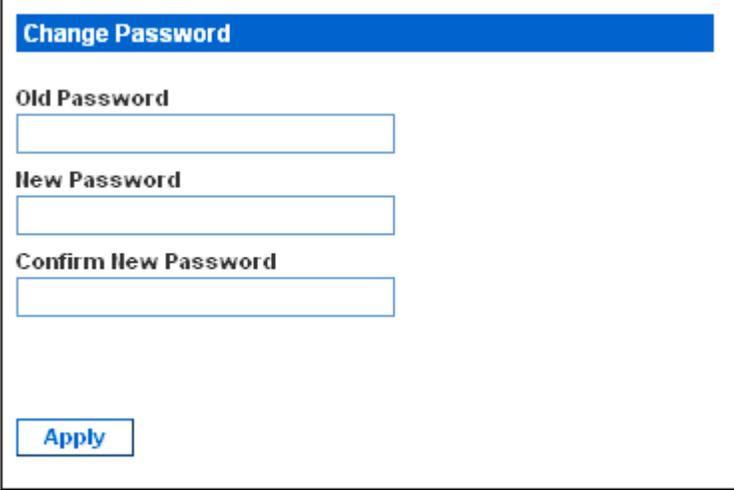
You must enable JavaScript in the web browser for proper operation. If Java Script is not enabled, features such as the Status Panel on the left side of the interface does not display correctly.



Changing Your Password

► **To change your password:**

1. Choose User Management > Change Password. The Change Password page opens.



The screenshot shows a web interface titled "Change Password". It features three input fields: "Old Password", "New Password", and "Confirm New Password". Below these fields is an "Apply" button.

2. Type the current password in the Old Password field.
3. Type your new password in the New Password and Confirm New Password fields. Passwords are case sensitive.
4. Click Apply. Your password is changed.

Web Interface Elements

Every page in the web interface provides menus and a navigation path across the top and a Status panel to the left.

Menus

There are several menus in the web interface, each with their own set of menu items:

Details
Outlet Details
Line Details
CB Details
PDU Details
Outlet Setup

Alerts

Alert Configuration
Alert Policies
Alert Policy Editor
Alert Destinations

User Management

Change Password
Users & Groups
User/Group System Permissions
User/Group Outlet Permissions

Device Settings

PDU Setup
Network
Security
Certificate
Date/Time
Authentication
SMTP Settings
SNMP Settings
Event Log
FIPS Setting

External Sensors

External Sensors Details
External Sensors Setup

Maintenance

Device Information
View Event Log
Update Firmware
Bulk Configuration
Unit Reset

Outlet Groups

Outlet Group Details

Outlet Group Devices
Outlet Group Editor
Diagnostics
Network Interface
Network Statistics
Ping Host
Trace Route to Host
Device Diagnostics
Help
About Dominion PX

► **To select a menu item:**

There are two ways to select an option from a menu:

- Click the menu name to display a page listing each menu item, and then click the item you want to select.

Note: The Home tab is not a menu. Clicking the Home tab takes you back to the Dominion PX Home page.

- Position the cursor on the menu name. A list of menu items drops down from the menu. Slide the cursor to the item you want and click it to select it.

Navigation Path

When you select an item from a menu and navigate to a specific page, the system displays a navigation path across the top that shows the menu and menu item you selected to get there.

For example, if you choose User Management > User/Group System Permissions, the navigation path looks like the following example.



To return to a previous page, click the page name in the navigation path. Every navigation path begins at the Home page, so a single click always takes you back to the Home page from anywhere in the interface. You can click the Home tab from any page to take you back to the Home page.

Status Panel

The Status panel appears on the left of every page in the interface. It shows:

- Present date and time
- Information about the user, including:
 - User name
 - User's present state (active, idle, and so on)
 - IP address of the user's computer
 - Date and time of the user's last login
- Information about the Dominion PX device, including:
 - PDU name
 - Model name and number
 - IP address
 - Firmware version
 - Firmware status
 - FIPS mode enabled (displayed in blue) or disabled (displayed in black)

- Information about all the users currently connected, including user name, IP address, and present state. Your active session is included in this list.
- Status of Dominion PX's serial port, indicating whether the serial port is supplying power to the connected Raritan power CIM, such as D2CIM-PWR
- A link to the User Guide on the Raritan website



The screenshot displays the Dominion PX web interface. At the top, there is a blue header with the text "Dominion PX". Below the header, the interface is divided into several sections:

- Time & Session:** 2012-01-30 13:39
User : admin
State : active
Your IP : 192.168.80.86
Last Login : 2012-01-30 13:21
- Device Information:**
Name: PNN1234567
Model: PX (PX-4080T)
IP Address: 192.168.80.65
Firmware: 01.05.05
Firmware Status: OK
FIPS mode is not set
- Connected Users:**
admin (192.168.80.86)
active
- Power Cim State:**
Power CIM is enabled

At the bottom of the interface, there is a blue link labeled "Help - User Guide".

The State field in the user information section considers a user to be "idle" 30 seconds after the last keyboard or mouse action. It then updates the idle time every 10 seconds until another keyboard or mouse action is detected.

If you exceed the idle time limit (by default, 15 minutes), you are logged out and re-directed to the login page automatically.

Important: Users still appear in the Connected Users list if they end their session by closing their browser window without logging off. The Dominion PX removes their names when their sessions reach the idle time limit.

*Note: If any PSoC update failure occurs during the firmware upgrade process, the failure is reported in the status panel. See **PSoC Firmware Upgrade Failure** (on page 70).*

Status Messages

When you perform an operation from the web interface, such as creating a user profile or changing a network setting, a message appears at the top of the page indicating whether or not the operation was successful. Be sure to check this message to confirm that an operation was successful.

Successful Messages

The following is an example of a status message after an operation has completed successfully:

[Home](#) > [Device Settings](#) > [Network Settings](#)

Operation completed successfully.

Unsuccessful Messages

The following is an example of a status message after an operation has completed unsuccessfully:

[Home](#) > [Alerts](#) > [Alert Destinations](#)

Error: The 'PET alert target IP' is too long. Maximum length is 15 characters.

Unavailable Options

Sometimes certain actions are unavailable. When this occurs, the appropriate buttons are non-functional, though different browsers may display this differently. For example, if you select the Admin User Group in Internet Explorer, the buttons for Copy, Modify, and Delete are grayed-out since you cannot Copy, Modify, or Delete the Admin user group. In Firefox, these buttons appear normal, but are unclickable.

Reset to Defaults

Many pages provide a Reset to Defaults button that returns all fields to their default values. If you use this button, you must click the Apply button afterward to save the defaults. If you do not, these fields retain the non-default values.

Default Asterisk

If a field has an asterisk after it, as shown below,

HTTP Port
 *

then this field is currently set to its default value. If you change the default, the asterisk disappears. If you reset it to the default, the asterisk returns.

Refresh

Many pages provide a Refresh button. If a page is open for a while, the information displayed may become "stale." Click this button periodically to reload the page and update the information displayed.

Using the Home Page

The Home page is the first page to appear after a successful login. It consists of a Lines Status Display, Circuit Breaker Status (if applicable), an Outlets list, and an All Outlets Control panel. The page also contains an External Sensors panel when environmental sensors are connected to the Dominion PX. The Home page refreshes every 30 seconds to keep the data displayed up to date.

You can return to the Home page from any other page in the web interface by clicking:

- The Home tab at the top of the interface
- The Home link in the navigation path
- The Raritan logo in the upper left of the window
- The Device Model Name under the logo

Line Loads Display

The Line Loads display shows the current load on each of the Dominion PX's current-carrying lines.

Line Loads	
Line 1:	1.08 Amps
Line 2:	1.05 Amps
Line 3:	1.05 Amps

The status of each line is represented by a status bar. As the load on the line increases, the colored portion grows to fill the bar. A status bar that is nearly full indicates that the particular line is approaching its rated current limit. The colored portion of the bar also changes colors as the load crosses configured thresholds.

For more information on the status of each line, choose Details > Line Details.

Circuit Breaker Status

For Dominion PX models with circuit breakers, a circuit breaker status display appears on the Home page. This provides a quick view of each circuit breaker's status and the current handled by each circuit breaker.

Circuit Breakers			
	Circuit Breaker 1	Circuit Breaker 2	Circuit Breaker 3
Status:	Closed	Closed	Closed
Current Drawn:	0.62 Amps	0.61 Amps	0.62 Amps

A status of Closed indicates that the circuit is closed and functioning properly. A status of Open and a change in color indicates that a circuit breaker has tripped.

For details on each circuit breaker, choose Details > CB Details.

Tip: The most efficient use of the Dominion PX occurs when current loads are balanced between all circuit breakers. Using the Outlet Mapping on the CB Details page, and the Circuit Breaker status on the Home Page, you can arrange where devices are plugged into the Dominion PX in order to maintain that balance.

Note: The current drawn through a circuit breaker indicates the amount of current flowing to a bank of outlets. In three-phase Dominion PX models, this number does not match the current draw on each line since each bank of outlets is tied to two lines.

Outlets List

The Outlets list displays each outlet on the Dominion PX device as a table row with a view of the power status, the RMS current, and the RMS Power through the individual outlet.

Name	State	Control			RMS Current	Active Power	Group Member
Outlet 1	on	<input type="button" value="On"/>	<input type="button" value="Off"/>	<input type="button" value="Cycle"/>	0.00 Amps	0.00 Watts	no
Outlet 2	on	<input type="button" value="On"/>	<input type="button" value="Off"/>	<input type="button" value="Cycle"/>	0.80 Amps	10.63 Watts	no
Outlet 3	on	<input type="button" value="On"/>	<input type="button" value="Off"/>	<input type="button" value="Cycle"/>	0.00 Amps	0.00 Watts	no
Outlet 4	on	<input type="button" value="On"/>	<input type="button" value="Off"/>	<input type="button" value="Cycle"/>	0.80 Amps	4.57 Watts	no
Outlet 5	on	<input type="button" value="On"/>	<input type="button" value="Off"/>	<input type="button" value="Cycle"/>	0.80 Amps	2.68 Watts	no
Outlet 6	on	<input type="button" value="On"/>	<input type="button" value="Off"/>	<input type="button" value="Cycle"/>	0.72 Amps	24.73 Watts	no
Outlet 7	on	<input type="button" value="On"/>	<input type="button" value="Off"/>	<input type="button" value="Cycle"/>	0.35 Amps	2.35 Watts	no
Outlet 8	on	<input type="button" value="On"/>	<input type="button" value="Off"/>	<input type="button" value="Cycle"/>	0.62 Amps	1.32 Watts	no

Note: RMS refers to Root Mean Square, a statistical method for measuring certain types of variables. In this context, it gives the value of current that is equivalent to a DC value.

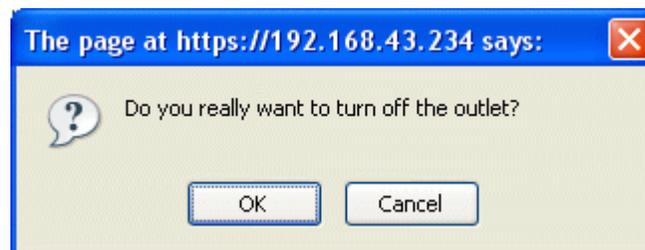
Turning an Outlet On, Off, or Cycling the Power

You can use the outlets list on the Home page to control the power state of individual outlets.

Note: Not all Dominion PX models support the outlet switching function, such as PX-4nnn or PX-3nnn, where n is a number.

► To turn an outlet on, off, or cycle the power

1. Click On, Off, or Cycle.
2. A dialog for confirming the operation appears. Click OK and the outlet switches ON, OFF, or cycles its power.



*Tip: You can also turn an outlet on or off or power cycle it from the Outlet Details page. See **Turning an Outlet On or Off** (on page 90) and **Power Cycling an Outlet** (on page 90).*

Displaying Additional Details

To display additional details about an outlet, click the outlet name. This displays the Outlet Details page. This page shows the name, status and line pair of the outlet, as well as:

- RMS Current
- Power Factor
- Maximum RMS Current
- Voltage
- Active Power
- Apparent Power
- Active Energy (applicable on some models following the PX-nnnn format, where n is a number)

Note: RMS refers to Root Mean Square, a statistical method for measuring certain types of variables. In this context, it gives the value of current that is equivalent to a DC value.

All Outlets Control

The All Outlets Control panel at the bottom of the Home page allows you to turn all outlets ON and OFF. Users must have permission to access all outlets in order to use All Outlets Control.

► **To control all outlets:**

1. Locate the All Outlets Control panel.
2. Click On to turn all outlets ON, or click Off to turn all outlets OFF.
3. A dialog for confirming the operation appears. Click OK to confirm the operation.



Note: Not all Dominion PX models support the outlet switching function, such as PX-4nnn or PX-3nnn, where n is a number.

Measurement Accuracy

- Voltage (per outlet): Range 0-255V, +/-5%, resolution 1V
- Current (per outlet): Range 0-25A, +/-5%, resolution 0.01A

Tip: Active Energy per outlet is available using either the web interface or command line interface except for the models with these prefixes: DPCS, DPCR, DPXR and DPXS. The Active Energy accuracy is +/-1%, but can be over +/-1% when the connected load is 0.15A or less. For DPCS, DPCR, DPXR and DPXS models, Active Power (Watts) per outlet, instead of Active Energy (kWh), is reported.

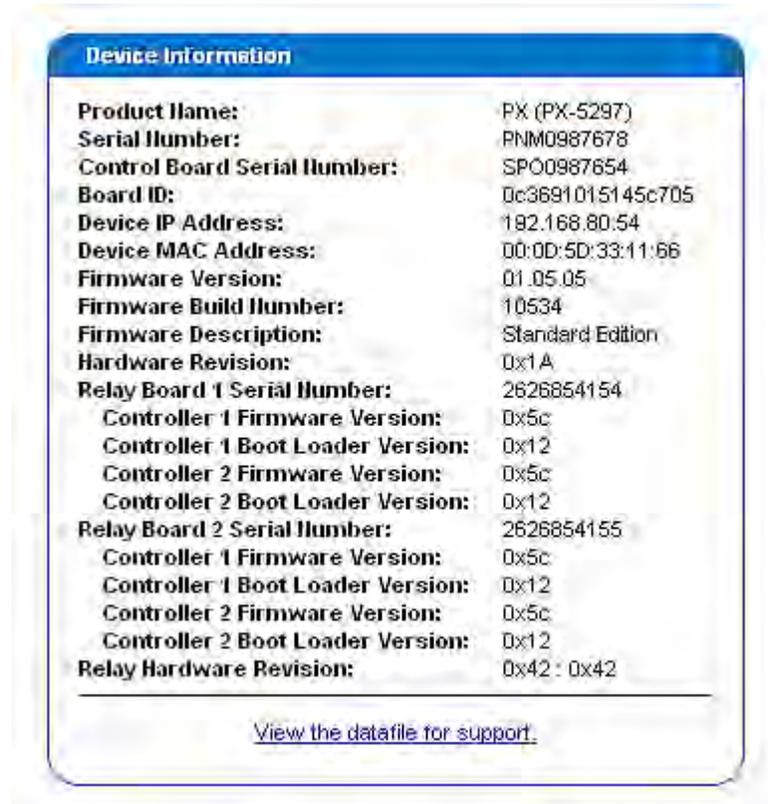
Managing the Dominion PX

You can display basic device information about the Dominion PX device, give it a new device name, and modify any of the network settings that were entered during the initial configuration process. You can also set the device's date and time and configure its SMTP settings so it can send email messages when alerts are issued.

Displaying Basic Device Information

► **To display basic information about a Dominion PX device:**

1. Choose Maintenance > Device Information. The Device Information page opens.



- The Device Information panel displays the product name, serial number, and IP and MAC addresses of the Dominion PX device, as well as detailed information about the firmware running in the PDU.
- To open or save an XML file providing details for Raritan Technical Support, click the "View the datafile for support" link.

*Tip: Below the Device Information panel is the Model Configuration panel. See **Displaying Model Configuration Information** (on page 53).*

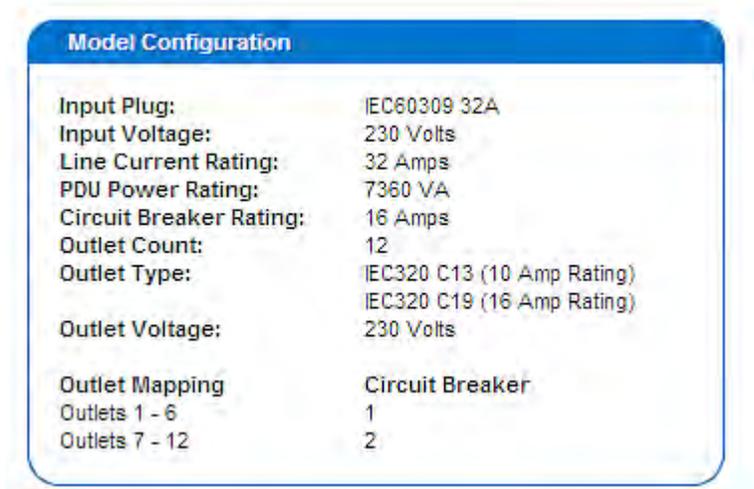
Displaying Model Configuration Information

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

► **To display the Model Configuration panel:**

- Choose Maintenance > Device Information. The Device Information page opens.

- Information about your model is shown in the Model Configuration Panel below the Device Information panel.



Model Configuration	
Input Plug:	IEC60309 32A
Input Voltage:	230 Volts
Line Current Rating:	32 Amps
PDU Power Rating:	7360 VA
Circuit Breaker Rating:	16 Amps
Outlet Count:	12
Outlet Type:	IEC320 C13 (10 Amp Rating) IEC320 C19 (16 Amp Rating)
Outlet Voltage:	230 Volts
Outlet Mapping	Circuit Breaker
Outlets 1 - 6	1
Outlets 7 - 12	2

This panel shows:

- The input voltage and plug type
- The PDU's maximum RMS current and power rating
- The outlet information, including total number of outlets, outlet types and outlet voltage
- The outlets governed by each circuit breaker (if available)

*Tip: Above the Model Configuration panel is the Device Information panel. See **Displaying Basic Device Information** (on page 52).*

Naming the Dominion PX Device

By default, the Dominion PX has a device name of its serial number. You may want to give it a more recognizable name for identification.

The PDU's default host name is identical to the device name. Assign a different host name if necessary.

► **To name the Dominion PX device:**

1. Choose Device Settings > Network. The Network Settings page opens. The left side of the page consists of the Basic Network Settings panel, which contains the device name.

Basic Network Settings

Device Name
pdu *

IP Auto Configuration
DHCP *

Preferred Host Name (DHCP only)
*

IP Address
192.168.50.214

Subnet Mask
255.255.255.0 *

Gateway IP Address
192.168.50.126

Primary DNS Server IP Address
192.168.50.114

Secondary DNS Server IP Address
192.168.50.115

2. Type a new name (up to 255 characters) in the Device Name field.
3. If DHCP is selected for IP configuration, the name entered in the field of Preferred Host Name (DHCP only) is registered with DNS and used on the assigned IPs by DHCP.
4. Click Apply. The Dominion PX device is renamed.

Tip: Device name shown in the web interface should be identical to the SNMP system name. However, the SNMP system name becomes inconsistent with the device name when the device name is changed. To make both names identical, you must restart the Dominion PX device or restart the SNMP agent after changing the device name in the web interface.

Modifying the Network Settings

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

► **To modify the network settings:**

1. Choose Device Settings > Network. The Network Settings page opens. The left side of the page consists of the Basic Network Settings panel, which shows the current network settings. See **Naming the Dominion PX Device** (on page 55) for details on this panel.
2. Do either of the following:
 - Auto configuration: To auto-configure the Dominion PX device, select DHCP or BOOTP from the IP Auto Configuration drop-down list.
 - With DHCP selected, you can enter a preferred DHCP host name, which is optional.
 - Static IP: To enter a static IP address, select None from the IP Auto Configuration drop-down list, and then enter:
 - IP address
 - Subnet mask
 - Gateway address
 - Primary and (optional) secondary DNS servers' addresses
3. When you are finished, click Apply. The network settings are modified.

Role of a DNS Server

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

Therefore, DNS server settings are important for LDAP authentication. With appropriate DNS settings, the Dominion PX can resolve the LDAP server's name to an IP address for establishing a connection. If the *SSL encryption* is enabled, the DNS server settings become critical since only fully qualified domain name can be used for specifying the LDAP server.

For information on LDAP authentication, see **Setting Up LDAP Authentication** (on page 114).

Modifying the Network Service Settings

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

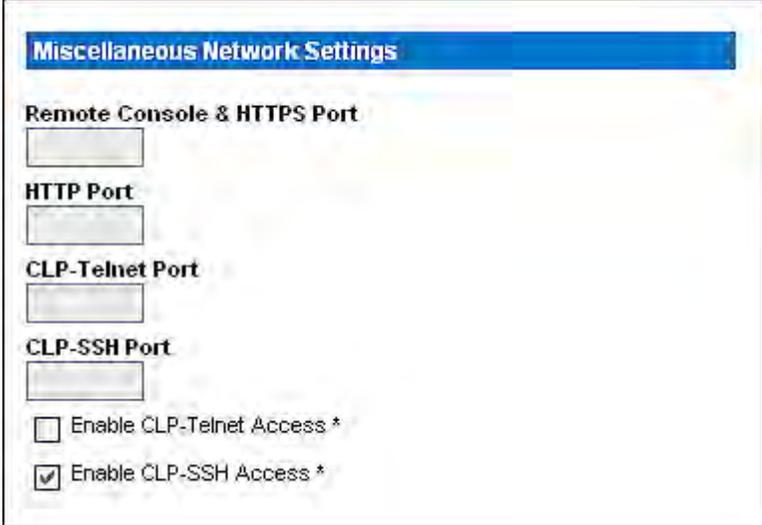
HTTPS and HTTP enable the access to the web interface, and Telnet and SSH enable the access to the **command line interface** (see "**Using the CLP Interface**" on page 180).

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.

► **To configure network communication services:**

1. Choose Device Settings > Network. The Network Settings page opens. The Miscellaneous Network Settings panel on the top right contains the communications, port, and bandwidth settings.



2. By default, CLP-Telnet is disabled and CLP-SSH is enabled. To change this, select or deselect either checkbox.

*Note: In the FIPS mode, the Telnet access is NOT supported so its settings become unavailable. See **FIPS Limitations** (on page 156).*

3. To use a different port for HTTPS, HTTP, Telnet, or SSH service, type a new port number in the corresponding text box. Valid range is 1 to 65535.

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

- When you are finished, click Apply. The settings are modified.

Modifying the LAN Interface Settings

The LAN interface speed and duplex mode were set during the installation and configuration process. See *Initial Network and Time Configuration* (on page 19).

► **To modify either setting:**

- Choose Device Settings > Network. The Network Settings page opens. The LAN Interface Settings panel on the bottom right shows the interface speed and duplex mode.

LAN Interface Settings

Current LAN Interface Parameters:
autonegotiation on, 100 Mbps, full duplex, link ok

LAN Interface Speed
Autodetect ▼

LAN Interface Duplex Mode
Autodetect ▼ *

- To change the LAN speed, select a different option in the LAN Interface Speed field.
 - Autodetect: System determines the optimum LAN speed through auto-negotiation.
 - 10 Mbps: The LAN speed is always 10 Mbps.
 - 100 Mbps: The LAN speed is always 100 Mbps.
- To change the duplex mode, select a different option in the LAN Interface Duplex Mode field.
 - Autodetect: The Dominion PX selects the optimum transmission mode through auto-negotiation.
 - Half duplex: Data is transmitted in one direction (to or from the Dominion PX device) at a time.
 - Full duplex: Data is transmitted in both directions simultaneously.
- When you are finished, click Apply. The settings are modified.

Setting the Date and Time

Set the internal clock on the Dominion PX device manually, or link to a Network Time Protocol (NTP) server and let it set the date and time for the Dominion PX.

Important: If you are using Raritan's Power IQ to manage the Dominion PX, you must configure Power IQ and the Dominion PX to have the same

date/time or NTP settings.

► **To set the date and time:**

1. Choose Device Settings > Date/Time. The Date/Time Settings page opens.

Date/Time Settings

Time Zone
Europe/London *

Adjust for daylight savings time †
 User specified time *

Date
2012 - 1 - 30 (yyyy-mm-dd)

Time
13 : 26 : 24 (hh:mm:ss)

Synchronize with NTP server
 Use NTP Servers provided by DHCP/BOOTP †

Primary Time Server
*

Secondary Time Server
*

If Use NTP Servers provided by DHCP/BOOTP is selected, the NTP Server configuration is obtained automatically. If DHCP/BOOTP do not provide NTP servers or if static IP is used, system will use user defined NTP servers.

* Stored value is equal to the default.

2. Enter a time zone by selecting an appropriate option from the Time Zone drop-down list. For example, select America/Antigua if you are located in Antigua.
3. Choose one of the methods to set the date and time:
 - To customize the date and time, select the User Specified Time radio button, and then enter the date and time in appropriate fields. Use the yyyy-mm-dd format for the date and the hh:mm:ss format for the time.

- To let an NTP server set the date and time, select the "Synchronize with NTP Server" radio button. There are two scenarios for this setting:
 - To use the DHCP- or BOOTP-assigned NTP servers only, select the "Use NTP Servers provided by DHCP/BOOTP" checkbox, and leave the Primary and Secondary Time Server fields blank. The NTP servers will be automatically discovered.
 - To make the DHCP- or BOOTP-assigned NTP servers the first choice, and the user-specified NTP servers the second choice if the first choice fails, do both of the following:
 - Select the "Use NTP Servers provided by DHCP/BOOTP" checkbox.
 - Specify the NTP servers in the Primary and Secondary Time Server fields.

Then if DHCP/BOOTP provides two NTP servers, both of the user-specified NTP servers are replaced and NOT used. If DHCP/BOOTP provides only one NTP server, only the primary user-specified NTP server is replaced and NOT used. If DHCP/BOOTP provides no NTP servers, both of the user-specified NTP servers are used.

- To use the user-specified NTP servers only, deselect the "Use NTP Servers provided by DHCP/BOOTP" checkbox and specify the NTP server in the Primary Time Server field. A secondary NTP server is optional.
4. Click Apply. The date and time settings are applied.

Specifying the Device Altitude

You must specify the Dominion PX device's altitude above sea level if a Raritan 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 255).

The default altitude measurement unit is meters. You can change to feet if this unit is preferred.

► To specify the altitude of the Dominion PX device:

1. Choose Device Settings > PDU Setup. The PDU Setup page opens.
2. Locate the panel labeled PDU Setup.
3. Select the measurement unit intended for the altitude by clicking one of the radio buttons -- Meters or Feet.
4. Type an integer number in the "Height Above sea level" field. Depending on the measurement unit selected, the range of valid numbers differs.
 - For meters (m), the value ranges between 0 and 3000.

- For feet (ft), the value ranges between 0 and 9842.
5. Click Apply. The settings are modified.

Tip: The device altitude can be also set in meters by using the SNMP set requests.

Configuring the SMTP Settings

The Dominion PX can be configured to send alerts or event messages to a specific administrator by email. To do this, you have to configure the SMTP settings and enter an IP address for your SMTP server and a sender's email address.

*Note: See **Configuring and Using Alert Notifications** (on page 131) for details on configuring alerts to send emails.*

► To configure the SMTP settings:

1. Choose Device Settings > SMTP Settings. The SMTP Settings page opens.

The screenshot shows two panels from a web interface. The left panel, titled "SMTP Settings", contains the following fields: "SMTP Server" with the value "mail.companyname.com", "Sender Email Address" with the value "px-rack1@companyname.com", a checkbox for "SMTP server requires password authentication" which is unchecked, "User Account" with an empty field, and "Password" with an empty field. The right panel, titled "Test SMTP Settings", contains a warning message: "Please ensure you have applied all changes before testing SMTP settings or changes will be lost!". Below the message is a "Receiver Address" field with an empty input box and a "Send" button.

2. Type the IP address of the mail server in the SMTP Server field.
3. Type an email address for the sender in the Sender Email Address field.
4. If your SMTP server requires password authentication, type a user name and password in the User Account and Password fields.
5. Click Apply. Email is configured.
6. Now that you have set the SMTP settings, you can test it to ensure it works properly. To do this, type the receiver's email address in the Receiver Address field and click Send.

Important: Do not test the SMTP settings until you have first applied them. If you do, you will lose the settings and be forced to re-enter them.

Configuring the SNMP Settings

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

► To configure the SNMP communication:

1. Choose Device Settings > SNMP Settings. The SNMP Settings page opens.

SNMP Settings

Enable SHMP Agent *

Enable SHMP v1 / v2c Protocol *

Read Community
 *

Write Community
 *

Enable SHMP v3 Protocol *

Force Encryption *

System Location
 *

System Contact
 *

Click [here](#) to view the PX (PCS20-20) SNMP MIB.

Apply **Reset To Defaults**

2. Select the Enable SNMP Agent checkbox to enable the Dominion PX to communicate with external SNMP managers. A number of options become available.
3. Select the Enable SNMP v1 / v2c Protocol checkbox to enable communication with an SNMP manager using SNMP v1 or v2c protocol. Type the SNMP read-only community string in the Read Community field and the read/write community string in the Write Community field.

*Note: In the FIPS mode, SNMP v1 / v2c protocol is NOT supported so its settings become unavailable. See **FIPS Limitations** (on page 156).*

4. Select the Enable SNMP v3 Protocol checkbox to enable communication with an SNMP manager using SNMP v3 protocol.

- Additionally, select the Force Encryption checkbox to force using encrypted SNMP communication.

In the FIPS mode, this encryption checkbox is automatically selected when you enable the SNMP v3 protocol. See **FIPS Limitations** (on page 156).

Note: To perform SNMP v3 operations successfully, make sure the name of your user group does NOT contain any spaces.

5. Type the SNMP MIBII sysLocation value in the System Location field.
6. Type the SNMP MIBII sysContact value in the System Contact field.
7. Click on the link at the bottom of the page to download an SNMP MIB for your Dominion PX to use with your SNMP manager.
8. Click Apply. The SNMP configuration is set.

Enabling Data Retrieval

The data retrieval feature allows the retrieval of the Dominion PX data by an SNMP manager, such as the data of PDU, outlet, line, and circuit breaker. When enabled, the Dominion PX measures all sensor data at regular intervals and stores these data samples for access over SNMP.

The Dominion PX stores up to the last 120 measurements (samples) in the data log buffer.

Configuring the delay between samples adjusts how often the sample measurements are made and stored for retrieval. The default delay is 300 seconds. Delays must be entered as multiples of 3 seconds.

The Dominion PX's SNMP agent must be enabled for this feature to work. See **Enabling SNMP** (on page 165) for more details. In addition, using an NTP time server ensures accurately time-stamped measurements.

Note: By default, Data Retrieval is disabled. Users belonging to the Admin user group can enable or disable this feature.

► To configure the data sample delay:

1. Choose Device Settings > PDU Setup. The PDU Setup page opens.

Data Retrieval

Enable Data Retrieval *

Sampling Period

* s Enter an integer multiple of 3 from 3-600.

2. By default, Data Retrieval is disabled. Select the Enable Data Retrieval checkbox, and the Sampling Period field becomes configurable.

3. Type a number in the Sampling Period field, indicating how often (in seconds) the Dominion PX stores data samples. Values in this field are restricted to multiples of 3 seconds, ranging from 3 to 600 seconds (10 minutes).
4. When you finish, click Apply. The retrieved data samples are stored immediately once this feature is enabled and the delay between samples is configured.

After data retrieval is enabled, an external manager or application (such as Raritan's Power IQ) can access the stored data using SNMP. Download the Dominion PX MIB file to assist you in configuring third-party managers to retrieve data. See **Using SNMP** (on page 165) for more details.

*Tip: You can also use the SNMP set requests to enable or disable the data retrieval feature, or set the sampling period. See **Setting Data Retrieval** (on page 173).*

Retrievable Data

The data retrieval feature makes the following types of data available:

- Time stamp indicating when data sample was collected in UTC format
- Unit Active Power, including the average, maximum and minimum
- Unit Apparent Power, including the average, maximum and minimum
- Data for each outlet as shown below:
 - Outlet Number
 - Outlet RMS current, including the average, maximum and minimum
 - Outlet Voltage, including the average, maximum and minimum
 - Outlet Power Factor, including the average, maximum and minimum
 - Outlet Up Time (number of seconds since the outlet was last switched on)
 - Outlet Active Energy, including the average, maximum and minimum
- Data for each circuit breaker as shown below:
 - Circuit breaker number
 - Circuit breaker current, including the average, maximum and minimum
- Data for each inlet pole as shown below:
 - Line identifier
 - Inlet pole RMS current, including the average, maximum and minimum
 - Inlet pole Voltage, including the average, maximum and minimum
 - Inlet pole Active Power, including the average, maximum and minimum
 - Inlet pole Apparent Power, including the average, maximum and minimum

Inlet pole Active Energy, including the average, maximum and minimum

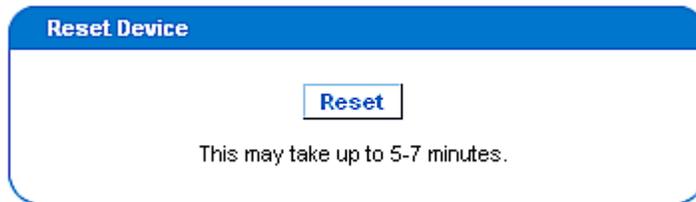
- Data for the inlet as shown below:
 - Inlet load unbalance, including the average, maximum and minimum
 - Inlet Active Power, including the average, maximum and minimum
 - Inlet Apparent Power, including the average, maximum and minimum
 - Inlet Active Energy, including the average, maximum and minimum

Resetting the Dominion PX Device

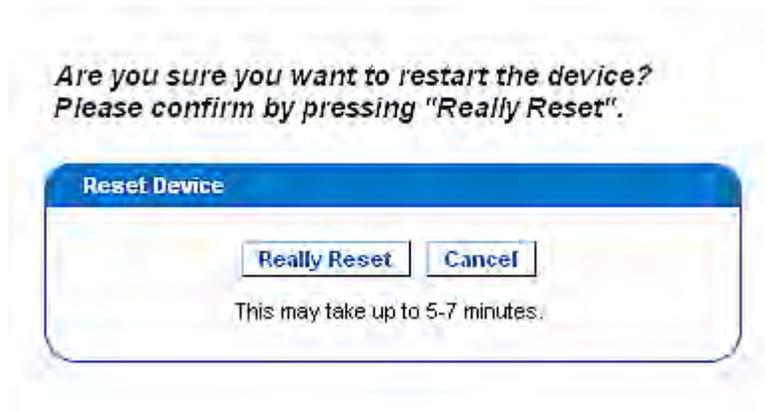
You can remotely reboot the Dominion PX device via the web interface.

► **To reset the Dominion PX device:**

1. Choose Maintenance > Unit Reset. The Reset Operations page opens.

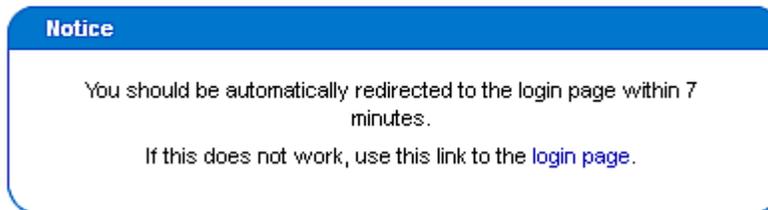


2. Click Reset. A Reset Confirmation page opens.



3. When you click Really Reset, the Dominion PX device reboots. If you change your mind, click Cancel to terminate the reset operation. If you choose to proceed with the reset, the page shown below opens and the reset takes place. The reset takes several minutes to complete.

The device will be reset in a few seconds.



- When the reset is complete, the Login page opens. Now you can log back in to the Dominion PX device.

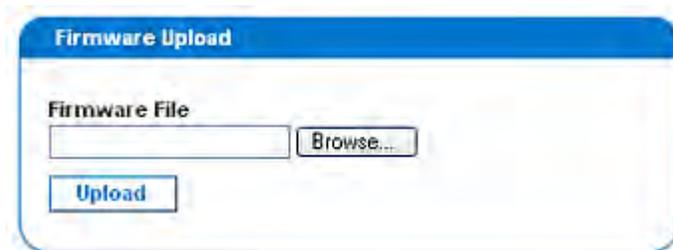
Updating the Firmware

Users must either use the admin account or have both the Firmware Update and Unit Reset privileges in order to successfully update the Dominion PX firmware.

The Dominion PX firmware files are available on the Raritan website's **Firmware and Documentation section** (<http://www.raritan.com/support/firmware-and-documentation/>).

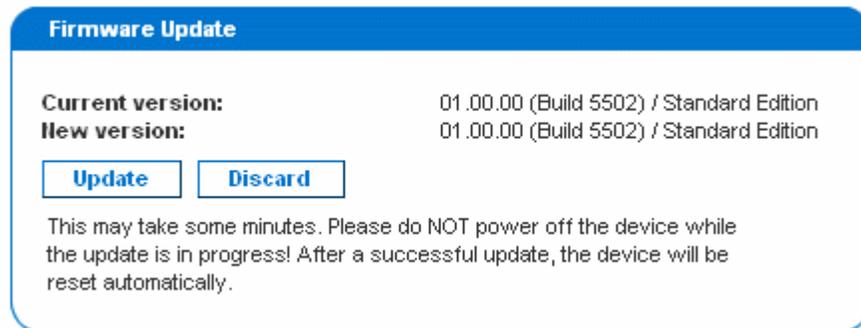
► To update firmware:

- Choose Maintenance > Update Firmware. The Firmware Upload page opens.



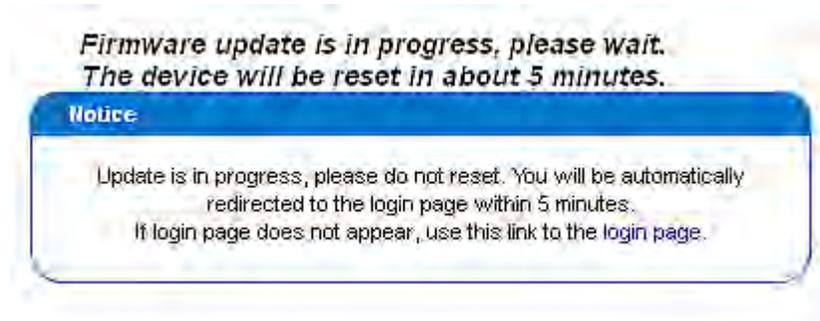
- In the Firmware File field, type the complete path to the firmware file on your computer, or click Browse and select the file.

3. Click Upload. The Firmware Update page opens. It shows the current firmware version and the new firmware version, and gives you a last chance to terminate the update.



Note: When upgrading a Dominion PX device over a low bandwidth network, after the firmware upload begins, do NOT switch the browser to another page until the upload is completed. This may take several minutes depending on the network speed.

4. To proceed with the update, click Update. To terminate the update, click Discard. The update may take 5 to 7 minutes and a message similar to the following appears.



In the FIPS mode, it takes longer to upgrade the firmware, ranging between 7 to 10 minutes.

Note: Do NOT power off the Dominion PX device during the update. To indicate at the rack that an update is in progress, the outlet LEDs flash and the device's three-digit LED display shows "FuP".

5. When the update is complete, the Dominion PX device resets, and the Login page re-opens. You can now log in and resume managing the Dominion PX.

Important: If you are using the Dominion PX with an SNMP manager, you should re-download the Dominion PX MIB after updating the firmware. This ensures your SNMP manager has the correct MIB for the release

you are using. See *Using SNMP* (on page 165) for details.

PSoC Firmware Upgrade Failure

All Raritan PDUs include two types of processors:

- The main PDU processor, which controls the unit's high level functionality, such as the web server, SNMP agent, environmental sensor management and so on.
- The PSoC (Programmable System On a Chip), which is responsible for low level outlet-related measurements, such as outlet current, voltage, power factor and so on.

Each PDU has one main PDU processor but can have one to six PSoC's depending on how many outlets it has.

The overall firmware upgrade process is controlled by the main PDU processor, which directs the upgrade of both its own firmware and the PSoC firmware. During the firmware upgrade, the main PDU processor first updates the PSoC's while it is still executing the old firmware. Though rare, if communication problems occur between the main PDU processor and a PSoC during the PSoC's firmware upgrade, that PSoC becomes temporarily inoperative, and a failure message is displayed at the end of the PSoC firmware upgrade step. Once the main PDU processor completes its own firmware upgrade, the new PDU processor firmware will check and recover any inoperative PSoC's. When it fails to recover any inoperative PSoC, the failed PSoC as well as any impacted outlets are all reported in the Firmware Status of the status panel.

The following status panel illustrates such a report.

Time & Session:
2012-07-20 13:16

User : admin
State : 39 sec idle
Your IP : 192.168.32.166
Last Login : 2012-07-20 11:34

Device Information:
Name: my_device
Model: PX (PX-5514)
IP Address: 192.168.57.151
Firmware: 01.05.05
Firmware Status: Failed
PSOCs: 2[O:5-8] 4[O:13-16] 6 [O:21-24]
FIPS mode is not set

Connected Users:
admin (192.168.32.166)
active

Power Cim State:
Power CIM is enabled

[Help - User Guide](#)

In the Firmware Status report, the number prior to the square brackets refers to the inoperative PSoC. The range of numbers within the square brackets indicates the impacted outlets.

For example, "Failed PSOCs: 2[O:5-8] 4[O:13-16] 6[O:21-24]" means:

- PSoC 2 firmware upgrade failed, and outlets 5 to 8 may not function properly since they are associated with PSoC 2
- PSoC 4 firmware upgrade failed, and outlets 13 to 16 may not function properly since they are associated with PSoC 4
- PSoC 6 firmware upgrade failed, and outlets 21 to 24 may not function properly since they are associated with PSoC 6

Full Disaster Recovery

If the firmware upgrade fails, causing the Dominion PX device to stop working, you can recover it by using a special utility rather than returning the device to Raritan.

Contact Raritan Technical Support for the recovery utility. An appropriate Dominion PX firmware file is required in the recovery procedure.

Copying Configurations with Bulk Configuration

The Bulk Configuration feature lets you save the settings of a configured Dominion PX device to your PC. You can use this configuration file to:

- Copy that configuration to other Dominion PX devices of the same model and firmware version.
- Restore the settings of the same Dominion PX device to previous configuration.

Users saving Dominion PX configurations require the Bulk Configuration system permission. Users copying configurations require both the Bulk Configuration and the Unit Reset permissions.

The image shows two dialog boxes from a web interface. The first dialog box is titled "Save Configuration" and contains two buttons: "Save Configuration" and "Cancel". The second dialog box is titled "Copy Configuration to Target" and contains a "File Name" label, a text input field, a "Browse..." button, and two buttons: "Copy Configuration" and "Cancel". Below the buttons in the second dialog box is a warning message: "Copy configuration may take several minutes. Please do NOT power off the device while copy is in progress! After a successful copy device will be reset automatically."

Saving a Dominion PX Configuration

A source device is an already configured Dominion PX device that is used to create a configuration file containing the settings that can be shared between Dominion PX devices. These settings include user and group configurations, thresholds, alert policies, the access control list, and so on. This file does NOT contain device-specific information, including:

- Device name
- System name, system contact and system location
- Network settings (IP address, gateway, netmask and so on)
- Device logs
- Outlet names
- Outlet status
- Environmental sensor names and mappings
- Environmental sensor X, Y and Z location values
- Local time
- Outlet grouping data
- Default outlet state (at either the Unit level or Outlet level)
- TCP port numbers for Telnet and SSH
- FIPS mode setting (enabled or disabled)

Note: It is strongly recommended to assign a number to Telnet and SSH ports when saving the PDU's configuration. A configuration file containing blank entries for Telnet and SSH ports restores the Telnet and SSH ports of the target PDUs to factory defaults.

The Default Outlet State setting is not saved. This prevents accidentally leaving outlets OFF after the configuration has been copied. Also, while the Local Time is not copied, the UTC time zone offset and any NTP settings are saved. Users should exercise caution when distributing a configuration file to the Dominion PX devices in a different time zone than the source device.

► **To save a configuration file:**

1. Choose Maintenance > Bulk Configuration. The Bulk Configuration page opens.
2. Click Save Configuration. Your web browser prompts you to save a file. Choose a suitable location and save the configuration file to your PC.

Copying a Dominion PX Configuration

A target device is a Dominion PX device that loads another Dominion PX device's configuration file.

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

- The user must be the Admin user.

Note: The bulk configuration operation is NOT available to any user other than the Admin user, even if the user is in the Admin group with full permissions.

- The target Dominion PX device must be of the same model type as the source Dominion PX device.
- The target Dominion PX device must be running the same firmware version as the source Dominion PX device.

► **To copy a Dominion PX Configuration:**

1. Log in to the target device's web interface.
2. If the target device's firmware version does not match that of the source device, update the target's firmware. See **Updating the Firmware** (on page 67).
3. Choose Maintenance > Bulk Configuration. The Bulk Configuration page opens.
4. Under the *Copy Configuration to Target* area, click Browse and select the configuration file on your PC.
5. Click Copy Configuration.

Note: If configured, SNMP, SMTP and the local event log records that a configuration copy occurred on the target device, but NFS and Syslog servers do not.

Note: If the source Dominion PX device is configured to "Force HTTPS for web access", and the target device is not, users may not be automatically redirected to the login page after the configuration copy is complete. In this case, users should simply refresh the web browser after the copying is complete and the login page appears.

Setting Up User Profiles

The Dominion PX is shipped with one built-in user profile: **admin**, which is used for initial login and configuration. This profile has full system and outlet permissions, and should be reserved for the system administrator. This profile cannot be modified or deleted.

All users must have a user profile, which specifies a login name and password, and contains additional (optional) information about the user. It also assigns the user to a User Group, and the User Group determines the user's system and outlet permissions.

If you choose, you can refrain from assigning some or all users to a User Group, and instead assign their system and outlets permissions on an individual basis.

Note: By default, multiple users can log in simultaneously using the same login name. You can change this so only one user at a time can use a specific login name. This is done by choosing Device Settings > Security and selecting the Enable Single Login Limitation checkbox.

Creating a User Profile

Creating new users adds a new login to the Dominion PX. To create a new user, you must have both the User/Group Management privilege and an IPMI Privilege Level of OEM.

► **To create a user profile:**

1. Choose User Management > Users & Groups. The User/Group Management page opens, divided into a User Management panel and a Group Management panel.

User Management

Existing Users
 --- select --- Refresh

New User Name

Full Name

Password

Confirm Password

Use Password as Encryption Phrase *

SHIMP v3 Encryption Phrase

Confirm SHIMP v3 Encryption Phrase

SHIMP v3 authentication settings
 MDS *

SHIMP v3 privacy settings
 DES *

Email Address

Mobile Number

User Group
 --- select ---

Enforce user to change password on next login *

Create Modify Copy Delete

*Note: Before entering any information in the user profile, make sure the User Group is created and available for selection. See **Setting Up User Groups** (on page 80).*

- In the User Management panel, type the following information about the user in the corresponding fields:

Field	Type this...
New User Name	The name the user enters to log in to the Dominion PX.
Full Name	The user's first and last names.
Password, Confirm Password	<p>The password the user enters to log in. Type it first in the Password field and then again in the Confirm Password field.</p> <ul style="list-style-type: none"> ▪ The password can be 4 to 32 characters long. ▪ It is case sensitive. ▪ Spaces are not permitted. <p>If the "Use Password as Encryption Phrase" checkbox is selected and SNMP v3 is used, the user password must be at least eight characters long.</p>

Field	Type this...
SNMP v3 Encryption Phrase, Confirm SNMP v3 Encryption Phrase	The password required when using secure SNMP v3 communication. When using SNMP v3, the encryption phrase must be at least eight characters long. See Using SNMP (on page 165). To make the SNMP v3 encryption phrase different from the user password, deselect the "Use Password as Encryption Phrase" checkbox. Then type it first in the SNMP v3 Encryption Phrase field and again in the Confirm SNMP v3 Encryption Phrase field.
SNMP v3 authentication settings	The authentication algorithm applied for SNMP v3. In the FIPS mode, only SHA_1 is supported. See FIPS Limitations (on page 156).
SNMP v3 privacy settings	The privacy algorithm applied for SNMP v3. In the FIPS mode, only AES_128 is supported. See FIPS Limitations (on page 156).
Email address	An email address where the user can be reached.
Mobile Number	A cell phone number where the user can be reached.

Note: New User Name, Password, and Confirm Password are the only required fields.

3. Select a user group from the drop-down list in the User Group field. The user group determines the system functions and outlets this user can access.
 - If you select None, the user is not assigned to a user group. This means you have to set the user's permissions individually. Before doing this, the user is blocked from accessing any system functions and outlets. See **Setting User Permissions Individually** (on page 79).
4. If you would like this user to set his or her own password, select the "Enforce user to change password on next login" checkbox. The user logs in the first time using the password you entered above, and then is forced to change it to his or her choice.
5. Click Create. The user profile is created.

Copying a User Profile

You can create a new user profile with the same settings as an existing profile using the copy function. Then modify the profile so that it differs as necessary from the original. This is a quick and easy way to create user profiles.

► **To copy a user profile:**

1. Choose User Management > Users & Groups. The User/Group Management page opens.

2. Select the existing user profile from the Existing Users drop-down list.
3. Type the name of the new user profile in the New User Name field.
4. Click Copy. A new user profile is created with the same settings as the existing profile. The new profile can be seen by clicking the drop-down list in the Existing Users field.

Modifying a User Profile

Users with User/Group Management permissions can modify user profiles. See **Setting the System Permissions** (on page 80) for details on setting user permissions.

► **To modify a user profile:**

1. Choose User Management > Users & Groups. The User/Group Management page opens.
2. Select the user profile you want to modify from the Existing Users drop-down list. All information in the user profile is displayed except the password.
3. Make all necessary changes to the information shown.

To change the password, type a new password in the Password and Confirm Password fields. If the password field is left blank, the password is not changed.

To change the SNMP v3 encryption phrase, type a new one in the SNMP v3 Encryption Phrase and Confirm SNMP v3 Encryption Phrase fields. If the encryption phrase field is left blank, the encryption phrase is not changed.

4. Click Modify. The user profile is modified.

Note: The name displayed in the "User (not in a group)" list of the User/Group System Permissions page remains unchanged even though you have modified the user name on the User/Group Management page. To make the user name assigned to the "None" User Group consistent on both pages, either leave the user name unchanged, or delete the user profile and then re-create it with a new name.

Deleting a User Profile

Remove a user profile when it is unnecessary.

► **To delete a user profile:**

1. Choose User Management > Users & Groups. The User/Group Management page opens.
2. Select the user profile you want to delete from the Existing Users drop-down list.

3. Click Delete. The user profile is deleted.

Setting User Permissions Individually

If you selected None for User Group when creating a user profile, you must set the user's permissions individually. Until you do this, the user is blocked from all system functions and outlets.

System Permissions

System permissions are the permissions to deal with system settings, including date/time settings, network settings, security settings, user management, and so on.

▶ To set the system permissions:

1. Choose User Management > User/Group System Permissions. The User/Group System Permissions page opens. See **Setting the System Permissions** (on page 80).
2. Select the user from the "User (not in group)" drop-down list. The drop-down list shows all user profiles that have NOT been assigned to a User Group.
3. Set the permissions as necessary. Click on the drop-down list to select a permission level for each permission listed.
4. When you are finished, click Apply. The permissions are applied to the user.

Outlet Permissions

Outlet permissions determine whether a user can configure each outlet's settings or switch it (if applicable).

▶ To set the outlet permissions:

1. Choose User Management > User/Group Outlet Permissions. The User/Group Outlet Permissions page opens. See **Setting the Outlet Permissions** (on page 82).
2. Select the user from the User drop-down list.
3. Set the permissions as necessary. Click on the drop-down list to select a permission level for each outlet.
4. When you are finished, click Apply. The permissions are applied to the user.

Note: A minimum IPMI privilege level "User" is required to switch outlets over IPMI, which causes no effect on web front-end use. However, privilege level has no effect on outlet permissions.

Setting Up User Groups

The Dominion PX is shipped with one user group built in: the Admin user group. This user group provides full system and outlet permissions. It can be neither modified nor deleted.

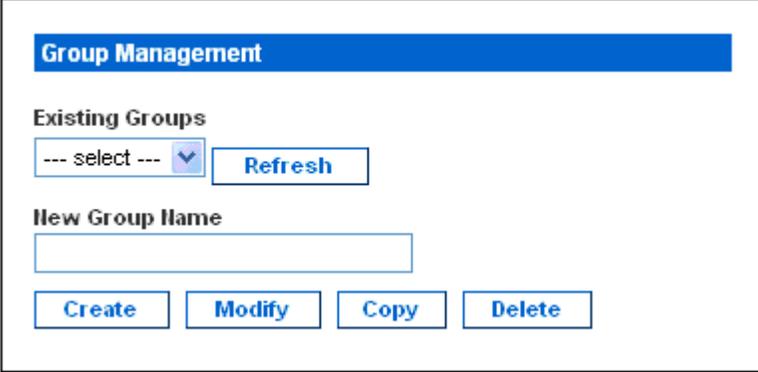
To restrict a user's permissions, create a user group with limited system and/or outlet permissions, and assign the user to that group.

Creating a User Group

It is better to create a user group with appropriate permissions before creating new user profiles that will have these permissions.

► **To create a user group:**

1. Choose User Management > Users & Groups. The User/Group Management page opens. This window is divided into a User Management panel and a Group Management panel.



The screenshot shows a web interface for Group Management. At the top is a blue header with the text "Group Management". Below this header, there are two main sections. The first section is labeled "Existing Groups" and contains a dropdown menu with the text "--- select ---" and a small downward arrow, followed by a blue button labeled "Refresh". The second section is labeled "New Group Name" and contains a single-line text input field. At the bottom of the panel, there are four blue buttons arranged horizontally: "Create", "Modify", "Copy", and "Delete".

2. In the Group Management panel, type the name of the group in the New Group Name field.

Note: To perform SNMP v3 operations successfully, make sure the name of your user group does NOT contain any spaces.

3. Click Create. The user group is created.

Setting the System Permissions

System permissions include all major functional areas of the web interface. When you first create a user group, all system permissions are set to NO.

► **To set the system permissions for a user group:**

1. Choose User Management > User/Group System Permissions. The User/Group System Permissions page opens.

User/Group System Permissions

Show permissions for:

User (not in a group)

Group

[Setup Outlet Access Permissions](#)

	Permission
Authentication Settings :	No
Bulk Configuration :	No
Change Password :	No
Date/Time Settings :	No
Environmental Sensor Configuration :	No
Firmware Update :	No
IPMI Privilege Level :	No Access
Log Settings :	No
Log View :	No
Network Settings :	No
Outlet Group Configuration :	No
SNMP Settings :	No
SNMP v3 Access :	Deny
SSH/Telnet Access :	No
SSL Certificate Management :	No
Security Settings :	No
Server Status via IPMI :	No
Unit & Outlet Configuration :	No
Unit Reset :	No
User/Group Management :	No
User/Group Permissions :	No

2. Select the user group from the Group drop-down list. The permissions that apply to this group appear. If this is the first time you are setting the permissions for this group, all permissions are set to No.
3. Set the permissions as necessary. Click on the drop-down list to select a permission level for each permission listed.
4. When you are finished, click Apply. The permissions are applied to the User Group.

Note: The "User (not in group)" field on this page is used to set individual user permissions. If you are setting group permissions, you may ignore this field.

Some permissions must be enabled with other permissions for the effects to apply. Check the individual task descriptions in this guide for details.

Setting the Outlet Permissions

Setting outlet permissions allows you to specify which outlets the members of a user group are permitted to access. When you first create a user group, all outlet permissions are set to NO.

► **To set the outlet permissions for a user group:**

1. Choose User Management > User/Group Outlet Permissions. The User/Group Outlet Permissions page opens.

User / Group Outlet Permissions

Show outlet permissions for:

User (not in a group) --- select ---

Group test

[Refresh](#)

Setup User / Group Permissions

At least IPML privilege level 'User' is necessary in order to switch outlets.

	Permission
Outlet 1:	Yes
Outlet 2:	Yes
Outlet 3:	No
Outlet 4:	Yes
Outlet 5:	Yes
Outlet 6:	Yes
Outlet 7:	Yes
Outlet 8:	No
Outlet 9:	No
Outlet 10:	No
Outlet 11:	No
Outlet 12:	No

2. Select the user group from the Group drop-down list. The permissions that apply to this group appear. If this is the first time you are setting the permissions for this group, all permissions are set to No.

3. Set the permissions as necessary. Click on the drop-down list to select a permission level for each outlet.
4. When you are finished, click Apply. The permissions are applied to the user group.

Note: The "User (not in a group)" field on this page is used to set individual user permissions. If you are setting group permissions, you may ignore this field.

Copying a User Group

You can create a new user group with the same permissions as an existing user group using the copy function. Then modify the group so that its permissions differ as necessary from the original. This is a quick and easy way to create user groups.

Any user group can be copied except for the Admin and <Unknown> groups.

► **To copy a user group:**

1. Choose User Management > Users & Groups. The User/Group Management page opens.
2. Select the existing user group from the Existing Groups drop-down list.
3. Type the name of the new user group in the New Group Name field.
4. Click Copy. A new user group is created with the same permissions as the existing group. The new user group can be seen by clicking the drop-down list in the Existing Groups field.

Modifying a User Group

The only attribute of a user group that can be modified is the group name.

► **To modify a user group's name:**

1. Choose User Management > Users & Groups. The User/Group Management page opens.
2. Select the user group you want to modify from the Existing Groups drop-down list. The name appears in the New Group Name field.
3. Make any necessary changes to the name.

Note: To perform SNMP v3 operations successfully, make sure the name of your user group does NOT contain any spaces.

4. Click Modify. The user group is modified.

*Note: To modify a user group's system or outlet permissions, repeat the procedure for setting the system or outlet permissions and make any necessary changes. See **Setting the System Permissions** (on page 80) and **Setting the Outlet Permissions** (on page 82).*

Deleting a User Group

You can remove a user group once it is obsolete.

▶ **To delete a user group:**

1. Choose User Management > Users & Groups. The User/Group Management page opens.
2. Select the user group you want to delete from the Existing Groups drop-down list.
3. Click Delete. The user group is deleted.

All members of the user group are automatically assigned to the "<Unknown>" group after the user group is deleted.

Setting Up and Managing Outlets

Global settings for all outlets can be configured at a time, such as the default outlet state and power cycling delay. Besides, with appropriate permissions, you should be able to access, set up, and switch an individual outlet.

Setting the Global Default Outlet State

Set a global default for the power state of the outlets when the Dominion PX device is powered on. Setting an individual outlet's startup state to something other than Device Default overrides this default state for that outlet. See **Naming and Configuring Outlets** (on page 88).

► To set the default outlet state:

1. Choose Device Settings > PDU Setup. The PDU Setup page opens.

PDU Setup

Default outlet state on device startup
 Last Known State ▼ *

PDU Power Cycling Delay
 0 * s

Power off period during outlet power cycling
 10 * s

Sequence Delay
 200 * ms

Height Above sea level
 0 *
 Meters Feet

Environmental Sensors

Use Rack Units ("U") for Z coordinate *

Data Retrieval

Enable Data Retrieval *

Sampling Period
 300 * * Enter an integer multiple of 3 from 3-600.
 (Measurements per data Log Entry is 1/3 value of Sampling Period: 1)

Unbalanced Load Detection

Enable Unbalanced Load Detection *

Thresholds

	lower			upper		
	hysteresis	critical	non-critical	non-critical	critical	
Voltage	4	195	207	243	253	* Volts
Line Current	1.00			15.42	18.88	* Amps
Neutral Line Current	1.00			15.42	18.88	* Amps
Unbalanced Load	2			5	10	* rel. %
Circuit Breaker 1 Current	1.00			12.91	15.21	* Amps
Circuit Breaker 2 Current	1.00			12.91	15.21	* Amps
Temperature	1	18	20	65	90	* degrees C

2. Select the default state from the "Default outlet state on device startup" drop-down list.
3. When you are finished, click Apply. The default state setting is applied.

Users require the Unit & Outlet Configuration permission to see the contents of the PDU Setup page.

Setting the Global Power Cycling Delay

When an outlet is power cycled, it is turned off and then back on. The number you enter on the PDU Setup page determines the length of time (in seconds) it takes for ALL outlets on the Dominion PX device to turn back on after being shut down during the power cycle.

► **To set the power cycling and sequence delay for all outlets:**

1. Choose Device Settings > PDU Setup. The PDU Setup page opens.
2. Type a number in the field labeled PDU Power Cycling Delay. When power to the Dominion PX device is cycled (either manually or because of a temporary power loss), this number determines how many seconds the Dominion PX waits before it provides power to the outlets. This is useful in cases where power may not initially be stable after being restored, or when UPS batteries may be charging. The PDU Power Cycling Delay can be set from 0 to 3600 seconds (one hour).
3. Type a number in the field labeled Power off period during outlet power cycling. When the outlets on the Dominion PX device are power cycled, they are turned off and then back on. The number you enter here determines the length of time (in seconds) it takes for the outlets to turn back on after they are shut down during the power cycle. The default is 10 seconds. The Power Off Period can be set from 0 to 3600 seconds (one hour).

*Tip: You can override this power cycling number for specific outlets. See **Naming and Configuring Outlets** (on page 88). You can power cycle an outlet from the **Outlet Details** page. See **Power Cycling an Outlet** (on page 90).*

4. Type a number of milliseconds (ms) in the field labeled Sequence Delay. The outlet sequence delay determines the time interval the Dominion PX device takes from outlet to outlet when powering ON or cycling all outlets. The default is 200 ms, which is sufficient to handle in-rush current conditions for most servers. Outlet sequence delay ranges from 1 to 255000 ms.

For SAN (storage area network), disk arrays, and some other equipment, the delay may need to be extended.

5. When you are finished, click Apply.

When there are a large number of outlets, set both the Power off period and the Sequence Delays to lower numbers. This way you can avoid a long wait before all the outlets are available again. This is especially useful when dealing with outlets grouped from other Dominion PX devices.

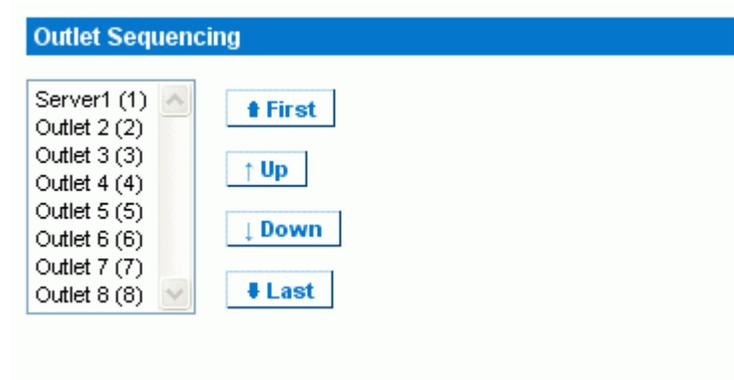
Users require the Unit & Outlet Configuration permission to see the contents of the PDU Setup page.

Setting the Outlet Power-On Sequence

By default, the outlets are sequentially powered on in ascending order from outlet 1 to the highest-numbered outlet when turning ON or power cycling all outlets on the Dominion PX device. You can change the order in which the outlets power ON. This is useful when there is a specific order in which the connected IT equipment should be powered up.

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

1. Choose Device Settings > PDU Setup. The PDU Setup page opens.



2. The current outlet power-on sequence appears in the list under Outlet Sequencing. To change the priority of an outlet, select it from the list and click one of the following buttons.
 - First: Moves the outlet to the top of the list, making it the first outlet to receive power.
 - Up: Moves the outlet up one position in the list.
 - Down: Moves the outlet down one position in the list.
 - Last: Moves the outlet to the bottom of the list, making it the final outlet to receive power.
3. Click Apply. The new sequence is saved.

Note: If you use Outlet Grouping to group outlets together, you should adjust the Outlet Sequencing to ensure that all outlets from this Dominion PX that are part of the same group, power up consecutively.

Naming and Configuring Outlets

You can give each outlet a name to help you identify the IT equipment connected to it. Besides, you can set the default state and power cycling delay for a specific outlet on the Outlet Setup page.

*Note: For configuring outlet thresholds and hysteresis, see **Setting Outlet Thresholds and Hysteresis** (on page 92).*

► To name and configure an outlet:

1. Choose Details > Outlet Setup. The Outlet Setup page opens.

Outlet 1 Setup

Show setup of outlet

Outlet 1 (1) Refresh

Outlet Name

Outlet state on device startup

Power off period during outlet power cycling
 * s (leave empty for [global setting](#))

Thresholds

	lower		upper			
	hysteresis	critical	non-critical	non-critical		critical
RMS Current	0.90	1.00	1.98	6.52	7.98	(max: 10.00) Amps

see also: [Model Configuration](#)

[Outlet 1 Details](#)

2. Select the outlet from the "Show setup of outlet" drop-down list.
3. Type a name for the outlet in the Outlet Name field. It is a good idea to give the outlet an easily recognizable name that helps you identify the device connected to it. You can always change names if the device is replaced.
4. Select an outlet state from the drop-down list in the "Outlet state on device startup" field. This determines if the outlet is ON or OFF when the Dominion PX device powers up. If set to Device Default, the state for this outlet is determined by the Default Outlet State on the PDU Setup page.
5. Type a number in the field labeled Power off period during outlet power cycling. If left blank, this outlet uses the value set on the PDU Setup page as a default. See **Setting the Global Power Cycling Delay** (on page 86).

*Note: You can power cycle an outlet from the Outlet Details page. See **Power Cycling an Outlet** (on page 90).*

6. Click Apply. The new name is applied.

Viewing Outlet Details

► **To display details about a particular outlet:**

1. Choose Details > Outlet Details. The Outlet Details page opens.

Outlet 1 Details

Show details of outlet

Outlet 1 (1)

Outlet Name: Outlet 1
Outlet Status: on
Line Pair: L1-L2
Circuit Breaker: Circuit Breaker 1

	Value	Status
RMS Current	0.08 Amps	ok
Power Factor	0.000 Ratio	ok
Maximum RMS Current	0.14 Amps	ok
Voltage	214 Volts	ok
Active Power	0.00 Watts	
Apparent Power	18.12 VA	
Active Energy	0 Watt Hours	

[Setup](#)

2. Select an outlet from the "Show details of outlet" drop-down list. The page shows these details about the outlet:
 - Outlet name
 - Outlet status
 - Line Pair (if applicable)
 - Circuit Breaker (if applicable)
 - Readings, including:
 - RMS current
 - Power Factor
 - Maximum RMS Current
 - Voltage

Active Power

Apparent Power

Active Energy (energy consumption, if applicable)

*Note: To display the Outlet Setup page, click the Setup link. See **Naming and Configuring Outlets** (on page 88) for a picture of the Outlet Setup page.*

Power Cycling an Outlet

Power Cycling an Outlet turns an outlet OFF, then ON again. This works only for outlets that are in the ON state.

► **To power cycle an outlet:**

1. Choose Details > Outlet Details. The Outlet Details page opens.
2. Select an outlet from the "Show details of outlet" drop-down list. The outlet must be ON.
3. Click Cycle.

*Tip: You can also power cycle an outlet from the Home page. See **Turning an Outlet On, Off, or Cycling the Power** (on page 50).*

*Note: The length of time between the off and on states in a power cycle can be set on the Dominion PX device as a whole, and for individual outlets. See **Setting PDU Thresholds and Hysteresis** (on page 91) and **Setting Outlet Thresholds and Hysteresis** (on page 92).*

Turning an Outlet On or Off

► **To turn an outlet on or off:**

1. Choose Details > Outlet Details. The Outlet Details page opens.
2. Select an outlet from the "Show details of outlet" drop-down list.
3. Click On to turn the outlet ON. Click Off to turn the outlet OFF.

*Tip: You can also turn an outlet on or off from the Home page. See **Turning an Outlet On, Off, or Cycling the Power** (on page 50).*

Setting Up Power Thresholds and Hysteresis

The Dominion PX is shipped with certain PDU and outlet power thresholds already defined, and with a hysteresis value already set for all thresholds. You can change the default Dominion PX thresholds and hysteresis values.

To understand how the hysteresis works, see **A Note about Untriggered Alerts** (on page 142).

*Note: When setting the thresholds, remember that you can set up alerts that are triggered whenever any thresholds are crossed. See **Configuring and Using Alert Notifications** (on page 131).*

Setting PDU Thresholds and Hysteresis

Users require the Unit & Outlet Configuration permission to see the contents of the PDU Setup page. Both the Unit & Outlet Configuration and the Line & Circuit Breaker Configuration permissions are required to adjust thresholds and hysteresis on this page.

► **To set the Dominion PX thresholds and hysteresis:**

1. Choose Device Settings > PDU Setup. The PDU Setup page opens.
2. Set the voltage, line current, temperature, and (if applicable) circuit breaker current thresholds for the PDU in the Thresholds panel. Enter critical or non-critical threshold for each item.

For the PDU's temperature thresholds, only positive numbers or zero are accepted so do NOT enter negative numbers.

Note: If you are using a Dominion PX in-line monitor, only the temperature threshold and hysteresis for the PDU are available on the PDU Setup page.

3. If necessary, change the hysteresis values for voltage, line current, temperature and (if applicable) circuit breaker current in the Thresholds panel. See **What is Threshold Hysteresis?** (on page 142) for the definition of the hysteresis.
 - To disable the hysteresis, type 0 (zero).
 - To enable the hysteresis, type a non-zero value, which must meet the rules described in the table:

Threshold	Criterion
Upper critical threshold	Larger than or equal to the following formula: upper non-critical threshold + hysteresis

Threshold	Criterion
Upper non-critical threshold	Larger than or equal to the following formula: lower non-critical threshold + (2 x hysteresis)
Lower non-critical threshold	Larger than or equal to the following formula: lower critical threshold + hysteresis

- When you are finished, click Apply.

Setting Outlet Thresholds and Hysteresis

You can set the thresholds for outlet RMS current, and by default, the Dominion PX assigns a hysteresis value for the outlet threshold.

Note: If you are using a Dominion PX in-line monitor, the outlet voltage threshold and hysteresis are also available on the same page.

► **To set the current thresholds and hysteresis of an outlet:**

- Choose Details > Outlet Setup. The Outlet Setup page opens.
- Select an outlet from the "Show setup of outlet" drop-down list.
- Set the RMS current threshold for the outlet in the Thresholds panel. Ensure the value you enter for the upper critical threshold is NOT larger than the maximum current ratings of the outlet.
- Adjust the hysteresis setting for the outlet threshold if necessary. See **What is Threshold Hysteresis?** (on page 142) for the definition of the hysteresis.
 - To disable the hysteresis, type 0 (zero).
 - To enable the hysteresis, type a non-zero value, which must meet the rules described in the table:

Threshold	Criterion
Upper critical threshold	Larger than or equal to the following formula: upper non-critical threshold + hysteresis
Upper non-critical threshold	Larger than or equal to the following formula: lower non-critical threshold + (2 x hysteresis)

Threshold	Criterion
Lower non-critical threshold	Larger than or equal to the following formula: lower critical threshold + hysteresis

5. When you are finished, click Apply. The setup details are applied.

Exception: For any 5A-rated outlet, default threshold values do NOT follow the above rules. Default upper and lower thresholds are within the default hysteresis limit of one another, which results in error messages when resetting or re-configuring the outlet threshold values. Therefore, it is strongly recommended to change the default hysteresis to 0.5A or less when resetting or configuring outlet thresholds.

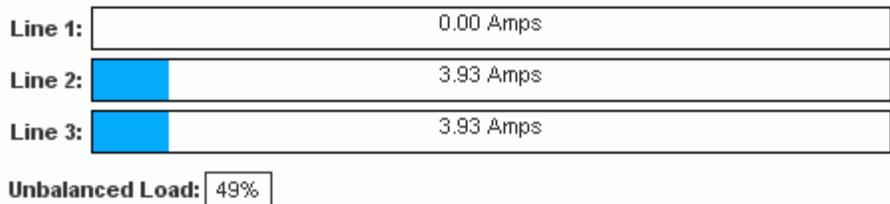
Monitoring Line and Circuit Breaker Status

The Dominion PX provides details for additional information on Line and Circuit Breaker status.

Monitoring Unbalanced Loads

In a three-phase Dominion PX device, a load imbalance occurs when the current on a line differs from the average current of all three lines. The largest absolute difference in current is expressed as a percentage of the average current. This value is the unbalanced load percentage.

Line Loads



An unbalanced load indicates that more current is being drawn from one line than it is from the others. The larger the percentage, the greater the difference. Reducing this imbalance maximizes the power available for use.

Enabling Unbalanced Load Detection displays the unbalanced loads percentage below the three individual Line graphs. This Unbalanced Load indicator is color coded:

- White indicates the imbalance is below the non-critical threshold.
- Yellow indicates the imbalance is above the non-critical threshold.
- Red indicates the imbalance is above the critical threshold.

Enabling Unbalanced Load Detection

To monitor unbalanced loads, you must enable unbalanced load detection.

► To enable unbalanced load detection:

1. Choose Device Settings > PDU Setup. The PDU Setup page opens.
2. Select the Enable Unbalanced Load Detection checkbox.
3. Click Apply.

You can configure non-critical and critical thresholds for the percentage of imbalance. This allows you to use the Alerts and Notification system as another means to react to load imbalance events.

Configuring Unbalanced Load Thresholds

Configuring these thresholds determines when the Unbalanced Load indicator changes colors from white to yellow or red. It also configures the unbalanced load event thresholds used in Alert Notifications.

Unbalanced Load Detection must be enabled before these thresholds take effect.

► **To configure unbalanced load thresholds:**

1. Choose Device Settings > PDU Setup. The PDU Setup page opens.
2. Set the Unbalanced Load percentage for the Upper Non-Critical threshold and the Upper Critical threshold.

Note: The difference between Critical and Non-Critical threshold values must be at least 2 percent, and both threshold values cannot exceed 100, so you must type a value below 99 for the Upper Non-Critical threshold.

3. Click Apply.

Balancing Loads

Balancing the current draw on your lines maximizes the power usage before a circuit breaker is tripped. To keep line loads as balanced as possible, move servers and other equipment from over-utilized lines to under-utilized ones.

In general this involves:

1. Checking what outlets receive power from the over-utilized line.
2. Unplugging a server from those outlets.
3. Plugging the server into an outlet receiving power from the under-utilized line.

Line Details Page

To open the Line Details page, choose Details > Line Details.

The screenshot displays two data cards. The first card, titled "Line 1 Status", contains a table with three columns: RMS Current, RMS Max Current, and Current Remaining. The values are 9.83 Amps, 11.43 Amps, and 10.03 Amps respectively. The second card, titled "Voltages", contains a single row for PDU Voltage with a value of 108 Volts.

Line 1 Status		
RMS Current	RMS Max Current	Current Remaining
9.83 Amps	11.43 Amps	10.03 Amps

Voltages
PDU Voltage
108 Volts

The page opens and displays for each line the present current draw, the largest amount of current drawn since the Dominion PX device's last boot, and the amount of available current that can be drawn.

The page also displays the amount of voltage provided by each line.

Circuit Breaker Details Page

To view the Circuit Breaker details, choose Details > CB Details.

The screenshot displays three data cards for different outlet banks. Each card contains a table with four columns: CB Status, RMS Current, RMS Max Current, and Current Remaining. All three banks show a status of "Closed", 0.00 Amps for RMS Current and RMS Max Current, and 16.00 Amps for Current Remaining.

Outlet Bank 1 (L1-II)			
CB Status	RMS Current	RMS Max Current	Current Remaining
Closed	0.00 Amps	0.00 Amps	16.00 Amps

Outlet Bank 2 (L1-II)			
CB Status	RMS Current	RMS Max Current	Current Remaining
Closed	0.00 Amps	0.00 Amps	16.00 Amps

Outlet Bank 3 (L2-II)			
CB Status	RMS Current	RMS Max Current	Current Remaining
Closed	0.00 Amps	0.00 Amps	16.00 Amps

Each bank of outlets governed by a circuit breaker is listed as a table, and indicates what lines they draw power from. Each table contains the status of the circuit breaker, present current draw through that bank, the largest amount of current that was drawn by that bank since the Dominion PX device last booted, and the amount of available current that the circuit breaker can handle.

Access Security Control

The Dominion PX provides tools to control access. You can require HTTPS encryption, enable the internal firewall and create firewall rules, and create login limitations.

In addition, you can disable the PDU's response to any ping request to further enhance the security.

Forcing HTTPS Encryption

HTTPS uses Secure Sockets Layer (SSL) technology to encrypt all traffic to and from the Dominion PX device so it is a more secure protocol than HTTP.

You can force users to access the Dominion PX web interface through the HTTPS protocol only. By default, this protocol is enabled.

► **To force HTTPS access to the Dominion PX web interface:**

1. Choose Device Settings > Security. The Security Settings page opens. The panel at the upper left is labeled HTTP Encryption.



2. Select the "Force HTTPS for web access" checkbox.

Note: In the FIPS mode, HTTPS access is automatically enabled so the HTTPS checkbox is replaced by the message "HTTPS for web access enabled in FIPS mode."

3. Click Apply. HTTPS is now required for browser access.

After enabling the HTTPS protocol, all access attempts using HTTP are redirected to HTTPS automatically.

Configuring the Firewall

The Dominion PX has a firewall that you can configure to prevent specific IP addresses and ranges of IP addresses from accessing the Dominion PX device. When the Dominion PX was initially configured, you were prompted to enable or disable IP access control. If you selected Disable (the default), the firewall was not enabled.

► **To configure the firewall:**

1. Enable the firewall. See **Enabling the Firewall** (on page 98).
2. Set the default policy. See **Changing the Default Policy** (on page 99).
3. Create firewall rules specifying which addresses to accept and which ones to discard. See **Creating Firewall Rules** (on page 99).

Changes made to firewall rules take effect immediately. Any unauthorized IP activities cease instantly.

*Note: The purpose of disabling the firewall by default is to prevent users from accidentally locking themselves out of the device. See **Initial Network and Time Configuration** (on page 19).*

Enabling the Firewall

The firewall rules, if any, take effect only after the firewall is enabled.

► **To enable the Dominion PX firewall:**

1. Choose Device Settings > Security. The Security Settings page opens. Locate the panel labeled IP Access Control.

Rule #	IP/Mask	Policy
		ACCEPT

2. Select the Enable IP Access Control checkbox. This enables the firewall.

3. Click Apply. The firewall is enabled.

Changing the Default Policy

After enabling the firewall, the default policy is to accept traffic from all IP addresses. This means only IP addresses discarded by a specific rule will NOT be permitted to access the Dominion PX.

You can change the default policy to DROP, in which case traffic from all IP addresses is dropped except the IP addresses accepted by a specific rule.

► To change the default policy:

1. Choose Device Settings > Security. The Security Settings page opens. Locate the panel labeled IP Access Control.
2. Ensure the Enable IP Access Control checkbox is selected.
3. The default policy is shown in the Default Policy field. To change it, select a different policy from the drop-down list.
4. Click Apply. The new default policy is applied.

Creating Firewall Rules

Firewall rules determine whether to accept or discard traffic intended for the Dominion PX, based on the IP address of the host sending the traffic. When creating firewall rules, keep these principles in mind:

- **Rule order is important.**

When traffic reaches the Dominion PX device, the rules are executed in numerical order. Only the first rule that matches the IP address determines whether the traffic is accepted or discarded. Any subsequent rules matching the IP address are ignored by the Dominion PX.

- **Subnet mask is required.**

When typing the IP address, you must specify BOTH the address and a subnet mask. For example, to specify a single address in a Class C network, use this format:

x.x.x.x/24

where /24 = a subnet mask of 255.255.255.0.

To specify an entire subnet or range of addresses, change the subnet mask accordingly.

Note: Valid IP addresses range from 0.0.0.0 through 255.255.255.255. Make sure the IP addresses entered are within the scope.

► **To create firewall rules:**

1. Choose Device Settings > Security. The Security Settings page opens. Locate the panel labeled IP Access Control.
2. Ensure the Enable IP Access Control checkbox is selected.
3. Create specific rules. See the table for different operations.

Action	Do this...
Add a rule to the end of the rules list	<ul style="list-style-type: none"> ▪ Type an IP address and subnet mask in the IP/Mask field. ▪ Select ACCEPT or DROP from the drop-down list in the Policy field. ▪ Click Append. <p>Do NOT enter a rule number. The system automatically numbers the rule.</p>
Insert a rule between two existing rules	<ul style="list-style-type: none"> ▪ Type a rule number where you want to insert a new rule above in the Rule # field. For example, to insert a rule between rules #3 and #4, type 4. ▪ Type an IP address and subnet mask in the IP/Mask field. ▪ Select ACCEPT or DROP from the drop-down list in the Policy field. ▪ Click Insert. <p>The system inserts the rule and automatically renumbers the following rules.</p>
Replace an existing rule	<ul style="list-style-type: none"> ▪ Type the number of the rule to be replaced in the Rule # field. ▪ Type an IP address and subnet mask in the IP/Mask field. ▪ Select ACCEPT or DROP from the drop-down list in the Policy field. ▪ Click Replace. <p>This system replaces the existing rule with the one you just created.</p>

- When finished, the rules appear in the IP Access Control panel.

IP Access Control

Please note: 'Apply' is required, or changes will be lost.

Enable IP Access Control *

Default policy

ACCEPT *

Rule #	IP/Mask	Policy
1	100.1.1.10/32	DROP
2	120.1.1.10/32	DROP
3	130.1.1.10/32	DROP
4	140.1.1.10/32	DROP

- Click Apply. The rules are applied.

Deleting Firewall Rules

When any firewall rules become obsolete or unnecessary, remove them from the rules list.

► To delete a firewall rule:

- Choose Device Settings > Security. The Security Settings page opens. Locate the panel labeled IP Access Control.
- Ensure the Enable IP Access Control checkbox is selected.
- Type the number of the rule to be deleted in the Rule # field.
- Click Delete. The rule is removed from the IP Access Control panel.
- Click Apply. The rule is deleted.

Creating Group Based Access Control Rules

Group based access control rules are similar to firewall rules, except they are applied to members of specific user groups. This enables you to give entire user groups system and outlet permissions, based on their IP addresses.

► To create group based access control rules:

- Enable the feature. See **Enabling the Feature** (on page 102).

2. Set the default action. See **Changing the Default Action** (on page 102).
3. Create rules that accept or drop traffic sending from specific addresses when they are associated with a specific user group. See **Creating Group Based Access Control Rules** (on page 103).

Changes made do not affect users currently logged in until the next login.

Enabling the Feature

You must enable this access control feature before any relevant rule can take effect.

► **To enable group based access control rules:**

1. Choose Device Settings > Security. The Security Settings page opens. Go to the panel labeled Group Based System Access Control.

Please note: 'Apply' is required, or changes will be lost.

Enable Group Based System Access Control

Default Action
ACCEPT

Rule #	Starting IP	Ending IP	Group / User (not in a group)	Action
1	0.0.0.0	255.255.255.255	All	ACCEPT
<input type="text"/>	<input type="text"/>	<input type="text"/>	Admin	ACCEPT

Append Insert Replace Delete

2. Select the Enable Group Based System Access Control checkbox. This enables the feature.
3. Create at least one "ACCEPT" rule, or all user groups CANNOT access the Dominion PX. See **Creating Group Based Access Control Rules** (on page 103).
4. Click Apply. Group based access control rules are enabled.

Changing the Default Action

The default action is shown in the Group Based System Access Control panel on the Security Settings page.

► **To change the default action:**

1. Choose Device Settings > Security. The Security Settings page opens. Go to the panel labeled Group Based System Access Control.

2. Make sure the Enable Group Based System Access Control checkbox is selected.
3. Select the action you want from the Default Action drop-down list.
4. Click Apply. The default action is applied.

Creating Group Based Access Control Rules

Group based access control rules accept or drop traffic intended for the Dominion PX device, based on the user's group membership. Like firewall rules, the order of rules is important, since the rules are executed in numerical order.

► To create group based access control rules:

1. Choose Device Settings > Security. The Security Settings page opens. Go to the panel labeled Group based System Access Control.
2. Make sure the Enable Group Based System Access Control checkbox is selected.
3. Create or delete specific rules:

Action	Do this...
Add a rule to the end of the rules list	<ul style="list-style-type: none"> ▪ Type a starting IP address in the Starting IP field. ▪ Type an ending IP address in the Ending IP field. ▪ Select a user group from the drop-down list in the "Group/User (not in a group)" field. This rule applies to members of the selected group or the selected individual user. ▪ Select ACCEPT or DROP from the drop-down list in the Action field. ▪ Click Append. <p>Do NOT enter a rule number. This system automatically numbers the rule.</p>
Insert a rule between two existing rules	<ul style="list-style-type: none"> ▪ Type the higher of the two rule numbers in the Rule # field. For example, to insert a rule between rules #3 and #4, type 4. ▪ Type a starting IP address in the Starting IP field. ▪ Type an ending IP address in the Ending IP field. ▪ Select ACCEPT or DROP from the drop-down list in the Action field. ▪ Click Insert. <p>The system inserts the rule and automatically renumbers the following rules.</p>
Replace an existing rule	<ul style="list-style-type: none"> ▪ Type the number of the rule to be replaced in the Rule # field.

Action	Do this...
	<ul style="list-style-type: none">▪ Type a starting IP address in the Starting IP field.▪ Type an ending IP address in the Ending IP field.▪ Select ACCEPT or DROP from the drop-down list in the Action field.▪ Click Replace. <p>This system replaces the existing rule with the one you just created.</p>

4. When you are finished, click Apply. The rules are applied.

Deleting Group Based Access Control Rules

When any access control rule becomes unnecessary or obsolete, remove it.

► **To delete a group based access control rule:**

1. Choose Device Settings > Security. The Security Settings page opens. Go to the panel labeled Group Based System Access Control.
2. Make sure the Enable Group Based System Access Control checkbox is selected.
3. Type the number of the rule to be deleted in the Rule # field.
4. Click Delete. The rule is removed from the Group Based System Access Control panel.
5. Click Apply. The rule is deleted.

Setting Up User Login Controls

You can set up login controls to make it more difficult for hackers to access the Dominion PX and the devices connected to it. You can arrange to lock persons out after a specified number of failed logins, limit the number of persons who log in using the same user name at the same time, and force users to create strong passwords.

Enabling User Blocking

User blocking determines how many times a user can attempt to log in to the Dominion PX and fail authentication before the user's login is blocked.

► **To enable user blocking:**

1. Choose Device Settings > Security. The Security Settings page opens. Go to the User Blocking panel.

User Blocking

Maximum number of failed logins
 (empty for infinite) *

Block Time (minutes)
 (empty for infinite) *

2. Type a number in the "Maximum number of failed logins" field. This is the maximum number of failed logins the user is permitted before the user's login is blocked from accessing the Dominion PX device. If no number is entered, there is no limit on failed logins.
3. Type a number in the Block Time field. This is the length of time in minutes the login is blocked. If no number is entered, there is no time limit on blocking the login.
4. Click Apply. The user blocking limits are applied.

Enabling Login Limitations

Login limitations determine whether more than one person can use the same login name at the same time, and whether users are required to change passwords at regular intervals.

► **To enable login limitations:**

1. Choose Device Settings > Security. The Security Settings page opens. Go to the Login Limitations panel.

Login Limitations

Enable Single Login Limitation *

Enable Password Aging *

Password Aging Interval (days)
60 *

Idle Timeout (minutes)
15 *

2. To prevent more than one person from using the same login at the same time, select the Enable Single Login Limitation checkbox.
3. To force users to change their passwords regularly, select the Enable Password Aging checkbox, and then enter a number of days in the Password Aging Interval field. Users are required to change their password every time that number of days has passed.
4. To adjust how long users can remain idle before they are forcibly logged out by the Dominion PX, enter a time in minutes in the Idle Timeout field. The default value is 15 minutes.
5. Click Apply. The login limitations are applied.

Tip: Keep the idle timeout to 15 minutes or less if possible. This reduces the number of idle sessions connected, and the number of simultaneous commands sent to the Dominion PX.

Enabling Strong Passwords

Use of strong passwords makes it more difficult for intruders to crack user passwords and access the Dominion PX device. By default, strong passwords should be at least eight characters long and contain upper- and lower-case letters, numbers, and special characters, such as @ or &.

► To force users to create strong passwords:

1. Choose Device Settings > Security. The Security Settings page opens. The Strong Passwords panel appears at the bottom of the page.

Strong Passwords

Enable Strong Passwords [^]

Minimum length of strong password
 ^{*}

Maximum length of strong password
 ^{*}

Enforce at least one lower case character [^]

Enforce at least one upper case character [^]

Enforce at least one numeric character [^]

Enforce at least one printable special character [^]

Number of restricted passwords based on history
 ^{*}

2. Select the Enable Strong Passwords checkbox to activate the strong password feature. The following are the default settings:

Minimum length	= 8 characters
Maximum length	= 16 characters
At least one lowercase character	= Required
At least one uppercase character	= Required
At least one numeric character	= Required
At least one printable special character	= Required
Number of restricted passwords	= 5

Note: The maximum password length accepted by the Dominion PX is 32 characters.

3. Make any necessary changes to the default settings.

4. When you are finished, click Apply. The changes are applied.

Disabling the PDU's Ping Response

The Dominion PX device responds to the ICMP ping request by default. You can have the PDU stop responding to any ICMP ping request if necessary.

► **To disable the PDU's response to ping:**

1. Choose Device Settings > Security. The Security Settings page opens. Go to the panel labeled Ping (ICMP Echo Request) Settings.
2. Deselect the "Ping enabled" checkbox.



3. When you are finished, click Apply. The changes are applied.

Setting Up a Digital Certificate

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

To obtain a certificate for the Dominion PX, create a Certificate Signing Request (CSR) and submit it to a certificate authority (CA). After the CA processes the information in the CSR, it provides you with an SSL certificate, which you must install on the Dominion PX device.

*Note: See **Forcing HTTPS Encryption** (on page 97) for instructions on forcing users to employ SSL when connecting to the Dominion PX.*

Creating a Certificate Signing Request

Follow this procedure to create the CSR for your Dominion PX device.

► **To create a CSR:**

1. Choose Device Setting > Certificate. The first page of the SSL Server Certificate Management page appears.

Certificate Signing Request (CSR)

Common Name

Organizational Unit

Organization

Locality/City

State/Province

Country (ISO Code)

Email

Challenge Password

Confirm Challenge Password

Key Length (bits)
 *

Create

2. Provide the information requested.

Field	Type this...
Common Name	The fully qualified domain name (FQDN) of your Dominion PX device.
Organizational Unit	The name of your department.
Organization	The registered name of your company.

Field	Type this...
Locality/City	The city where your company is located.
State/Province	The full name of the state or province where your company is located.
Country (ISO Code)	The country where your company is located. Use the standard ISO country code. For a list of ISO codes, visit the ISO website (http://www.iso.org/iso/country_codes/iso_3166_code_lists.htm).
Email	An email address where you or another administrative user can be reached.
Challenge Password Confirm Challenge Password	The password is used to protect the certificate or CSR. Type it first in the Challenge Password field and then again in the Confirm Challenge password field. The password is case sensitive, so ensure you capitalize the letters correctly.

Note: All fields are mandatory, including the Organizational Unit, Locality/City and State/Province fields. If you generate a CSR without values entered in the required fields, you cannot obtain third party certificates.

3. Select the key length (bits) from the drop-down list in this field. Default is 1024, but you can select 2048.
4. Click Create. The CSR is created and the second page of the SSL Server Certificate Management page opens. This page shows the information you entered when creating the CSR.



5. To download the newly-created CSR to your computer, click Download. You are prompted to open or save the file, named csr.txt.
6. After the file is stored on your computer, submit it to a CA to obtain the digital certificate.

Note: If any information in the CSR is incorrect, you can click Delete to delete the CSR. Then click Really Delete to confirm the deletion, and re-create the CSR.

Installing a Certificate

After the CA provides a signed certificate according to the CSR you submitted, you must install it on the Dominion PX device.

To upload an SSL certificate, you must log in as the administrator (admin).

▶ **To install the certificate:**

1. Choose Device Settings > Certificate. The second page of the Server Certificate Management page opens.
2. Type the path and name of the certificate file in the SSL Certificate File field, or click Browse and select the file.
3. Click Upload. The certificate is installed on the Dominion PX device.

Setting Up External User Authentication

For security purposes, users attempting to log in to the Dominion PX must be authenticated. The Dominion PX supports the access using one of the following authentication mechanisms:

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

*Exception: In the FIPS mode, RADIUS authentication is NOT supported, and LDAP authentication can be supported only when the SSL encryption is enabled. See **FIPS Limitations** (on page 156).*

By default, the Dominion PX is configured for local authentication. If you stay with this method, you do not need to do anything other than create user profiles for each authorized user. If you prefer to use an external LDAP or RADIUS server, you must:

- Provide the Dominion PX with the information about the server.
- Create user profiles for users who are authenticated externally because a user profile determines the User Group to which the user belongs, and determines the system and outlet permissions for the user accordingly.

When users log in with external authentication, even though they are authorized to perform outlet operations, they cannot perform operations on Outlet Groups. Only local users can perform operations on Outlet Groups so users must authenticate locally to do this.

Note: Setting the LDAP user attribute `rciusergroup` to `admin` allows an Active Directory® user to log in to the Dominion PX with Administrator privileges. This occurs even if the user is assigned to the Unknown user group that normally has no access permissions.

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

Gathering Information for LDAP Configuration

It requires knowledge of your LDAP server and directory settings to configure the Dominion PX for LDAP authentication. If you are not familiar with the settings, consult your LDAP administrator for help.

To configure LDAP authentication, you need to check:

- The IP address or hostname of the LDAP server
- The IP address of a backup or secondary LDAP server (optional)
- Whether the Secure LDAP protocol (LDAP over SSL) 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:
 - *A generic LDAP server*
 - *Novell Directory Service*
 - *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)

Setting Up LDAP Authentication

The Dominion PX supports both LDAP and LDAPS authentication only when the FIPS mode is disabled. In the FIPS mode, only LDAPS authentication works properly so all LDAP connections must be made over SSL. See **FIPS Limitations** (on page 156).

▶ **To set up LDAP authentication:**

1. Choose Device Settings > Authentication. The Authentication Settings page opens.

Authentication Settings

Local Authentication *
 LDAP

Type of external LDAP server
 Generic LDAP Server *

User LDAP Server
 192.168.51.101 *

Backup User LDAP Server
 192.168.40.101 *

SSL Enabled *

Port
 389 *

SSL Port
 636 *

Certificate File
 Browse...

Anonymous bind *
 Bind with credentials *

Bind DN
 *

Password
 *

Base DN of user LDAP server
 *

Name of login-name attribute
 *

Name of user-entry objectclass
 *

User Search Subfilter
 *

Active Directory Domain
 *

2. Select the LDAP radio button to enable the LDAP section of the page.
3. Type of external LDAP/LDAPS server. Choose from among the options available:

- Generic LDAP Server.
 - Novell Directory
 - Microsoft Active Directory. Active Directory is an implementation of LDAP/LDAPS directory services by Microsoft for use in Windows environments.
4. User LDAP Server - Type the IP address or DNS name of your LDAP/LDAPS remote authentication server (up to 37 characters). When the SSL Enabled checkbox is selected, the DNS name (fully qualified domain name) must be used.

Important: You must specify one LDAP/LDAPS server in this field or the Dominion PX cannot perform remote authentication.

5. Backup User LDAP Server - Type the IP address or DNS name of your backup LDAP/LDAPS server (up to 37 characters). When the SSL Enabled checkbox is selected, the DNS name (fully qualified domain name) must be used. Note that the remaining fields share the same settings with the User LDAP Server field. **Optional**
6. SSL Enabled - Select this checkbox if you would like to use SSL. Secure Sockets Layer (SSL) is a cryptographic protocol that allows the Dominion PX to communicate securely with the LDAP/LDAPS server.

Note: In the FIPS mode, only LDAPS authentication is supported so you must enable the SSL.

7. Port - The default Port is 389. Either use the standard LDAP TCP port or specify another port.
8. SSL Port - The default is 636. Either use the default port or specify another port. This field is enabled when the SSL Enabled checkbox is selected.
9. Certificate File - Consult your authentication server administrator to get the CA certificate file in Base64 encoded X-509 format for the LDAP/LDAPS server. Use the Browse button to navigate to the certificate file. This field is enabled when the SSL Enabled checkbox is selected.
10. Anonymous bind - For "Generic LDAP Server" or "Novell Directory Service," use this checkbox to enable or disable anonymous bind.
- To use anonymous bind, select this checkbox. By default it is selected.
 - When a Bind DN and password are required to bind to the external LDAP/LDAPS server, deselect this checkbox.
11. Bind with credentials - For "Microsoft Active Directory," use this checkbox to enable or disable anonymous bind.
- To use anonymous bind, deselect this checkbox. By default it is deselected.

- When a Bind DN and password are required to bind to the external LDAP/LDAPS server, select this checkbox.
12. Bind DN - Type the Bind DN when Bind DN and password are required.
 13. Password - Type the Bind password when Bind DN and password are required.
 14. Base DN of user LDAP server - Enter the name you want to bind against the LDAP/LDAPS server (up to 255 characters), and where in the database to begin searching for the specified Base DN. An example Base Search value might be:
`cn=Users,dc=raritan,dc=com`. Consult your authentication server administrator for the appropriate values to enter into these fields.
 15. Type the following information in the corresponding fields. LDAP needs this information to verify user names and passwords.
 - Login name attribute (also called AuthorizationString)
 - User entry object class
 - User search subfilter (also called BaseSearch)
 16. Active Directory Domain - Type the name of the Active Directory Domain. For example, testradius.com. Consult with your Active Directory Administrator for a specific domain name.
 17. Click Apply. LDAP authentication is now in place.

Note: If the Dominion PX clock and the LDAP server clock are out of sync, the certificates are considered expired and users are unable to authenticate using LDAP. To ensure proper synchronization, administrators should configure the Dominion PX and the LDAP server to use the same NTP server.

More Information about AD Configuration

For more information about the LDAP configuration using Microsoft Active Directory, see **LDAP Configuration Illustration** (on page 257).

Setting Up RADIUS Authentication

The Dominion PX supports the RADIUS authentication only when the FIPS mode is disabled. In the FIPS mode, RADIUS authentication is NOT supported so its settings become unavailable. See **FIPS Limitations** (on page 156).

► To set up RADIUS authentication:

1. Choose Device Settings > Authentication. The Authentication Settings page opens. The RADIUS parameters are located at the bottom of the page.

	Server	Shared Secret	Auth. Port	Acc. Port	Timeout	Retries
1.	<input type="text"/>	<input type="text"/>	<input type="text" value="1812"/>	<input type="text" value="1813"/>	<input type="text" value="1"/>	<input type="text" value="3"/>

Global Authentication Type: CHAP

[More Entries](#)

[Apply](#) [Reset To Defaults](#)

2. Click the RADIUS radio button.
3. Type the IP address of the RADIUS server in the Server field.
4. Type the shared secret in the Shared Secret field. The shared secret is necessary to protect communication with the RADIUS server.
5. By default, the Dominion PX uses the standard RADIUS port 1812 (authentication) and 1813 (accounting). If you prefer to use non-standard ports, change the ports.
6. Type the timeout period in seconds in the Timeout field. This sets the maximum amount of time to establish contact with the RADIUS server before timing out. Default is 1 second.
7. Type the number of retries permitted in the Retries field. Default is 3.
8. If you have additional RADIUS servers, click More Entries. Fields for four additional servers appear. Enter the same information in Steps 3-7 for each additional server.
9. Select an authentication protocol from the drop-down list in the Global Authentication Type field. Your choices include:
 - PAP (Password Authentication Protocol)
 - CHAP (Challenge Handshake Authentication Protocol)

CHAP is generally considered more secure because the user name and password are encrypted, while in PAP they are transmitted in the clear.
10. Click Apply. RADIUS authentication is now in place.

Environmental Sensors

The Dominion PX can monitor the environmental conditions, such as temperature and humidity, where environmental sensors are placed.

► **To add environmental sensors:**

1. Physically connect environmental sensors to the Dominion PX device. See ***Connecting Environmental Sensors (Optional)*** (on page 25).

2. Log in to the Dominion PX web interface. The Dominion PX should have detected the connected sensors, and display them in the web interface.
3. Identify each sensor through the sensor's serial number. See **Identifying Environmental Sensors** (on page 119).
4. The Dominion PX should automatically manage the detected sensors. Verify whether detected sensors are managed. If not, have them managed. See **Managing Environmental Sensors** (on page 121).
5. Configure the sensors. See **Configuring Environmental Sensors** (on page 122). The steps include:
 - a. Name the sensor.
 - b. If the connected sensor is a Raritan contact closure sensor, specify an appropriate sensor type.
 - c. Mark the sensor's physical location on the rack or in the room.
 - d. If the sensor is a *numeric* sensor, configure its upper and lower thresholds.

Note: Numeric sensors use numeric values to indicate the environmental or internal conditions while discrete (on/off) sensors use alphabetical characters to indicate the state. Only numeric sensors have the threshold settings.

Identifying Environmental Sensors

An environmental sensor includes a serial number tag on the sensor cable.



The serial number for each sensor appears listed in the web interface after each sensor is detected by the Dominion PX.

Sensor ID	Serial Number	Type	Channel Name	Reading	State	Managed?
1	PRC0190292	Contact(On/Off) 1	On/Off PRC0190292 1		Normal	Remove
2	PRC0190292	Contact(On/Off) 2	On/Off PRC0190292 2		Normal	Remove
3	AEI7A00022	Humidity	Humidity AEI7A00022	56 rel. %	ok	Remove
4	AEI7A00022	Temperature	Temperature AEI7A00022	27 degrees C 80 degree F	ok	Remove
5	AEI7A00021	Humidity	Humidity AEI7A00021	58 rel. %	ok	Remove
6	AEI7A00021	Temperature	Temperature AEI7A00021	26 degrees C 79 degree F	ok	Remove

Match the serial number from the tag to those listed in the sensor table.

Managing Environmental Sensors

The Dominion PX starts to retrieve an environmental sensor's reading and/or state and records the state transitions after the environmental sensor is managed.

The Dominion PX device can manage a maximum of 16 environmental sensors.

When there are less than 16 managed sensors, the Dominion PX automatically brings detected environmental sensors under management. You should only have to manually manage a sensor when it is not under management.

► To manually manage an environmental sensor:

1. Choose External Sensors > External Sensors Details. The External Sensor Details page opens. All environmental sensors are listed on the page after they are detected.

Sensor ID	Serial Number	Type	Channel Name	Reading	State	Managed?
1	PRC0190292	Contact(On/Off) 1	On/Off PRC0190292 1		Normal	Remove
2	PRC0190292	Contact(On/Off) 2	On/Off PRC0190292 2		Normal	Remove
3	AEI7A00022	Humidity	Humidity AEI7A00022	59 rel. %	ok	Remove
4	AEI7A00022	Temperature	Temperature AEI7A00022	28 degrees C 82 degree F	ok	Remove
	AEI7A00021	Humidity				Manage
	AEI7A00021	Temperature				Manage

2. Verify whether desired sensors are being managed by checking the Managed? column.
 - Presence of the Remove button indicates that the corresponding sensor is being managed.
 - Presence of the Manage button indicates that the corresponding sensor is NOT being managed.
3. To manage a sensor that is not under management, do either of the following:
 - **Click the corresponding Manage button:** An ID number and a name are automatically assigned to the managed sensor, and the Dominion PX starts to track and display the sensor's reading and/or state.

- **Manually assign an ID number to the sensor:** A sensor becomes "managed" after you assign an ID number to it. The default name is automatically assigned. If another sensor already occupied the ID number at the time of assignment, that sensor becomes "unmanaged" after losing the ID number. For details, see **Assigning or Changing the ID Number** (on page 131).

Assign sensor : to sensor ID:

A sensor's default name comprises the sensor type and serial number, such as *Humidity AEI7A00021*. If the sensor is a contact closure sensor, a channel number is added to the end of the default name.

*Note: When the number of managed sensors reaches the maximum, you CANNOT manage additional sensors until you remove or replace any managed sensors. To remove a sensor, see **Unmanaging Environmental Sensors** (on page 130). To replace a sensor, see **Assigning or Changing the ID Number** (on page 131).*

Configuring Environmental Sensors

You can assign new names to managed sensors for identifying them easily, and to provide them with location descriptions.

For *numeric* sensors, you can also configure thresholds that enable the Dominion PX to generate an alert or notification when environmental conditions detected by the sensors move outside of your ideal values.

Note: Numeric sensors use numeric values to indicate the environmental or internal conditions while discrete (on/off) sensors use alphabetical characters to indicate the state. Only numeric sensors have the threshold settings.

► To configure environmental sensors:

1. You can trigger the setup page for the desired environmental sensor by doing either of the following:
 - Choose External Sensors > External Sensors Setup. The External Sensor Setup page opens.
Select the desired environmental sensor from the drop-down list of the "Show setup of external sensor" field.
 - Choose External Sensors > External Sensors Details. The External Sensor Details page opens.
Click the name of the sensor that you want to configure. The External Sensor Setup page opens.

2. If the sensor selected in the previous step is a Raritan contact closure sensor connected with third-party detectors/switches, the On/Off Sensor Subtype field is displayed for you to select the detector/switch type:
 - Contact: The detector/switch is designed to detect the door lock or door open/closed status.
 - Smoke Detection: The detector/switch is designed to detect the appearance of smoke.
 - Water Detection: The detector/switch is designed to detect the appearance of water on the floor.
 - Vibration: The detector/switch is designed to detect the vibration in the floor.
3. Type a new name in the Sensor Name field.

A sensor's default name comprises the sensor type and serial number, such as *Humidity AE17A00021*. If the sensor is a contact closure sensor, a channel number is added to the end of the default name.

4. Describe the sensor's location by assigning alphanumeric values to the X, Y and Z coordinates. See **Describing the Sensor Location** (on page 126). All location fields are optional.

External Sensor 1 Setup

Show setup of external sensor

Humidity AEI7A00021 (1) ▼
Refresh

Serial Number: AEI7A00021

Type: Humidity

Sensor Id: 1

Sensor Name:

Location (X):

Location (Y):

Location (Z Rack Units): Rack Unit ("U")

Thresholds

lower		upper		
hysteresis	critical	non-critical	non-critical	critical
1	10	15	85	90
				ref. %

5. Configure the upper and lower thresholds for *numeric* sensors.
 - The Upper Critical and Lower Critical values are points at which the Dominion PX considers the operating environment critical and outside the range of the acceptable threshold.
 - Once critical, the sensor reading must drop below the Upper Non-critical or raise above the Lower Non-critical value before the Dominion PX considers the environment to be acceptable again.

Note: Only numeric sensors have the threshold settings. A discrete sensor, such as a contact closure sensor, does not have threshold settings so the Thresholds panel is unavailable.

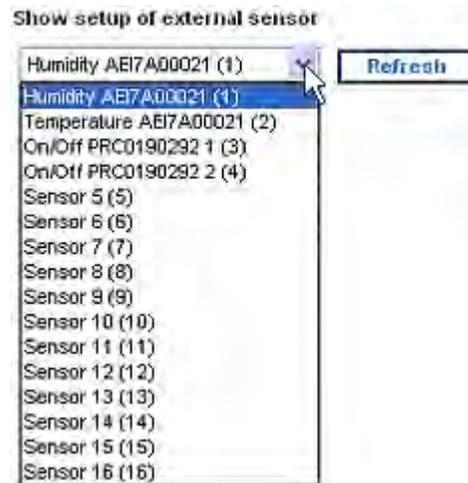
6. If necessary, change the default hysteresis value in the Thresholds panel.
 - To disable the hysteresis, type 0 (zero).

- To enable the hysteresis, type a non-zero value, which must meet the rules described in the table:

Threshold	Criterion
Upper critical threshold	Larger than or equal to the following formula: upper non-critical threshold + hysteresis
Upper non-critical threshold	Larger than or equal to the following formula: lower non-critical threshold + (2 x hysteresis)
Lower non-critical threshold	Larger than or equal to the following formula: lower critical threshold + hysteresis

- Click Apply. The sensor settings are saved.
- If necessary, select another managed sensor from the "Show setup of external sensor" drop-down list, and repeat these steps to configure it.

Note: The number in parentheses following a sensor name is the ID number assigned to each sensor.



Note: The maximum ambient operating temperature (TMA) for the Dominion PX varies between 40 to 60 degrees Celsius, depending on the model and certification standard (CE or UL). If necessary, contact Raritan Technical Support for this information for your model.

Describing the Sensor Location

Location (X):

9 feet

Location (Y):

4 feet

Location (Z Rack Units):

5

Rack Unit ("U")

Optional: Use the X, Y and Z coordinates to describe each sensor's physical location. You can use these location values to track records of environmental conditions in fixed locations around your IT equipment. The X, Y and Z values act as additional attributes and are not tied to any specific measurement scheme. If you choose to, you can use non-measurement values. For example:

X = Brown Cabinet Row

Y = Third Rack

Z = Top of Cabinet

Values for the X, Y and Z coordinates may consist of:

- For X and Y: Any combination of alphanumeric characters. The value can be 0 to 24 characters long.
- For Z when the 'Rack Units ("U")' checkbox is deselected: Any combination of alphanumeric characters, from 0 to 24 characters long.
- For Z when the 'Rack Units ("U")' checkbox is selected: Any integer from 0 to 60.

A selected 'Rack Units ("U")' checkbox indicates that the height of the Z coordinate is measured in standard rack units. See **Using Rack Units for the Z Coordinate Value** (on page 126).

Note: To configure and retrieve these coordinate values over SNMP, see the Dominion PX MIB.

Using Rack Units for the Z Coordinate Value

You can use the number of rack units to describe the vertical location (Z coordinate) of an environmental sensor.

► **To use rack units for the Z coordinate value:**

1. Choose Device Settings > PDU Setup. The PDU Setup page opens.
2. Select the 'Use Rack Units ("U") for Z coordinate' checkbox.
3. Click Apply.

Now you can use the number of rack units to describe the height of the sensor's location. See **Configuring Environmental Sensors** (on page 122).

Viewing Sensor Readings and States

The Home page shows the following information for environmental sensors:

- Number of managed sensors
- Number of unmanaged sensors
- Managed sensors along with their readings and/or states

For a temperature sensor, the reading is displayed in both Celsius and Fahrenheit.

- "C" represents Celsius.
- "F" represents Fahrenheit.

External Sensors

Number of managed sensor(s): 4

Number of unmanaged sensor(s): 2

Name	Reading	State
On/Off PRC0190292 1		Normal
On/Off PRC0190292 2		Normal
Humidity AEI7A00022	58 rel. %	ok
Temperature AEI7A00022	28 degrees C 82 degree F	ok

To view the readings and states from any other page, click Home in the navigation path at the top of the page.

Sensor Measurement Accuracy

Raritan environmental sensors are with the following factory specifications. Calibration is not required for environmental sensors.

- Temperature: +/-2 degrees Celsius
- Humidity: +/-5% (when humidity < 60%) or +/-8% (when humidity > 60%)
- Differential air pressure: +/-1.5%
- Air flow: +/-6.5%

States of Managed Sensors

An environmental sensor shows the state after being managed.

Available sensor states vary depending on the sensor type -- numeric or discrete. For example, a contact closure sensor is a discrete sensor so it switches between three states only -- unavailable, alarmed and normal.

Note: Numeric sensors use numeric values to indicate the environmental or internal conditions while discrete (on/off) sensors use alphabetical characters to indicate the state.

Sensor state	Applicable to
unavailable	All sensors
alarmed	Discrete sensors
normal	Discrete sensors
ok	Numeric sensors
below lower critical	Numeric sensors
below lower non-critical	Numeric sensors
above upper non-critical	Numeric sensors
above upper critical	Numeric sensors

Note: The state change of a contact closure sensor occurs only if the sensor enters the new state for at least 1 consecutive sample.

"unavailable" State

The *unavailable* state means the connectivity to the sensor is lost.

The Dominion PX pings all managed sensors at regular intervals in seconds. If it does not detect a particular sensor for three consecutive scans, the *unavailable* state is displayed for that sensor.

When the communication with a contact closure sensor's processor is lost, all detectors (that is, all switches) connected to the same sensor module show the "unavailable" state.

Note: When the sensor is deemed unavailable, the existing sensor configuration remains unchanged. For example, the ID number assigned to the sensor remains associated with it.

The Dominion PX continues to ping unavailable sensors, and moves out of the *unavailable* state after detecting the sensor for two consecutive scans.

"normal" State

This state indicates the sensor is in the normal state.

For a contact closure sensor, this state is the normal state you have set.

- If the normal state is set to Normally Closed, the *normal* state means the contact closure switch is closed.
- If the normal state is set to Normally Open, the *normal* state means the contact closure switch is open.

Note: See **Configuring a Contact Closure Sensor** (on page 28) for setting the normal state.

"alarmed" State

This state means a discrete (on/off) sensor is in the "abnormal" state.

For a contact closure sensor, the meaning of this state varies based on the sensor's normal state setting.

- If the normal state is set to Normally Closed, the *alarmed* state means the contact closure switch is open.
- If the normal state is set to Normally Open, the *alarmed* state means the contact closure switch is closed.

Note: See **Configuring a Contact Closure Sensor** (on page 28) for setting the normal state.

Tip: A contact closure sensor's LED is lit after entering the alarmed state. If the sensor module has two channels for connecting two switches, two LEDs are available. Check which contact closure switch is in the "abnormal" status according to the channel number of the LED.

"ok" State

Only a numeric sensor shows this state. This state means the sensor reading is within the acceptable range as indicated below:

$$\text{Lower Non-Critical threshold} \leq \text{Reading} < \text{Upper Non-Critical threshold}$$

Note: The symbol \leq means smaller than ($<$) or equal to ($=$).

"below lower critical" State

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

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

"below lower non-critical" State

Only a numeric sensor shows this state.

This state means the sensor reading is below the lower non-critical threshold as indicated below:

$$\text{Lower Critical Threshold} \leq \text{Reading} < \text{Lower Non-Critical Threshold}$$

Note: The symbol \leq means smaller than ($<$) or equal to ($=$).

"above upper non-critical" State

Only a numeric sensor shows this state.

This state means the sensor reading is above the upper non-critical threshold as indicated below:

$$\text{Upper Non-Critical Threshold} \leq \text{Reading} < \text{Upper Critical Threshold}$$

Note: The symbol \leq means smaller than ($<$) or equal to ($=$).

"above upper critical" State

This state means a numeric sensor's reading is above the upper critical threshold as indicated below:

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

Note: The symbol \leq means smaller than ($<$) or equal to ($=$).

Unmanaging Environmental Sensors

When it is unnecessary to monitor a particular environmental factor, you can unmanage or release the corresponding environmental sensor so that the Dominion PX device stops retrieving the sensor's reading and/or state.

► **To release a managed sensor:**

1. Choose External Sensors > External Sensors Details. The External Sensor Details page opens.
2. Click Remove for the sensor that you want to release.

After a sensor is removed from management, the ID number assigned to that sensor is released and can be automatically assigned to any newly-detected sensor.

Assigning or Changing the ID Number

Instead of letting the Dominion PX assign an ID number to the sensor, you can manually assign any ID number (1 to 16) to a detected or managed sensor. With the feature, you can:

- Have a sensor managed if it has not been managed yet
- Change the ID number of a managed sensor
- Replace a managed sensor with an identical type of sensor by assigning its ID number to another one

This feature is especially useful when there are 16 managed sensors because it removes a sensor from management while assigning its ID number to a different sensor at the same time.

*Tip: You can also rearrange or change the ID numbers of all managed sensors at once via SNMP. See **Changing ID Numbers of Environmental Sensors** (on page 174).*

► To assign or change the ID number:

1. Choose External Sensors > External Sensors Details. The External Sensor Details page opens.
2. In the "Assign sensor" field, select a sensor from the drop-down list. Each sensor is identified with a combination of the ID number (if available), serial number and sensor type, such as *1 AEI700021 Humidity*.

Assign sensor : to sensor ID:

3. In the "to sensor ID" field, select an ID number from the drop-down list.
4. Click Assign. The selected ID number is assigned to the selected sensor.
 - The selected sensor becomes managed if it was not.
 - If the selected ID number was previously used by a sensor, that sensor becomes unmanaged after losing this ID number.
 - If the selected ID number was previously used by a sensor that had been physically disconnected, that sensor disappears from the list after losing this ID number.

Configuring and Using Alert Notifications

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

Components of an Alert

The alert is a condition statement: if "A" happens, then do "B". This condition statement describes what the Dominion PX does in certain situations and is composed of multiple parts:

- **Event:** This is the "A" portion of an alert and describes the Dominion PX (or part of it) meeting a certain condition. For example, a specific outlet's voltage exceeds the non-critical threshold.
- **Policy:** This is the "B" portion of an alert and describes the response to the event. For example, the Dominion PX notifies the system administrator of the event and records the event in the log.
- **Threshold or alarm:** This is a condition met by the event. For example, a temperature warning level or a contact closure alarm.
- **Destination:** This is a target of the policy. For example, a system administrator's e-mail address.

Thresholds are user-configurable and are adjusted on the appropriate setup page for the desired part of the Dominion PX:

- Outlet-specific thresholds are assigned on the Outlet Setup page.
- Unit-wide thresholds are assigned on the PDU Setup page.
- Environmental thresholds are assigned on the External Sensor Setup page.

Destinations are configured as part of the Alert creation process. E-mail alert destinations require that the Dominion PX be set up for SMTP communication. See **Configuring the SMTP Settings** (on page 62).

How to Configure an Alert

The best way to create a new set of alerts, in sequence, is:

- Create the necessary destinations.
- Create policies based on notifying these destinations.
- Create an alert that executes a policy.

By working in this order, you have destinations to choose from when creating a policy, and policies to choose from when creating an alert. If you try to create an alert and find you do not have a desired policy or destination available, you will have to interrupt the process to add the policy or destination, and then must create the alert again.

Creating Alert Destinations

To set up new Alerts, first create the necessary destinations on the Alert Destinations page. Choose Alerts > Alert Destinations to open the page.

Alert Destinations		
Destination		
Event Log		(read only)
Switch Outlets	Outlets 1 - 24 (Off, On, Cycle)	(read only)
eMail	sysadmin@companyname.com	Delete
eMail	weekend@companyname.com	Delete
SNMP	192.168.33.24	Delete

Destination Type: **Receiver eMail Address:**
 [Add](#)

[Alert Destination](#) - [Alert Policies](#) - [Alert Policy Editor](#)

This table on the page lists the existing destinations configured on the Dominion PX. Two destinations, Event Log and Switch Outlets, are always available as part of the system.

You can add and delete additional destinations. There are four destination types:

- **Event Log:** One of the system default destinations. Adding the event log destination to a policy causes the Dominion PX to record alert notifications in the system log. This destination cannot be deleted and additional ones of this type cannot be created.
- **Switch Outlets:** One of the system default destinations. Adding the Switch Outlets destination to a policy allows the Dominion PX to switch the power state of outlets in response to an event. This destination cannot be deleted and additional ones of this type cannot be created.
- **eMail:** A user-configurable destination. Adding an e-mail destination to a policy causes the Dominion PX to send alert notifications to the specified e-mail address. Multiple e-mail destinations can be created.
- **SNMP:** A user-configurable destination. Adding an SNMP destination to a policy causes the ThresholdAlarm trap to be sent to the specified IP address. Multiple SNMP destinations can be created.

*Tip: To generate all SNMP traps described in the MIB, you should choose Device Settings > Event Log to configure the SNMP feature instead. See **Configuring the SNMP Traps** (on page 169) and **Suggestion for SNMP Trap Configuration** (on page 170).*

► **To add an eMail destination:**

1. Choose Alerts > Alert Destinations. The Alerts Destination page opens.
2. Select eMail from the Destination Type drop-down list.
3. Type the address of the recipient in the Receiver eMail Address field.
4. Click Add.

Note: If an address is configured for SMTP logging and all event-types are selected, that address will already receive notifications for an event that triggers an alert. However, you can use eMail destinations to send notifications to additional addresses. Furthermore, these notifications can be limited to the events that are relevant to those recipients.

► **To add an SNMP destination:**

1. Choose Alerts > Alert Destinations. The Alerts Destination page appears.
2. Select SNMP from the Destination Type drop-down list.

3. Type the IP address of the SNMP manager in the Destination IP field. This must be a numeric IP address. DNS names are not allowed.

*Tip: Although you can specify SNMP destinations in this field, it is highly recommended to specify the SNMP destination on the Event Log Settings page only. See **Configuring the SNMP Traps** (on page 169) and **Suggestion for SNMP Trap Configuration** (on page 170).*

4. Type the SNMP community string for this trap in the Community String field.
5. Click Add.

Note: SNMP alert traps are distinct from PX-specific traps. PX-specific traps are used for event logging if SNMP is configured on the Event Log Settings page.

For SNMP alert destinations, the Dominion PX sends IPMI-PET (platform event traps) traps to the SNMP manager. The traps are generated in the alert configuration and sent out in IPMI-specific formats containing raw data.

Details of these traps can be referenced at:

http://www.intel.com/design/servers/ipmi/pdf/IPMIv2_0_rev1_0_E3_markup.pdf

http://www.intel.com/design/servers/ipmi/pdf/ipmiv2_0_rev1_0_e3_markup.pdf (Chapter 17.16) and at:

<http://download.intel.com/design/servers/ipmi/PET100.pdf>

<http://download.intel.com/design/servers/ipmi/pet100.pdf>.

Once added, your new destinations appear on the destinations table. To delete a destination from the system, click Delete next to the desired destination.

Creating Alert Policies

Once your destinations are created, you can create policies based on notifying these destinations. This is done on the Alert Policies Editor, which you can reach by choosing Alerts > Alert Policy Editor.

Alert Policy Editor

Existing Policies

--- select ---

New Policy Name

Destinations

System

Event Log

eMail

sysadmin@companyname.com

weekend@companyname.com

SHMP

192.168.33.24

Selected Outlet	Off	On	Cycle
<input checked="" type="checkbox"/> Current Outlet	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
<input type="checkbox"/> Outlet 1	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<input type="checkbox"/> Outlet 2	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<input type="checkbox"/> Outlet 3	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

On this page, you can select an existing policy to modify, or create a new policy. The table on this page lists all the configured alert destinations available.

► **To create an Alert Policy:**

1. Choose Alerts > Alert Policy Editor.
2. Type a descriptive policy name in the New Policy Name field (or select an existing policy to modify from the Existing Policies drop-down list).
3. Check a destination in the Destinations table to add it to the policy. A single policy can notify multiple destinations. For example, you can record the alert in the event log AND e-mail a system administrator.

- Event Log: causes the Dominion PX to record alert notifications in the system log.
- Addresses listed under eMail: causes the Dominion PX to send alert notifications to the specified e-mail address.
- Addresses listed under SNMP: causes an SNMP trap to be sent to the specified IP address.
- Current Outlet: allows you to set the power state of the outlet that generated the alert. Choose to turn the outlet OFF or ON, or to cycle the power to the outlet.

*Note: Current Outlet applies only when the event is an outlet event. It has no effect for other types of events. See **Creating Alerts** (on page 138).*

- Outlets listed under Switch Outlet: allows you to set the power state of the selected outlets. Choose to turn the outlets OFF or ON, or to cycle power to the outlets.
4. Click Create to create the new policy, or click Modify if modifying an existing one.

Note: For the Dominion PX models without outlet switching, the Current Outlet and Switch Outlet destinations have no effect.

These policies are now available as a response when creating an Alert. When the alert is triggered, outlets are switched and alert notifications are sent to the event log, e-mail accounts, and SNMP managers as dictated by the selected policy.

When Event Log is set as a destination, alert events are sent to all logging services enabled on the Event Logs page. This can result in duplicate messages if the email and SNMP destinations for this Policy are the same as those used for event logging. In this case, select different SNMP and email destinations to avoid duplicate notices.

Creating Alerts

The Alert Configuration page is where you specify how the Dominion PX responds to certain events. First describe an event that triggers an alert and then select the policy the Dominion PX should take in response.

Alert Configuration

You may want to [adjust outlet sensor thresholds](#) according to your needs.

Event	Event Direction	Policy	Destinations	
Unit: temperature above upper critical threshold	Assert & Deassert	System Event Log	Event Log	Delete
Circuit Breaker 2: Tripped	Assert	Outlet Off + SNMP	SNMP: 192.168.55.212 switch off current outlet	Delete
Outlet 1: current above upper critical threshold	Assert & Deassert	System Event Log	Event Log	Delete

Event:
Event Direction:
Policy:
 [Edit Policies](#)

► **To Create an Alert:**

1. Choose Alerts > Alert Configuration. The Alert Configuration page opens.
2. Under the Event drop-down list, select the segment this event affects.
 - Unit: refers to the Dominion PX device. Temperature refers to the internal temperature as measured on the PCB board.
 - Line: refers to a current carrying line. Three-phase PDUs have three current lines, and single-phase PDUs only have one.
 - Outlet: refers to a specific, single outlet on the Dominion PX device.
 - Circuit Breaker: refers to an internal circuit breaker that governs current to a group of outlets.
 - Environmental Temperature: refers to the temperature as measured by external temperature probes. The Dominion PX must have environmental temperature probes configured and connected to the PDU for this alert event to trigger.
 - Environmental Humidity: refers to the humidity as measured by external humidity probes. The Dominion PX must have environmental humidity probes configured and connected to the PDU for this alert event to trigger.
 - Environmental Contact: refers to the contact closure status as detected by external contact closure probes. The Dominion PX must have contact closure probes configured and connected to the PDU for this alert event to trigger.

3. If you selected a Line, Outlet, or Circuit Breaker segment, indicate the specific line, outlet, or circuit breaker using the new drop-down list that appears.
4. Select an alert event that occurs to the specified segment. The list of events depends on the selected segment.
5. Pick an event direction. This describes how a numeric sensor's threshold must be exceeded or how a discrete sensor changes its state to trigger the alert.
 - Assert & Deassert: causes the alert to trigger when the numeric sensor's measured value moves past a threshold in either direction or when the discrete sensor's state change occurs.
 - Assert: causes this alert to trigger only when the numeric sensor's measured value moves past the threshold (above an upper threshold or below a lower threshold), or when the discrete sensor changes its state from *Normal* to *Alarmed*. This means the status of the described event transits from FALSE to TRUE.
 - Deassert: causes this alert to trigger only when the numeric sensor's measured value returns towards "normal" from beyond the threshold (below an upper threshold or above a lower threshold), or when the discrete sensor changes its state from *Alarmed* to *Normal*. This means the status of the described event transits from TRUE to FALSE.

For example, if you select "Environmental Temperature above upper critical threshold" and set the event direction to Assert & Deassert, the selected policy executes when the temperature of the cabinet exceeds the critical threshold. When the environment cools and the temperature drops below the critical threshold, the policy executes again.

6. Select a policy to execute from the Policy drop-down list. This list includes all of the alert policies created in the Alert Policy Editor.

*Note: If the policy involves the "Current Outlet" destination, make sure you select "Outlet" as the event, or the "Current Outlet" destination has no effect. See **Creating Alert Policies** (on page 136). For the outlet current threshold events, avoid choosing an alert policy that cycles the power to "Current Outlet" because the "cycle current outlet" destination may generate the infinite output cycle loop.*

7. Click Add.

Added alerts are now tracked by the Dominion PX. When an alert's event conditions are met, the associated policy executes.

Note: If Environmental Temperature or Environmental Humidity is selected as part of the Event, an alert event is created for each Temperature or Humidity sensor. These event alerts can be deleted so that only the ones you want are present.

Note: It is possible for an alert to set the same outlet state twice. For example, a temperature threshold Alert is created with the Event Direction set to Assert & Deassert. This alert calls a policy that turns the outlet OFF. In such a scenario, the alert triggers the outlet OFF policy once when the temperature rises above the threshold, and once more when the temperature drops below the threshold. Any event logs recording the outlet state note that the power to this outlet was turned OFF twice in a row.

Sample Alerts

Sample Outlet-Level Alert

In this example, we want the Dominion PX to notify us when the current draw on a specific outlet (Outlet 6) approaches the critical limit. To do that we would set up an alert like this:

- Event: Outlet; Outlet 6 (6); current above upper critical threshold
- Event Direction: Assert & Deassert
- Policy: Log + Notify

We select "Outlet" to indicate we are measuring at the outlet level. We then specify "Outlet 6 (6)" because that is the outlet in question and select "current above upper non-critical threshold" because we want to know when the PDU crosses into the warning range BEFORE the current draw is at critical levels.

The event direction is set to "Assert & Deassert." In this case, we want to know when the current on the outlet is higher than normal AND we want to know when it has returned to normal.

For the policy, we selected "Log + Notify." Our example policy has Event Log, the IP address of an SNMP manager, and the email address of the facilities manager checked. With these settings, the Dominion PX records the alert in its internal Event Log, send a trap to an SNMP manager, and email the facilities manager each time the current rises above and falls below the non-critical threshold.

Sample Unit-Level Alert

In this example, we want the Dominion PX to shut down most of its outlets if the Dominion PX device becomes too hot. However, since mission-critical servers are plugged into Outlets 1 and 2, we want to leave them running. Our alert would look something like this:

- Event: Unit; Temperature Above Upper Non-Critical Threshold
- Event Direction: Assert
- Policy: Non-Essential OFF

Here, we have specified "Unit" since the whole Dominion PX is our concern. We have set the upper non-critical temperature as our "warning" mark, and so we want the temperature crossing that threshold to trigger the alert.

The event direction is set to "Assert" only, since we only want to take action when the temperature is past the Upper-Non-Critical Threshold.

Our example policy, "Non-Essential OFF," has the Switch Outlet destination selected and Outlet 1 and Outlet 2 set to ON. The remaining outlets are set to OFF to reduce the power draw through the Dominion PX and the amount of heat expelled into the rack.

Sample Environmental Alert 1

In this example, our Dominion PX is equipped with environmental temperature sensors and we want to create an alert to address abnormally high ambient temperatures. For instance, if the ventilation system in the server room were to stop working. We would place our environmental temperature sensors outside of the rack to measure the room temperature. Then we would configure an alert to look something like this:

- Event: Environmental Temperature; Temperature above critical threshold
- Event Direction: Assert
- Policy: Outlets OFF + Facilities

Here, we have configured the Dominion PX to monitor the "Environmental temperature" sensors and to trigger an alert when it measures a "Temperature above critical threshold."

The event direction is set to "Assert" only, since only want to take these actions when the temperature is above the critical threshold.

Our example policy, "Outlets OFF + Facilities," would have the following destinations checked: Switch Outlets, with all outlets set to OFF; e-mail for the system administrator and e-mail for the facilities manager. This way, all equipment powered through the Dominion PX device would power OFF to avoid damage and prevent from adding more heat to the room. The system admin and the facilities manager would both receive a notification stating that the room temperature was too high.

Sample Environmental Alert 2

We can configure a complimentary alert that looks something like this:

- Event: Environmental Temperature; Temperature above non-critical threshold
- Event Direction: Deassert
- Policy: Outlets ON + Facilities

This powers on all the outlets again when the temperature is normal. Again, we are using the environmental temperature sensors to monitor the ambient temperature of the room. This time, it checks whether the temperature is above (or below) the non-critical threshold, which is generally set as a boundary between normal and warning states.

The event direction is set to "Deassert" only, since we only want to power ON the outlets again when the ambient temperature *stops* being above the non-critical threshold. This would indicate that the temperature has dropped below the warning level and is now normal again.

Our example policy, "Outlets ON + Facilities," would have the following destinations checked: Switch Outlets with all outlets set to ON; email for the system administrator and email for the facilities manager. This way, when the temperature returns to normal (for example, if the ventilation system works properly again), the Dominion PX powers on all of its outlets. Additionally, the system administrator and the facilities manager receive e-mail notification stating that the room temperature dropped below the warning level.

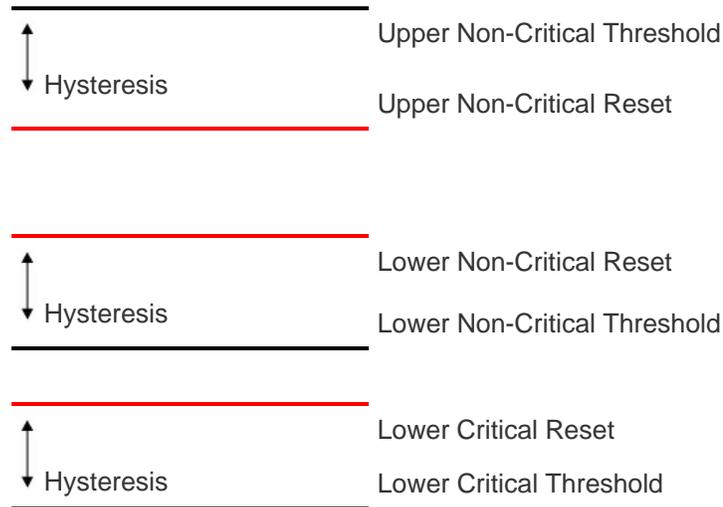
A Note about Untriggered Alerts

In some cases, a measurement exceeds a threshold causing the Dominion PX to generate an alert. The measurement then returns to a value within the threshold, but the Dominion PX does not generate an alert message for the Deassertion event. Such scenarios can occur due to the hysteresis tracking the Dominion PX uses.

What is Threshold Hysteresis?

The hysteresis setting determines when a threshold condition is reset. This diagram illustrates how hysteresis values relate to thresholds:





The hysteresis values define a reset threshold. For upper thresholds, the measurement must fall past this reset threshold before a deassertion event is generated. For lower thresholds, the measurement must rise above this reset threshold before a deassertion event is generated.

See **Default Hysteresis Values for Thresholds** (on page 253) for default hysteresis values of each measurement type.

How to Disable the Hysteresis

By default, the Dominion PX assigns a hysteresis value for each setting in the Thresholds panels on the Outlet Setup and PDU Setup pages. You can disable the hysteresis for any setting.

► To disable a specific hysteresis:

1. Access the desired page:
 - To access the Outlet Setup page, choose Details > Outlet Setup.
 - To access the PDU Setup page, choose Device Settings > PDU Setup.
2. Type 0 (zero) for the hysteresis setting you want to disable in the Thresholds panel.

Tip: To re-enable the use of the disabled hysteresis setting, type a non-zero value to replace the zero value.

Example: When Hysteresis is Useful

This example demonstrates when a deassertion hysteresis is useful.

The current critical threshold for Outlet 1 is set to 10 amps (A). The current draw rises to 11A, triggering a Current Critical alert. The current then continues to fluctuate between 9.8A and 11A.

With the hysteresis set to 0.9A, the Dominion PX continues to indicate that the current in Outlet 1 is above critical. With the hysteresis disabled (that is, set to zero), the Dominion PX would de-assert the condition each time the current dropped to 9.9A, and re-assert the condition each time the current reached 10A or higher. With the fluctuating current, this could result in a number of repeating SNMP traps, and/or an e-mail account full of repeating SMTP alert notifications.

Example: When to Disable Hysteresis

This is an example of when you want to disable the use of hysteresis for outlets.

The upper non-critical threshold for current in Outlet 2 is set to 8A. In normal usage, Outlet 2 draws 7.6A of current. A spike in demand causes the current to reach 9A, triggering an alert. The current then settles to the normal draw of 7.6A.

With the hysteresis disabled (that is, set to zero), the Dominion PX de-asserts the condition once the current drops to 7.9A. If the hysteresis remained enabled and the current never dropped to 7.0A, the outlet would still be considered above non-critical. The condition would not de-assert, even if the current draw returned to normal.

Setting Up Event Logging

By default, the Dominion PX captures certain system events and saves them in a local (internal) event log. You can expand the scope of the logging to also capture events in the NFS, SMTP, and SNMP logs.

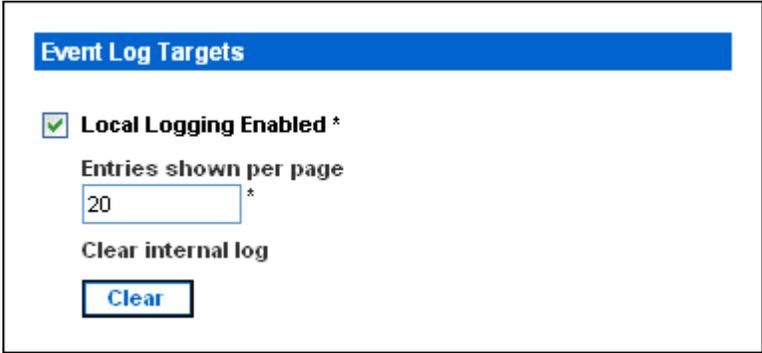
Note: When configuring the Dominion PX to use more than one logging method, configure each method individually and apply the changes before configuring the next.

Configuring the Local Event Log

Follow this procedure to determine whether the local logging function is enabled and which types of events are logged in the local log.

► **To configure the local event log:**

1. Choose Device Settings > Event Log. The Event Log Settings page opens. The Local Logging panel appears first. This panel controls the local event log.



The screenshot shows a web interface panel titled "Event Log Targets" with a blue header. Below the header, there is a checked checkbox labeled "Local Logging Enabled *". Underneath, the text "Entries shown per page" is followed by a text input field containing the number "20" and an asterisk. Below that is the text "Clear internal log" and a blue button labeled "Clear".

2. The local event log is enabled by default. To turn it off, deselect the Local Logging Enabled checkbox.
3. By default, 20 log entries appear on each page of the local event log when it is displayed. To change this, type a different number in the Entries Shown Per Page field.
4. To clear all events from the local event log:
 - a. Click Clear. The button changes to Really Clear and you are prompted to click only if you really want to clear the log.
 - b. Click Really Clear to complete the clear operation, or click Cancel to terminate it.

- By default, when the local event log is enabled, seven event types appear in the Event Log Assignments panel to the right. All are enabled by default. To disable any of these event types, deselect the appropriate checkboxes.

Event Log Assignments	
Event	List
Outlet Control	<input checked="" type="checkbox"/> *
User/Group Administration	<input checked="" type="checkbox"/> *
Security Relevant	<input checked="" type="checkbox"/> *
User Activity	<input checked="" type="checkbox"/> *
Device Operation	<input checked="" type="checkbox"/> *
Outlet/Unit/Environmental Sensors	<input checked="" type="checkbox"/> *
Device Management	<input checked="" type="checkbox"/> *
Virtual Device Management	<input checked="" type="checkbox"/> *

*Note: See **Event Types** (on page 253) for a more detailed explanation of these event types.*

- When you are finished, click Apply. Local logging is configured.

Viewing the Local Event Log

To display the internal event log, choose Maintenance > View Event Log.

Event Log

Page (13 total): [First](#) [Prev](#) 1 2 3 [Next](#) [Last](#)

Date	Event	Description
2000-02-18 02:23:07	User Activity	User logged in successfully, user 'admin' from host '192.168.43.181'.
2000-02-18 01:28:19	User Activity	User logged in successfully, user 'admin' from host '192.168.43.181'.
2000-02-18 01:27:11	Device Operation	Device successfully started
2000-02-18 01:26:03	Device Operation	Board Reset performed by user 'admin', user 'admin' from host '192.168.43.181'.
2000-02-18 01:23:39	Device Management	The device update has started
2000-02-18 01:21:49	User Activity	User logged in successfully, user 'admin' from host '192.168.43.181'.
2000-02-17 04:52:10	User Activity	User logged out, user 'admin' from host '192.168.43.181'.
2000-02-17 04:52:10	User Activity	User session timeout, user 'admin' from host '192.168.43.181'.
2000-02-17 04:13:47	User Activity	User logged in successfully, user 'admin' from host '192.168.43.181'.
2000-02-17 04:13:42	Security Relevant	User login failed, user 'admin' from host '192.168.43.181'.
2000-02-17 04:13:29	User Activity	User logged out, user 'admin' from host '192.168.43.181'.
2000-02-17 04:13:29	User Activity	User session timeout, user 'admin' from host '192.168.43.181'.
2000-02-17 03:43:18	User Activity	User logged in successfully, user 'admin' from host '192.168.43.181'.
2000-02-14 02:40:56	User Activity	User logged out, user 'admin' from host '192.168.43.181'.
2000-02-14 02:40:56	User Activity	User session timeout, user 'admin' from host '192.168.43.181'.
2000-02-14 02:10:44	User Activity	User logged in successfully, user 'admin' from host '192.168.43.181'.
2000-02-13 23:28:11	User Activity	User logged out, user 'admin' from host '192.168.43.181'.
2000-02-13 23:28:11	User Activity	User session timeout, user 'admin' from host '192.168.43.181'.
2000-02-13 22:28:36	User Activity	User logged in successfully, user 'admin' from host '192.168.43.181'.
2000-02-13 12:01:50	User Activity	User logged out, user 'admin' from host '192.168.32.33'.

[Clear](#)

Each event entry in the local log consists of:

- Date and time of the event
- Type of the event
- A description of the event (For example, for an authentication event, the entry in the log shows the user's login name and the IP address of the user's computer.)

*Note: By default, the local log displays 20 entries per page. See **Configuring the Local Event Log** (on page 145) if you want to change this number.*

Configuring the NFS Logging

This procedure describes how to enable the Network File System (NFS) logging function and determine which types of events are recorded in the NFS log file.

► **To configure the NFS logging:**

1. Choose Device Settings > Event Log. The Event Log Settings page opens. The NFS Logging panel controls NFS logging.

2. Select the NFS Logging Enabled checkbox.
3. Type the IP address of the NFS server in the NFS Server field.
4. Type the name of the shared NFS directory in the NFS Share field.
5. Type the name of the NFS log file in the NFS Log File field. Default is evtlog.
6. By default, when NFS logging is enabled, seven event types appear in the Event Log Assignments panel to the right. All are disabled by default. To enable any of these event types, select the corresponding checkboxes.

Event Log Assignments		
Event	List	NFS
Outlet Control	<input checked="" type="checkbox"/> *	<input checked="" type="checkbox"/> *
User/Group Administration	<input checked="" type="checkbox"/> *	<input checked="" type="checkbox"/> *
Security Relevant	<input checked="" type="checkbox"/> *	<input checked="" type="checkbox"/> *
User Activity	<input checked="" type="checkbox"/> *	<input type="checkbox"/> *
Device Operation	<input checked="" type="checkbox"/> *	<input checked="" type="checkbox"/> *
Outlet/Unit/Environmental Sensors	<input checked="" type="checkbox"/> *	<input checked="" type="checkbox"/> *
Device Management	<input checked="" type="checkbox"/> *	<input type="checkbox"/> *
Virtual Device Management	<input checked="" type="checkbox"/> *	<input checked="" type="checkbox"/> *

7. Click Apply. NFS logging is configured.

Configuring the SMTP Logging

You can enable the Simple Mail Transfer Protocol (SMTP) logging function and determine which types of events are recorded in the SMTP log file.

► To configure the SMTP logging:

1. Ensure the SMTP server settings have been configured properly. See **Configuring the SMTP Settings** (on page 62).
2. Choose Device Settings > Event Log. The Event Log Settings page opens. The SMTP Logging panel controls SMTP logging.

SMTP Logging Enabled *

Receiver Email Address

*

You have to configure SMTP server [here](#) before you can use SMTP destinations!

3. Select the SMTP Logging Enabled checkbox.
4. Type the receiver's email address in the Receiver Email Address field.
5. By default, when SMTP logging is enabled, seven event types appear in the Event Log Assignments panel to the right. All are disabled by default. To enable any of these event types, select the appropriate checkboxes.

Event Log Assignments

Event	List	SMTP
Outlet Control	<input checked="" type="checkbox"/> *	<input checked="" type="checkbox"/> *
User/Group Administration	<input checked="" type="checkbox"/> *	<input checked="" type="checkbox"/> *
Security Relevant	<input checked="" type="checkbox"/> *	<input checked="" type="checkbox"/> *
User Activity	<input checked="" type="checkbox"/> *	<input type="checkbox"/> *
Device Operation	<input checked="" type="checkbox"/> *	<input checked="" type="checkbox"/> *
Outlet/Unit/Environmental Sensors	<input checked="" type="checkbox"/> *	<input checked="" type="checkbox"/> *
Device Management	<input checked="" type="checkbox"/> *	<input type="checkbox"/> *
Virtual Device Management	<input checked="" type="checkbox"/> *	<input checked="" type="checkbox"/> *

6. Click Apply. SMTP logging is configured.

*Note: You must configure the SMTP settings first, for SMTP logging to work. See **Configuring the SMTP Settings** (on page 62).*

Configuring the SNMP Logging

Event logging can be performed by sending SNMP traps to a third-party SNMP manager. See **Using SNMP** (on page 165) for instructions on enabling SNMP Event Logging.

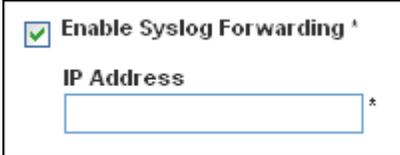
Configuring the Syslog Forwarding

To make the Dominion PX automatically forward events to a specific destination, enable the syslog forwarding function and determine which types of events should be logged in the syslog record.

Note: After enabling Syslog Forwarding, a "--MARK--" message may appear in the Syslog record every 20 minutes. This is a keep-alive method used by the Dominion PX.

► **To configure the Syslog Forwarding:**

1. Choose Device Settings > Event Log. The Event Log Settings page opens. The Syslog Forwarding panel controls forwarding of system logs.



Enable Syslog Forwarding ^

IP Address *

2. Select the Enable Syslog Forwarding checkbox.
3. Type an IP address in the IP Address field. This is the address to which syslog is forwarded.
4. By default, when Syslog Forwarding is enabled, seven event types appear in the Event Log Assignments panel to the right. All are disabled by default. To enable any of these event types, select the appropriate checkboxes.

Event Log Assignments		
Event	List	Syslog
Outlet Control	<input checked="" type="checkbox"/> *	<input checked="" type="checkbox"/> *
User/Group Administration	<input checked="" type="checkbox"/> *	<input checked="" type="checkbox"/> *
Security Relevant	<input checked="" type="checkbox"/> *	<input type="checkbox"/> *
User Activity	<input checked="" type="checkbox"/> *	<input checked="" type="checkbox"/> *
Device Operation	<input checked="" type="checkbox"/> *	<input checked="" type="checkbox"/> *
Outlet/Unit/Environmental Sensors	<input checked="" type="checkbox"/> *	<input type="checkbox"/> *
Device Management	<input checked="" type="checkbox"/> *	<input checked="" type="checkbox"/> *
Virtual Device Management	<input checked="" type="checkbox"/> *	<input checked="" type="checkbox"/> *

5. Click Apply. Syslog Forwarding is configured.

Note: If you want to disable Syslog forwarding, deselect all checked event types under the Syslog column and click Apply. Then deselect Enable Syslog Forwarding. If event types are still selected in the Syslog column when you disable Syslog forwarding, you may be unable to deselect those event types from the internal event log list.

Outlet Grouping

Using the Outlet Grouping feature, you can combine outlets from separate Dominion PX devices into a single logical group, allowing control from a single Dominion PX. Outlets that are grouped together power on and power off together in unison, making outlet grouping ideal for servers with power supplies plugged into multiple Dominion PX devices.

Users, or the group they belong to, must have the Outlet Group Configuration permission under User/Group System Permissions in order to manage or access an Outlet Group. Only locally authenticated users may perform actions on outlet groups.

Note: Outlet Grouping supports adding outlets from up to four other Dominion PX devices. All PDUs must be accessible over IP and must be running firmware version 1.1 or higher.

Identifying Other Dominion PX Devices

To add outlets from other Dominion PX devices, you must first identify which Dominion PX devices are sharing their outlets.

► **To identify other Dominion PX devices:**

1. Choose Outlet Groups > Outlet Group Devices. The Outlet Group Devices page opens.

Outlet Group Devices

Name: **IP Address:** [Add / Modify](#)

Username: **Password:** (leave empty for 'Outlet Groups' to use user credentials)

Name	IP Address	Outlets	Model	Status	Access User	
Local Device	127.0.0.1	20	DPCR20-20	alive	n/a	Delete
Weaver's PX	192.168.42.96	n/a	n/a	unknown	admin	Delete

2. Type a name to identify the Dominion PX device you want to add in the Name field.
3. Type the IP Address of the Dominion PX device you want to add in the IP Address field.
4. Type the **admin** username and password in the Username and Password fields. Do NOT leave these fields blank as they can authenticate on the Dominion PX device being added.
5. Click Add/Modify. The new Dominion PX device is now available for outlet grouping.

To modify the name or the Username and Password used to access a participating Dominion PX device, retype the information for the same Dominion PX device and click Add/Modify again.

Note: You can re-add the Dominion PX device you are accessing (if you deleted it from the list) or modify its details by using the IP address 127.0.0.1.

Grouping Outlets Together

Once the participating Dominion PX devices have been added to list of outlet group devices, their individual outlets can be grouped together. Outlets that are grouped together power on and power off in unison, using a control panel from the Dominion PX device where the outlet group was created.

► To group outlets together:

1. Choose Outlet Groups > Outlet Group Editor. The Outlet Group Editor page opens.

Outlet Group Editor

Outlet Groups:

Name:

Comment:

Capabilities:
 On Off Cycle

Collection Of Real Outlets:

Device	Outlets
Local Device 127.0.0.1	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7 <input checked="" type="checkbox"/> 8
Weaver's PX 192.168.42.98	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7 <input checked="" type="checkbox"/> 8

2. Type a name for the outlet group in the Name field. It is a good idea to give the outlet group a recognizable name that helps identify the device(s) connected to it.

Note: You cannot modify the name of an outlet group after the group is created.

3. Type a comment for the outlet group in the Comment field. This can be used to further identify device(s) powered by the group.
4. Under the Capabilities field, check the boxes of the Power Control abilities you want available for this outlet.

5. A list of available Dominion PX devices and their outlets appears under Collection of Real Outlets. Select the checkbox representing the desired physical outlet to make it part of the outlet group. All outlets that are selected are grouped together when you click Create.

Note: You should not add a physical outlet to more than one outlet group.

6. Click Create. The outlet group is created and added to the Outlet Groups list.

Grouped outlets are designed to be controlled together. Avoid doing anything to affect these outlets individually, such as turning one of the outlets ON or OFF, or unplugging one of the participating Dominion PX devices. Once grouped, power control to those outlets should be managed from the Outlet Groups List.

Viewing and Controlling Outlet Groups

Any outlet groups created from this Dominion PX device appear in the Outlet Groups List. From this list, you can power ON, Power OFF, or cycle power to the outlet group (if the capability is available).

► **To control the power to an outlet group:**

1. Choose Outlet Groups > Outlet Group Details. The Outlet Groups List appears.

Outlet Groups		
Name	Control	Outlets
Test Box 1 (Testing group's server in the first server rack)	On Off Cycle	off off
Marketing File Server (Purple box in the server rack. Marketing Materials)	On Off Cycle	off off off
Weaver's Test Server (Weaver's new server. temp install. Plugged into both outlet 8s)	On Off Cycle	on on

Note: Only outlet groups created through this specific Dominion PX device appear in this Outlet Groups list. Outlet groups created through another Dominion PX device do not appear here, even if they contain outlets from this device.

2. To turn an outlet group on, off, or cycle the power to it, click On, Off, or Cycle in the row for the outlet group.
3. You are prompted to confirm your choice. Click OK to proceed.

4. The page refreshes once to indicate that the desired command was performed, and again a few seconds later to update the status of the outlet group.

Note: The page must finish loading or refreshing before selecting an action. If you select an action before the page has finished updating the status of all outlet groups, the command is ignored.

If you want to view or edit the composition of an outlet group, clicking on the name of the outlet group in the list takes you to the Outlet Group Editor for the selected outlet group.

Editing or Deleting Outlet Groups

1. Choose Outlet Groups > Outlet Group Editor. The Outlet Group Editor page opens.
2. Select the desired outlet group from the Outlet Groups drop-down list.
3. The details for the outlet group appear. Change the comment, capabilities, or any of the included Real Outlets if you are modifying the group.
4. Click Modify to save any changes if you are modifying the outlet group, or click Delete to remove the group from the outlet groups list.

Note: You cannot modify the name of an outlet group after the group is created.

Deleting Outlet Group Devices

► **To delete a Dominion PX device from outlet grouping when it is no longer available or in use:**

1. Choose Outlet Groups > Outlet Group Devices. The Outlet Group Devices page opens, displaying a list of known Dominion PX devices.
2. Click Delete for the Dominion PX device you want to remove from outlet grouping.

Note: If you delete a Dominion PX device that still has outlets in a group, it removes the associated outlets from that group, but the group still exists. Remove the group itself using the Outlet Group Editor. You should not delete the host device (the Dominion PX device you are currently accessing) from the Outlet Group Devices list. If you do, you can add it back to the list using the IP address 127.0.0.1.

Setting the FIPS Mode

The Dominion PX supports the Security Requirements for Cryptographic Modules of the Federal Information Processing Standards (FIPS), which is defined in the *FIPS PUB 140-2* (<http://www.nist.gov/cmvp/>), *Annex A: Approved Security Functions*. These standards are used to protect the Federal government's sensitive information with the cryptographic-based security systems in the U.S. and Canada.

FIPS Limitations

In the FIPS mode, only the FIPS approved security algorithms are supported, resulting in the necessity to disable or stop supporting some algorithms implemented with the Dominion PX.

After enabling the FIPS:

- HTTP access to the Dominion PX is NOT supported, and HTTPS access is forced automatically.
- Telnet access to the Dominion PX is NOT supported, but SSH access is still supported.

The following SSH algorithms are supported:

- Ciphers:
 - AES128-CBC
 - 3DES-CBC
 - AES256-CBC
- Hash:
 - HMAC-SHA1-96
 - HMAC-SHA1
- LDAP authentication is NOT supported, and only the LDAPS (SSL enabled) authentication is supported.
You must use FIPS required ciphers for SSL.
- Radius authentication is NOT supported.
- The SNMP v1/v2c protocol is NOT supported, but the SNMP v3 protocol is still supported.

If the SNMP v3 protocol is enabled, the Dominion PX automatically forces the SNMP v3 encryption, which cannot be reset. After enabling this protocol, you must:

- Enable the authentication and privacy to set the security level to authPriv.
- Select SHA as the authentication algorithm.
- Select AES as the privacy algorithm.

Note: MD5 and DES are NOT FIPS approved algorithms.

- Only IPMI v2.0 is supported. The following algorithms are supported in the FIPS mode:
 - Authentication algorithms:
 - RAKP-HMAC-SHA1
 - RAKP-HMAC-SHA256
 - Integrity algorithms:
 - HMAC-SHA1-96
 - HMAC-SHA256-128
 - Encryption algorithms:
 - AES-CBC-128
 - ipmitool:
 - You must use the *lanplus* interface. See **IPMI in the FIPS Mode** (on page 251).
 - The parameter used with the -C option for ciphersuite must be 3.

Impact on the Raritan Product Integration

The Dominion PX can be integrated with other Raritan products. See **Integration** (on page 216). However, some integration is affected by the limitations caused by the FIPS mode.

- Currently the CommandCenter Secure Gateway (CC-SG) CANNOT manage or control the Dominion PX running in the FIPS mode, but a new release of CC-SG (version 5.3) scheduled for the second quarter of 2012 will implement its management or control.
- Power IQ must use SNMP v3 to manage or control the Dominion PX running in the FIPS mode.

Configuring the FIPS Mode

Only the **admin** user can enable or disable this FIPS capability on the Dominion PX using any interfaces. The Dominion PX can send SNMP v1/v2c traps whenever the FIPS mode is enabled or disabled.

► To activate the FIPS mode:

1. Choose Device Settings > FIPS Setting.
2. Click Enable FIPS.
3. An alert message appears, listing the limitations that will be applied in the FIPS mode.
4. Click Really Enable FIPS to confirm activating the FIPS mode.
5. The Dominion PX will reset. Wait until the reset is complete.

After the FIPS mode is enabled, the message "FIPS mode is set" is displayed in blue in the status panel. See **Status Panel** (on page 45).

▶ **To deactivate the FIPS mode:**

1. Choose Device Settings > FIPS Setting.
2. Click Disable FIPS.
3. An alert message appears, stating that weak ciphers are permitted after deactivating the FIPS mode.
4. Click Really Disable FIPS to confirm deactivating the FIPS mode.
5. The Dominion PX will reset. Wait until the reset is complete.

After the FIPS mode is disabled, the message "FIPS mode is not set" is displayed in the status panel. See **Status Panel** (on page 45).

Diagnostics

The Dominion PX provides the following tools in the web interface for diagnosing potential networking issues.

- Network Interface
- Network Statistics
- Ping Host
- Trace Route to Host
- Device Diagnostics

Network Interface Page

The Dominion PX provides information about the status of your network interface.

▶ **To view information about your network interface:**

- Choose Diagnostics > Network Interface. The Network Interface page opens.

The following information is displayed:

- Whether the Ethernet interface is up or down.
- Whether the gateway is pingable or not.
- The LAN port that is currently active.

▶ **To refresh this information:**

- Click Refresh.

Network Statistics Page

The Dominion PX provides statistics about your network interface.

▶ **To view statistics about your network interface:**

1. Choose Diagnostics > Network Statistics. The Network Statistics page opens.

2. Click Refresh. The relevant information is displayed in the Result field.

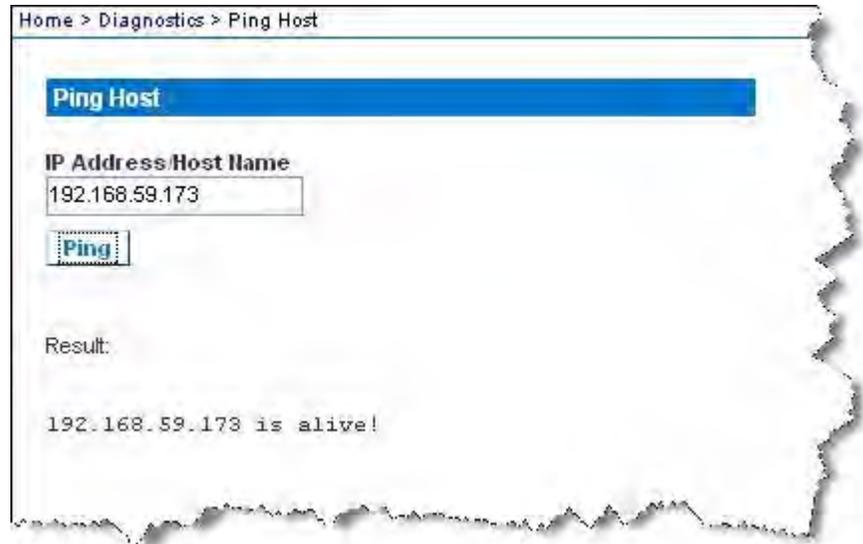


Ping Host Page

Ping is a network tool used to test whether a particular host or IP address is reachable across an IP network. Using the Ping Host page, you can determine if a target server or another Dominion PX is accessible.

► **To ping the host:**

1. Choose Diagnostics > Ping Host. The Ping Host page appears.



2. Type either the hostname or IP address into the IP Address/Host Name field.

Note: The host name cannot exceed 232 characters in length.

Trace Route to Host Page

Trace route is a network tool used to determine the route taken to the provided hostname or IP address.

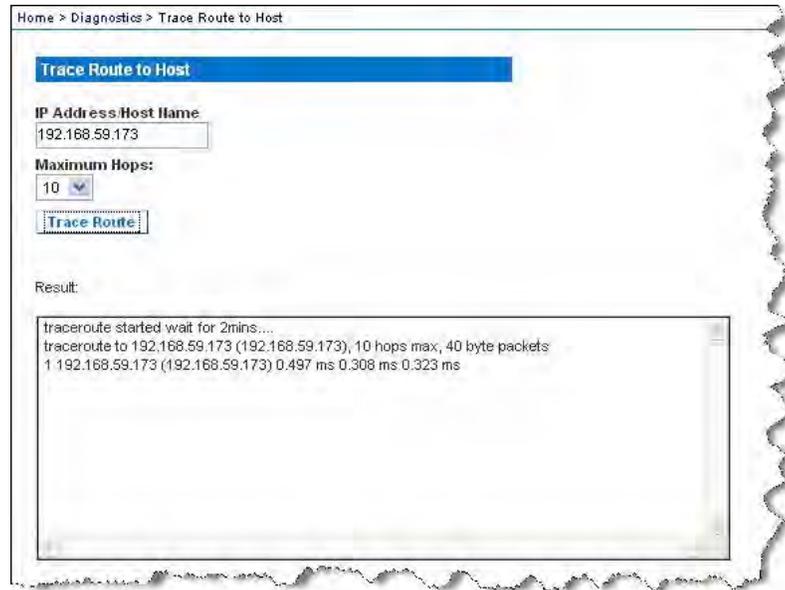
► **To trace the route to the host:**

1. Choose Diagnostics > Trace Route to Host. The Trace Route to Host page opens.
2. Type either the IP address or host name into the IP Address/Host Name field.

Note: The host name cannot exceed 232 characters in length.

3. Choose the maximum hops from the drop-down list (5 to 50 in increments of 5).

4. Click Trace Route. The trace route command is executed for the given hostname or IP address and the maximum hops. The output of trace route is displayed in the Result field.



Saving a Device Diagnostics File

When instructed by Raritan Technical Support, you can download the diagnostics file from the Dominion PX device and send it to Raritan Technical Support for troubleshooting.

► **To download a device diagnostics file:**

1. Choose Diagnostics > Device Diagnostics. The Device Diagnostics page opens.
2. Click Save To File. A File Download dialog appears.
3. Click Save to save the file onto your computer.

Using Online Help

The Dominion PX User Guide is also provided in the form of online help, and accessible over the Internet.

To use online help, Active Content must be enabled in your browser. If you are using Internet Explorer 7, you must enable Scriptlets. Consult your browser help for information on enabling these features.

► **To use the Dominion PX online help:**

1. Click the User Guide link in the Status Panel. The online help opens in the default web browser.
2. To view the content of any topic, click the topic in the left pane. Then its content is displayed in the right pane.
3. To select a different topic, do any of the following:
 - To view the next topic, click the Next icon  in the toolbar.
 - To view the previous topic, click the Previous icon .
 - To view the first topic, click the Home icon .
4. To expand or collapse a topic that contains sub-topics, do the following:
 - To expand any topic, click the white arrow  prior to the topic, or double-click that topic. The arrow turns into a black, gradient arrow , and sub-topics appear below the topic.
 - To collapse any expanded topic, click the black, gradient arrow  prior to the topic, or double-click the expanded topic. The arrow then turns into a white arrow , and all sub-topics below that topic disappear.
5. To search for specific information, type the key word(s) or string(s) in the Search text box, and press Enter or click the Search icon  to start the search.
 - If necessary, select the "Match partial words" checkbox to include information matching part of the words entered in the Search text box.

The search results are displayed in the left pane.

6. To have the left pane show the list of topics, click the Contents tab at the bottom.
7. To show the Index page, click the Index tab.
8. To email any URL link to the currently selected topic to any person, click the "Email this page" icon  in the toolbar.

9. To email your comments or suggestions regarding the user guide to Raritan, click the "Send feedback" icon .
10. To print the currently selected topic, click the "Print this page" icon .

Chapter 6 Using SNMP

This SNMP section helps you set up the Dominion PX for use with an SNMP manager. The Dominion PX can be configured to send traps to an SNMP manager, as well as receive GET and SET commands in order to retrieve status and configure some basic settings.

In This Chapter

Enabling SNMP	165
Configuring the SNMP Traps.....	169
SNMP Gets and Sets	171

Enabling SNMP

To communicate with an SNMP manager, you must first enable the SNMP agent on the Dominion PX device.

► **To enable SNMP:**

1. Choose Device Settings > SNMP Settings. The SNMP Settings page opens.

SNMP Settings

Enable SHMP Agent *

Enable SHMP v1 / v2c Protocol *

Read Community
 *

Write Community
 *

Enable SHMP v3 Protocol *

Force Encryption *

System Location
 *

System Contact
 *

Click [here](#) to view the PX (PCS20-20) SNMP MIB.

2. Select the Enable SNMP Agent checkbox to enable the Dominion PX to communicate with external SNMP managers. A number of options become available.
3. Select the Enable SNMP v1 / v2c Protocol checkbox to enable communication with an SNMP manager using SNMP v1 or v2c protocol. Type the SNMP read-only community string in the Read Community field and the read/write community string in the Write Community field.

*Note: In the FIPS mode, SNMP v1 / v2c protocol is NOT supported so its settings become unavailable. See **FIPS Limitations** (on page 156).*

4. Select the Enable SNMP v3 Protocol checkbox to enable communication with an SNMP manager using SNMP v3 protocol.
 - Additionally, select the Force Encryption checkbox to force using encrypted SNMP communication.

In the FIPS mode, this encryption checkbox is automatically selected when you enable the SNMP v3 protocol. See **FIPS Limitations** (on page 156).

Note: To perform SNMP v3 operations successfully, make sure the name of your user group does NOT contain any spaces.

5. Type the SNMP MIBII sysLocation value in the System Location field.
6. Type the SNMP MIBII sysContact value in the System Contact field.
7. Click on the link at the bottom of the page to download an SNMP MIB for your Dominion PX to use with your SNMP manager.
8. Click Apply. The SNMP configuration is set.

Configuring Users for Encrypted SNMP v3

The SNMP v3 protocol allows for encrypted communication. To take advantage of this, users need to have an Encryption Phrase, which acts as a shared secret between them and the Dominion PX. This encryption phrase can be set on the User Management page.

► **To configure users for SNMP v3 encrypted communication:**

1. Choose User Management > Users & Groups. The User/Group Management page opens.

The screenshot shows the 'User Management' web interface. At the top, there is a blue header with the text 'User Management'. Below this, there is a section titled 'Existing Users' which contains a dropdown menu with 'tester' selected and a 'Refresh' button. The main form area contains several fields: 'New User Name' (text input with 'tester'), 'Full Name' (text input with 'Ron. T'), 'Password' (text input), 'Confirm Password' (text input), a checkbox for 'Use Password as Encryption Phrase' which is unchecked, 'SNMP v3 Encryption Phrase' (password input with dots), 'Confirm SNMP v3 Encryption Phrase' (password input with dots), 'SNMP v3 authentication settings' (dropdown menu with 'SHA_1'), 'SNMP v3 privacy settings' (dropdown menu with 'AES_128'), 'Email Address' (text input with 'ront@systemname.com'), 'Mobile Number' (text input), and 'User Group' (dropdown menu with 'TrialGroup').

2. Select the user profile you want to modify from the drop-down list in the Existing Users field.

3. Type a new password for the user if necessary. The user password must be at least 8 characters long to use SNMP v3.
4. There are two ways to specify the SNMP v3 encryption phrase.
 - To use the user's password as the Encryption Phrase, select the Use Password as Encryption Phrase checkbox.
 - To specify a different encryption phrase, deselect this checkbox. Type a new phrase in the SNMP v3 Encryption Phrase field, then type it again in the Confirm SNMP v3 Encryption Phrase field. The SNMP v3 Encryption phrase must be at least 8 characters long.

*Note: In the FIPS mode, the SNMP v3 encryption is automatically forced if the SNMP v3 is enabled. Then you must specify the SNMP v3 encryption phrase for the user to use the SNMP v3 communication. See **FIPS Limitations** (on page 156).*

5. Make changes to the SNMP v3 authentication and/or privacy settings if necessary. Note that the Dominion PX only supports specific authentication and privacy algorithms if the FIPS mode is enabled.
 - Authentication: Select either MD5 or SHA_1. In the FIPS mode, only SHA_1 is supported.
 - Privacy: Select either DES or AES_128. In the FIPS mode, only AES_128 is supported.
6. Click Modify. The user is now set up for encrypted SNMP v3 communication.

Note: The admin user is the only member of the Admin group to have SNMP v3 access. All other users must be added to a different user group with SNMP v3 Access permissions in order to have SNMP v3 access.

Restarting the SNMP Agent after Adding Users

If you have just added or re-configured a user for SNMP v3 access, you must restart the Dominion PX SNMP agent before the user can log in with SNMP v3 access.

► **To restart the SNMP agent after adding users:**

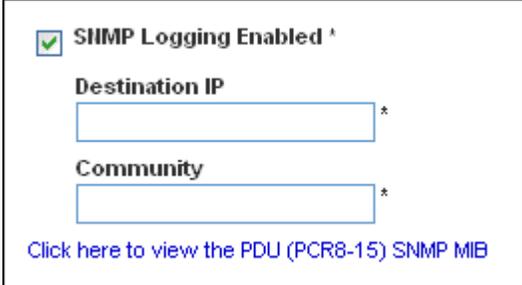
1. Choose Device Settings > SNMP Settings. The SNMP Settings page opens.
2. De-select the Enable SNMP Agent checkbox.
3. Click Apply to disable the SNMP agent.
4. Select the Enable SNMP Agent checkbox.
5. Click Apply to re-enable the SNMP agent.

Configuring the SNMP Traps

The Dominion PX automatically keeps an internal log of events that occur. See **Setting Up Event Logging** (on page 144). These events can also be used to send SNMP traps to a third party manager. Note that the Dominion PX sends traps via SNMP v2c protocol only.

► To configure the Dominion PX to send SNMP traps:

1. Choose Device Settings > Event Log. The Event Log Settings page opens. The SNMP Logging panel controls the use of SNMP traps.



SNMP Logging Enabled *

Destination IP

*

Community

*

[Click here to view the PDU \(PCR8-15\) SNMP MIB](#)

2. Select the SNMP Logging Enabled checkbox.
3. Type an IP address in the Destination IP field. This is the address to which traps are sent by the SNMP system agent.
4. Type the name of the SNMP community in the Community field. The community is the group representing the Dominion PX and all SNMP management stations.
5. To take a look at the Management Information Base (MIB), click the link labeled "Click here to view the PX (<model name>) SNMP MIB". It is located under the Community field.
6. When SNMP logging is enabled, eight event types appear in the Event Log Assignments panel to the right. All are disabled by default. To enable any of these event types, select the appropriate checkboxes.

Event Log Assignments

Event	List	SNMP
Outlet Control	<input checked="" type="checkbox"/> *	<input checked="" type="checkbox"/> *
User/Group Administration	<input checked="" type="checkbox"/> *	<input checked="" type="checkbox"/> *
Security Relevant	<input checked="" type="checkbox"/> *	<input type="checkbox"/> *
User Activity	<input checked="" type="checkbox"/> *	<input checked="" type="checkbox"/> *
Device Operation	<input checked="" type="checkbox"/> *	<input type="checkbox"/> *
Outlet/Unit/Environmental Sensors	<input checked="" type="checkbox"/> *	<input checked="" type="checkbox"/> *
Device Management	<input checked="" type="checkbox"/> *	<input type="checkbox"/> *
Virtual Device Management	<input checked="" type="checkbox"/> *	<input checked="" type="checkbox"/> *

7. Click Apply. SNMP logging is configured.
8. From the Maintenance tab, select Unit Reset to reset the Dominion PX device. You must reset the Dominion PX when enabling SNMP logging or changing the Destination IP address. If you do not, traps are not sent to the Destination IP address.

Note: You should update the MIB used by your SNMP manager when updating to a new Dominion PX release. This ensures your SNMP manager has the correct MIB for the release you are using.

Suggestion for SNMP Trap Configuration

The Dominion PX web interface allows you to specify the SNMP destinations using two menu items, which generate different types of SNMP traps as described in the table.

Menu item	Trap type	Protocol
Device Settings > Event Log	All traps described in the MIB can be generated, including the ThresholdAlarm trap.	SNMP v2c
Alerts > Alert Destinations	Only the ThresholdAlarm trap is generated.	SNMP v2c

Therefore, when configuring the Alert policy for SNMP, it is highly recommended to do the following by choosing Device Settings > Event Log:

- Select the SNMP Logging Enabled checkbox
- Specify the SNMP destination on the Event Log Settings page only (instead of doing it on the Alert Destinations page)

A False Circuit Breaker Trip Trap

If the Dominion PX generates an SNMP trap of voltage measurement failure for the circuit breaker, it indicates a false circuit breaker trip caused by the hardware failure. In that case, you have to return the PDU to Raritan for fixing the problem. Contact Raritan Technical Support when such a trap is generated.

SNMP Gets and Sets

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

- Get requests are used to retrieve information about the Dominion PX, such as the system location, and the current on a specific outlet.
- Set requests are used to configure a subset of the information, such as the SNMP system name.

Note: The SNMP system name is the Dominion PX device name. When you change the SNMP system name, the device name shown in the web interface is also changed.

The Dominion PX does NOT support configuring IPv6-related parameters using the SNMP set requests.

Valid objects for these requests are limited to those found in the SNMP MIB-II System Group and the custom Dominion PX MIB.

You must target only one item at a time with SNMP set requests. Any attempt to configure multiple targets with a single set request results in all targets receiving the last assigned value. For example, if you use SNMP to set the status of Outlet 1 to ON and Outlet 4 to OFF, both Outlet 1 and Outlet 4 are set to OFF.

The Dominion PX MIB

This MIB is available from the SNMP Settings page, the Event Logging page, or by pointing your browser to `http://<ip-address>/MIB.txt`, where `<ip-address>` is the IP address of your Dominion PX.

Layout

Opening the MIB reveals the custom objects that describe the Dominion PX system at the unit level as well as at the individual-outlet level.

As standard, these objects are first presented at the beginning of the file, listed under their parent group. The objects then appear again individually, defined and described in detail.

```

about the outlets, including sensor readings."
 ::= { groups 2 }

unitSensorsGroup
    OBJECT-GROUP
    OBJECTS { unitCurrent,
              unitVoltage,
              unitActivePower,
              unitApparentPower,
              unitCpuTemp,
              unitCircuitBreak0State,
              unitCircuitBreak1State,
              unitCircuitBreak2State,
              unitCircuitBreak0Current,
              unitCircuitBreak1Current,
              unitCircuitBreak2Current,
              unitVoltageLowerWarning,
              unitVoltageUpperWarning,
              unitVoltageLowerCritical,
              unitVoltageUpperCritical,
              unitCurrentUpperWarning,
              unitCurrentUpperCritical,
              unitTempLowerWarning,
              unitTempUpperWarning,
              unitTempLowerCritical,
              unitTempUpperCritical }
    STATUS current
    DESCRIPTION
        "A collection of objects providing unit level sensor
readings."

```

For example, the unitSensorsGroup group contains objects for sensor readings of the Dominion PX as a whole. One object listed under this group, unitCurrent, is described later in the MIB as "The value for the unit's current sensor in millamps"--the measure of the current drawn by the Dominion PX. outletCurrent, part of the outletsGroup group describes the current passing through a specific outlet.

SNMP Sets and Configurable Objects

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 Dominion PX to generate a warning and send an SNMP trap when certain parameters are exceeded.

*Note: When configuring the thresholds via SNMP set commands, ensure the value of upper critical threshold is higher than that of upper non-critical threshold. See **Setting Up Power Thresholds and Hysteresis** (on page 91) for a description of how thresholds work.*

Configuring the Hysteresis

You can configure the hysteresis values using the SNMP set command. Different from the Dominion PX web interface, SNMP accepts only integer values as the hysteresis values so decimal point values will be rejected. To set a decimal point value, you must use the web interface to change the hysteresis values.

See **A Note about Untriggered Alerts** (on page 142) for a description of how a hysteresis value works.

Disabling Outlet Switching

Using the SNMP set command, you can disable the switching of outlet states on your Dominion PX device.

For any Dominion PX device not implemented with the outlet switching function, such as an in-line monitor, you should always disable the switching function.

Refer to the Dominion PX MIB for more details.

This feature is configurable through SNMP only. Firmware upgrade does not affect this setting.

Setting Data Retrieval

You can use the SNMP set command to configure the data retrieval-related settings.

- Use "dataLogging" for enabling or disabling the data retrieval feature.
- Use "dataLoggingInterval" or "measurementsPerLogEntry" for setting the sampling period.

The dataLoggingInterval (sampling period) is equal to the value of measurementsPerLogEntry times three. For example, if the measurementsPerLogEntry is set to 20, the sampling period becomes 60 seconds (20x3=60).

*Tip: To use the web interface to configure the data retrieval-related settings, see **Enabling Data Retrieval** (on page 64).*

Retrieving Energy Usage

You can discover how much energy an IT device consumes by retrieving the Active Energy for the outlet this IT device is plugged into. An SNMP manager can send an SNMP get request for an outlet's outletWattHours value. The value returned is the number of WattHours consumed by the target outlet.

Configuring the FIPS Mode

The Dominion PX supports using the SNMP command to enable or disable the FIPS mode. Make sure you have downloaded the latest version of the MIB file to perform this function. See **The Dominion PX MIB** (on page 171).

To configure the FIPS mode via SNMP, you must:

- Use SNMP v3 only to enable or disable the mode.
- Use the admin account.

After enabling the FIPS mode, some security limitations are applied. See **FIPS Limitations** (on page 156) for details. The following lists the SNMP-related limitations in the FIPS mode.

- The SNMP v1/v2c protocol is NOT supported, but the SNMP v3 protocol is still supported.

If the SNMP v3 protocol is enabled, the Dominion PX automatically forces the SNMP v3 encryption, which cannot be reset. After enabling this protocol, you must:

- Enable the authentication and privacy to set the security level to authPriv.
- Select SHA as the authentication algorithm.
- Select AES as the privacy algorithm.

Note: MD5 and DES are NOT FIPS approved algorithms.

Changing ID Numbers of Environmental Sensors

All ID numbers of existing environmental sensors can be rearranged at a time by using the SNMP MIB variable "reorderexternalSensorsTableEntries" and a comma-separated list.

Below are the guidelines of using this variable:

- ID numbers of all managed sensors must be present in the list no matter their ID numbers will be changed or retained.
- The list cannot contain more than 16 ID numbers, or it is discarded.
- A valid ID number ranges between 1 to 16.
- Each ID number must appear only once in the list.
- If there are missing numbers in the original ID numbers, mark each missing number with a comma when changing ID numbers.

Example without Missing Numbers

If you have five environmental sensors with the ID numbers 1, 2, 3, 4, and 5, and want to change the ID numbers as shown below:

- 1 to 13
- 2 to 8
- 3 to 9
- 4 remains unchanged
- 5 to 2

The original ID numbers are consecutive without any missing numbers so no additional commas should be added.

Position	1	2	3	4	5
Original ID numbers	1,	2,	3,	4,	5
New ID numbers	13,	8,	9,	4,	2

Therefore, your comma-separated list looks like the following:

13,8,9,4,2

Example with Missing Numbers

If you have five environmental sensors with the ID numbers 2, 5, 6, 7, 11, and want to change the ID numbers as shown below:

- 2 to 13
- 5 to 8
- 6 to 9
- 7 to 16
- 11 remains unchanged

Since the original ID numbers are not consecutive because of missing numbers 1, 3, 4, 8, 9 and 10, you must mark each missing number with a comma in the comma-separated list.

Position	1	2	3	4	5	6	7	8	9	10	11
Original ID numbers		2,			5,	6,	7,				11
New ID numbers	,	13,	,	,	8,	9,	16,	,	,	,	11

Therefore, your comma-separated list looks like the following:

`,13,,,8,9,16,,,,,11`

A Note about Measurement Units

The measurement units for current and unit voltage vary depending on the type of SNMP operation.

For current, all current values are measured in milliampere (mA) when performing an SNMP get, but measured in ampere (A) when performing an SNMP set.

For unit voltage, it is measured in volt (V) when performing an SNMP get, but measured in millivolt (mV) when performing an SNMP set.

Retrieving and Interpreting Sensor Readings

You can use the `snmpget` or `snmpwalk` commands to retrieve different environmental sensors' information. To interpret the sensor reading information retrieved via SNMP, you must apply the retrieved sensor information to the sensor reading formula shown below:

`externalSensorValue / 10externalSensorDecimalDigits`

► **To retrieve and interpret environmental sensor readings using the SNMP commands:**

1. Find out the sensor numbers by using the `externalSensorTable` OID `1.3.6.1.4.1.13742.4.3.3.1.1`.
2. Retrieve the desired sensor's type using the `externalSensorType` OID `1.3.6.1.4.1.13742.4.3.3.1.2`.
 - The OID syntax is `1.3.6.1.4.1.13742.4.3.3.1.2.<sensor ID>`

3. Check the information of `TypeOfSensorEnumeration` to determine the sensor's type.

```

TypeOfSensorEnumeration ::= TEXTUAL-CONVENTION
    STATUS current
    DESCRIPTION
        "The types a sensor can be."
    SYNTAX      INTEGER {
        rmsCurrent(1),
        peakCurrent(2),
        unbalancedCurrent(3),
        rmsVoltage(4),
        activePower(5),
        apparentPower(6),
        powerFactor(7),
        activeEnergy(8),
        apparentEnergy(9),
        temperature(10),
        humidity(11),
        airFlow(12),
        airPressure(13),
        onOff(14),
        trip(15),
        vibration(16),
        waterDetection(17),
        smokeDetection(18),
        binary(19),
        contact(20),
        other(30),
        none(31)
    }

```

4. Retrieve the desired sensor's value using the `externalSensorValue` OID
1.3.6.1.4.1.13742.4.3.3.1.41.
 - The OID syntax is
1.3.6.1.4.1.13742.4.3.3.1.41.<sensor ID>
 - This retrieves an unscaled sensor value.
5. Retrieve the desired sensor's decimal digits using the `externalSensorDecimalDigits` OID
1.3.6.1.4.1.13742.4.3.3.1.17.
 - The OID syntax is
1.3.6.1.4.1.13742.4.3.3.1.17.<sensor ID>
 - This retrieves the scaling factor, which represents the number of digits displayed to the right of the decimal point.

6. Retrieve the desired sensor's measurement units using the `externalSensorUnits` OID
1.3.6.1.4.1.13742.4.3.3.1.16.
 - The OID syntax is
1.3.6.1.4.1.13742.4.3.3.1.16.<sensor ID>
7. Check the information of `SensorUnitsEnumeration` to determine the measurement unit of the reading.

```

SensorUnitsEnumeration ::= TEXTUAL-CONVENTION
    STATUS current
    DESCRIPTION
        "The types a sensor can be."
    SYNTAX      INTEGER { none(-1),
                        other(0),
                        volt(1),
                        amp(2),
                        watt(3),
                        voltamp(4),
                        wattHour(5),
                        voltampHour(6),
                        degreeC(7),
                        hertz(8),
                        percent(9),
                        meterpersec(10),
                        pascal(11),
                        psi(12),
                        g(13),
                        degreeF(14),
                        feet(15),
                        inches(16),
                        cm(17),
                        meters(18)
                        }
    
```

8. Use the sensor reading formula to calculate the sensor readings.

Example

This section illustrates the retrieval and interpretation of a specific sensor's readings via SNMP commands.

If the ID number of the environmental sensor whose readings you want to retrieve is **3**, then follow the procedure below to get the readings.

1. Use OID 1.3.6.1.4.1.13742.4.3.3.1.2.**3** to retrieve the sensor type value.
 - Assume the retrieved value is 10.

2. According to the information of `TypeOfSensorEnumeration`, 10 represents a temperature sensor.
3. Use OID `1.3.6.1.4.1.13742.4.3.3.1.41.3` to retrieve the sensor value.
 - Assume the retrieved value is 465.
4. Use OID `1.3.6.1.4.1.13742.4.3.3.1.17.3` to retrieve the sensor's decimal digit value.
 - Assume the retrieved value is 1.
5. Use OID `1.3.6.1.4.1.13742.4.3.3.1.16.3` to retrieve the sensor's measurement unit value.
 - Assume the retrieved value is 14.
6. According to the information of `SensorUnitsEnumeration`, 14 represents degreeF (°F).
7. Use the sensor reading formula to interpret the sensor readings as shown below.
 - $465 / 10^1 = 46.5 \text{ } ^\circ\text{F}$

Chapter 7 Using the CLP Interface

This section explains how to use the Command Line Protocol (CLP) interface to administer a Dominion PX device.

In This Chapter

About the CLP Interface	180
Logging in to the CLP interface	180
Showing Outlet Information	183
Showing In-Depth Outlet Information	185
Switching an Outlet.....	187
Querying an Outlet Sensor	188
Setting the Sequence Delay	188
Showing Environmental Sensor Information	188
Configuring the Thresholds for Environmental Sensors.....	191
Querying the PDU's Serial Number.....	192
Resetting the Dominion PX Device	192
Using the Help Command	192

About the CLP Interface

The Dominion PX provides a command line interface that enables data center administrators to perform some basic management tasks.

The interface is based on the Systems Management Architecture for Server Hardware (SMASH) Command Line Protocol (CLP).

Using this interface, you can do the following:

- Reset the Dominion PX device
- Display the name, power state (on or off), and sensors associated with each outlet
- Turn each outlet on or off
- Display the status of the sensors associated with each outlet

You can access the interface over a serial connection using a terminal emulation program such as HyperTerminal, or via a Telnet or SSH client such as PuTTY.

*Note: Telnet access is disabled by default because it communicates openly and is thus insecure. To enable Telnet, see **Modifying the Network Service Settings** (on page 58).*

Logging in to the CLP interface

Logging in via HyperTerminal over a local connection is a little different than logging in using SSH or Telnet.

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 Dominion PX device 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 = 9600
 - Data bits = 8
 - Stop bits = 1
 - Parity = None
 - Flow control = None
3. Press Enter. A command prompt appears.

```
Welcome!  
At the prompt type one of the following commands:  
- "clp" : Enter Command Line Protocol  
- "config" : Perform initial IP configuration  
- "unblock" : Unblock currently blocked users  
192.168.50.214 command:
```

4. At the command prompt, type `clp` and press Enter. You are prompted to enter a login name.

```
192.168.50.214 command: clp  
  
Entering character mode  
Escape character is '^]'.  
  
PDU CLP Server (c) 2000-2007  
  
Login: _
```

5. Type a name and press Enter. The login name is case-sensitive, so make sure you capitalize the correct letters. Then you are prompted to enter a password.

```
Login: admin
Password: _
```

6. Type a password and press Enter. The password is case sensitive, so make sure you capitalize the correct letters. After properly entering the password, the `clp:/->` system prompt appears.

```
Login: admin
Password:
clp:/->
```

7. You are now logged in to the command line interface and can begin administering the Dominion PX device.

With SSH or Telnet

You can remotely log in to the command line interface using an SSH or Telnet client, such as PuTTY.

Note: PuTTY is a free program you can download from the Internet. See PuTTY's documentation for details on configuration.

► **To log in using SSH or Telnet:**

1. Ensure SSH or Telnet has been enabled. See **Modifying the Network Service Settings** (on page 58).
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 login name is case-sensitive, so make sure you capitalize the correct letters.

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@192.168.50.214's password: █
```

4. Type a password and press Enter. The password is case sensitive, so make sure you capitalize the correct letters. After properly entering the password, the `clp:/->` system prompt appears.

```
login as: admin
admin@192.168.50.214's password:
=== SM CLP v1.0.0 SM ME Addressing v1.0.0 Raritan CLP v0.1 ===
clp:/-> █
```

5. You are now logged in to the command line interface and can begin administering the Dominion PX device.

Closing a Serial Connection

Close the window or terminal emulation program when you finish accessing a Dominion PX device over the serial connection.

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

Showing Outlet Information

The show command displays the name, power state (on or off), and associated sensors for one outlet or for all outlets.

Note: When displaying outlet information, the outlet names are returned as OUTLET1, OUTLET2, and so on. The CLP interface does not reflect the names assigned to the outlets from the web interface.

Syntax

The following is the syntax for the show command:

```
clp:/-> show /system1/outlet<outlet number>
```

where <outlet number> is the number of the outlet. To display information for all outlets, type the wildcard asterisk (*) instead of a number.

Attributes

You can use the name and powerState attributes to filter the output of the show command. The name attribute displays only the name of the outlet, and the powerState attribute displays only the power state (on or off).

The following shows the syntax for both attributes:

```
clp:/-> show -d properties=name /system1/outlet<outlet number>
```

```
clp:/-> show -d properties=powerState /system1/outlet<outlet  
number>
```

where <outlet number> is the number of the outlet. In both cases, the outlet number can also be a wildcard asterisk (*).

Examples

The following are examples of the show command.

Example 1 - No Attributes

The diagram shows the output of the show command without any attributes entered.

```

clp:/-> show /system1/outlet7
/system1/outlet7
Properties:
  Name is OUTLET7
  powerState is 1 (on)

Associations:
  CIM_authorizedTarget => /system2/authorizedpriv8
  CIM_SystemDevice => /system1
  CIM_AssociatedSensor => /system1/ncurrsensor13
  CIM_AssociatedSensor => /system1/nsensor29
  CIM_AssociatedSensor => /system1/ncurrsensor14
  CIM_AssociatedSensor => /system1/nsensor30
  CIM_AssociatedSensor => /system1/nsensor31

```

Example 2 - Name Attribute

The diagram shows the output of the show command with the name attribute.

```

clp:/-> show -d properties=name /system1/outlet7
/system1/outlet7
Properties:
  Name is OUTLET7

```

Example 3 - powerState Attribute

The diagram shows the output of the show command with the powerState attribute.

```

clp:/-> show -d properties=powerState /system1/outlet7
/system1/outlet7
Properties:
  powerState is 1 (on)

```

Showing In-Depth Outlet Information

Use the show command to display the RMS Current, Power Factor, Max Current, Active Power and Apparent Power of a specific outlet.

► **To show in-depth outlet information:**

1. Perform the show command on an outlet. This displays the sensors associated with the designated outlet.

2. Perform the show command on sensors associated with the outlet.

Outlet Sensor Properties

When you perform the show command on an outlet sensor, several properties appear.

- Name
- Threshold state
- Measurement taken by the sensor

The Name property identifies what a sensor measures.

If the name contains:	The sensor measures:
Current	RMS Current
PwrFactor	Power Factor
Max Curr	Maximum Current
Act. Power	Active Power
Apt. Power	Apparent Power
Active Energy	Active Energy

Tip: Sometimes the OtherSensorTypeDescription property is also helpful for identifying the outlet sensor type.

Examples of Showing In-Depth Outlet Information

1. Perform the show command on the outlet without additional attributes.

```

clp:/-> show /system1/outlet7
/system1/outlet7
Properties:
  Name is OUTLET7
  powerState is 1 (on)

Associations:
  CIM_AuthorizedTarget => /system2/authorizedpriv8
  CIM_SystemDevice => /system1
  CIM_AssociatedSensor => /system1/ncurrsensor13
  CIM_AssociatedSensor => /system1/nsensor29
  CIM_AssociatedSensor => /system1/ncurrsensor14
  CIM_AssociatedSensor => /system1/nsensor30
  CIM_AssociatedSensor => /system1/nsensor31
    
```

2. Perform the show command on the associated sensors.

```

clp:/-> show /system1/nsensor29
/system1/nsensor29
Properties:
  SystemCreationClassName is CIM_ComputerSystem
  SystemName is Management
  CreationClassName is CIM_NumericSensor
  DeviceID is 49.0.32
  Name is R.07 PwrFactor(49.0.32)
  SensorType is 1 (Other)
  OtherSensorTypeDescription is Power Factor
  CurrentState is OK
  PossibleStates is OK
  BaseUnits is 1 (Other)
  UnitModifier is -5
  RateUnits is 0 (None)
  CurrentReading is 0.000000
  NominalReading is 0

Associations:
  CIM_SystemDevice => /system1
  CIM_ConcreteDependency => /system2
  CIM_AssociatedSensor => /system1/outlet7

```

Switching an Outlet

The set command can turn an outlet on or off.

Turning an Outlet On

Using the keyword `on` turns the outlet on.

```
clp:/-> set /system1/outlet<outlet number> powerState=on
```

where <outlet number> is the number of the outlet.

Turning an Outlet Off

Using the keyword `off` turns the outlet off.

```
clp:/-> set /system1/outlet<outlet number> powerState=off
```

where <outlet number> is the number of the outlet.

Querying an Outlet Sensor

The show command with the keyword *Antecedent* queries an outlet's sensors.

```
clp:/-> show -d properties=Antecedent /system1/outlet<outlet
number>=>CIM_AssociatedSensor
```

where <outlet number> is the number of the outlet.

Setting the Sequence Delay

The set command can change the sequence delay for all outlets.

```
clp:/-> set /system1 powerOnDelay=X
```

where X represents the number in the time scale of 100ms. For example, *powerOnDelay=2* means the sequence delay is set to 200ms, and *powerOnDelay=10* means the sequence delay is set to 1000ms (1 second).

Showing Environmental Sensor Information

The following is the syntax for the show command for environmental sensors:

```
clp:/-> show /system1/externalsensor<ID number>
```

where <ID number> is the ID number assigned to the environmental sensor while having the environmental sensor managed. The maximum number is 16 since the Dominion PX device can manage up to 16 environmental sensors.

To display information for all environmental sensors, type the wildcard asterisk (*) instead of a number.

Identifying Sensor Types

When you perform the show command for an environmental sensor, you can check the OtherSensorTypeDescription property to identify the sensor type.

If the property shows:	Sensor type
Humidity	Humidity sensor
Temperature	Temperature sensor
Contact	Contact closure sensor

Example 1 - No Attributes

This diagram shows the output of the show command without any attributes entered for a humidity sensor, whose ID number is 1.

```

clp:/-> show /system1/externalsensor1
/system1/externalsensor1
Properties:
  SystemCreationClassName is CIM_ComputerSystem
  SystemName is Management
  CreationClassName is Raritan_CIMExternal
  DeviceID is unknown
  Name is Humidity AEI7A00022 (196.0.32)
  SensorType is 1 (Other)
  OtherSensorTypeDescription is Humidity
  CurrentState is OK
  PossibleStates is [OK,Lower Non-Critical,Lower Critical,Lower Non-Recoverable,Upper Non-Critical,Upper Critical,Upper Non-Recoverable]
  BaseUnits is 1 (Other)
  UnitModifier is 0
  RateUnits is 0 (None)
  CurrentReading is 57.000000
  NominalReading is 45
  Status is Sensor is available

Associations:
  CIM_SystemDevice => /system1
  CIM_ConcreteDependency => /system2

Verbs: cd help set show

```

The diagram shows the output of the show command without any attributes entered for a contact closure sensor, whose ID number is 3.

```

clp:/-> show /system1/externalsensor3
/system1/externalsensor3
Properties:
  SystemCreationClassName is CIM_ComputerSystem
  SystemName is Management
  CreationClassName is Raritan_CIMExternal
  DeviceID is unknown
  Name is On/Off PRC0190292 1(198.0.32)
  SensorType is 1 (Other)
  OtherSensorTypeDescription is Contact
  CurrentState is OK
  PossibleStates is [OK,Transition to Idle,Transition to Ac
tive]
  BaseUnits is 1 (Other)
  UnitModifier is 0
  RateUnits is 0 (None)
  CurrentReading is 0.000000
  NominalReading is 0
  Status is Sensor is unavailable

Associations:
  CIM_SystemDevice => /system1
  CIM_ConcreteDependency => /system2

Verbs: cd help set show

```

Example 2 - Name Attribute

The diagram shows the output of the show command with the name attribute for the environmental sensor 1.

```

clp:/-> show -d properties=Name /system1/externalsensor1
/system1/externalsensor1
Properties:
  Name is Humidity AEI7A00022 (196.0.32)

```

Example 3 - CurrentReading Attribute

The diagram shows the output of the show command with the CurrentReading attribute for the environmental sensor 1.

```

clp:/-> show -d properties=CurrentReading /system1/externalsensor1
/system1/externalsensor1
Properties:
  CurrentReading is 62.000000

```

Configuring the Thresholds for Environmental Sensors

The following shows the syntax for configuring the thresholds of numeric environmental sensors, such as temperature sensors. Note that a discrete (on/off) sensor does not have threshold properties.

```
clp:/-> set /system1/externalsensor<ID number>
        LowerThresholdCritical=<LC_value>
        LowerThresholdNonCritical=<LNC_value>
        UpperThresholdNonCritical=<UNC_value>
        UpperThresholdCritical=<UC_value>
```

<ID number> is the ID number assigned to the environmental sensor while having the environmental sensor managed. The maximum number is 16 since the Dominion PX device can manage up to 16 environmental sensors.

<LC_value> is the numeric value assigned to the lower critical threshold.

<LNC_value> is the numeric value assigned to the lower non-critical threshold.

<UNC_value> is the numeric value assigned to the upper non-critical threshold.

<UC_value> is the numeric value assigned to the upper critical threshold.

When setting the thresholds, make sure the threshold values you set meet the rules shown in this table:

Threshold	Criterion
Upper critical threshold	Larger than or equal to the following formula: upper non-critical threshold + hysteresis
Upper non-critical threshold	Larger than or equal to the following formula: lower non-critical threshold + (2 x hysteresis)
Lower non-critical threshold	Larger than or equal to the following formula: lower critical threshold + hysteresis

Important: In the CLP interface, the Dominion PX does NOT verify whether new threshold values meet the rules so it is strongly recommended to double check new values before applying them.

Querying the PDU's Serial Number

The show command with the keyword *serialNumber* queries the serial number of the Dominion PX device.

```
clp:/-> Show -d properties=serialNumber /system1
```

Resetting the Dominion PX Device

The reset command restarts the Dominion PX management application only. The power state of individual outlets remains unchanged.

This command is not a factory reset.

```
clp:/-> reset /system1
```

*Note: To perform the factory reset, see **Resetting to Factory Defaults** (on page 267).*

Using the Help Command

The help command is useful when you are not familiar with the CLP commands, such as supported options or the syntax of a specific command.

Example 1 - Help Information for the Show Command

To show the help information for a specific command, add that command to the end of the help command.

The diagram shows the output of the help information for the show command.

```
clp:/-> help show
The Show command is used to display information about objects
within the CLP namespace.

Usage: SHOW [options] [target]

Use "-output verbose" option for more detailed help.
```

Example 2 - Getting In-Depth Help Information

To show detailed help information, add the option `-output verbose` between the help command and the queried command.

The diagram shows the output of the help information for the show command in details.

```
clp:/-> help -output verbose show
The Show command is used to display information about objects
within the CLP namespace.

Usage: SHOW [options] [target]

Supported options:
  -display <arg> (-d)   Select information to display.
  -examine          (-x) Check syntax, don't execute command.
  -help            (-h)   Display this help.
  -level <n>       (-l)   Recurse n (or 'all') levels below target.
  -output <arg>   (-o)   Specify output format.
  -version         (-v)   Display version information.
```

Chapter 8 In-line Monitors

The model name of a Dominion PX in-line monitor follows this format: PX-3nnn, where n is a numeric digit.

Unlike most of the Dominion PX devices, an in-line monitor may have multiple inlets. Each inlet is connected to an outlet only, so an inlet's rating is the same as an outlet's rating.

Raritan provides both single-phase and three-phase in-line monitors to satisfy different needs.

In This Chapter

Overview.....	194
Flexible Cord Installation Instructions.....	196
In-line Monitor's LED Display	204
In-line Monitor's Web Interface.....	205
SNMP and CLP Interfaces	208

Overview

An in-line monitor is implemented with the same number of inlets and outlets. An inlet is connected to a power source for receiving electricity, such as electric distribution panels or branch circuit receptacles. An outlet is connected to a device that draws power, such as a cooling or IT device.

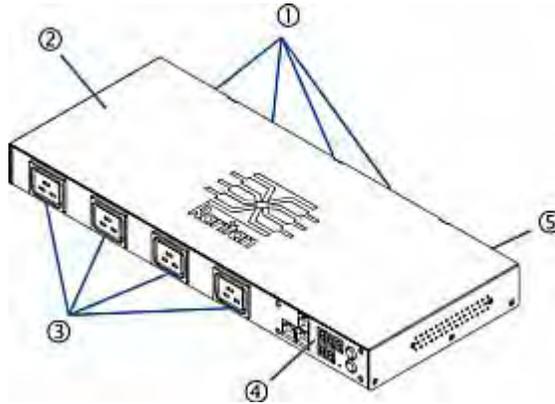
Inlets are located at the side labeled **Line**, and outlets are located at the side labeled **Load**.

Two types of mechanical designs are available for an in-line monitor's inlets and outlets:

- Power-socket type, such as PX-3411
- Cable-gland type, such as PX-3420

Models with Power Sockets

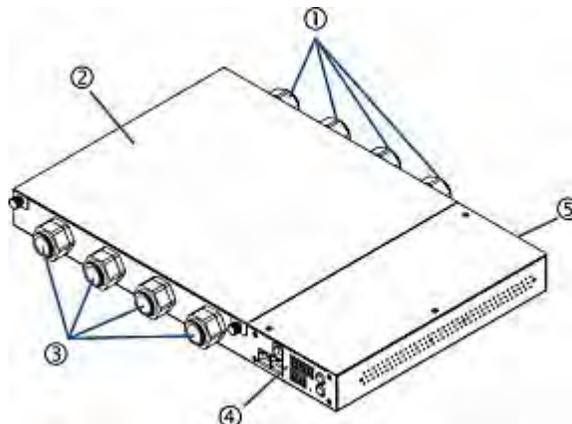
This diagram shows an in-line monitor whose inlets and outlets are in the form of power sockets or receptacles. The total number of inlets and outlets varies depending on the model you purchased.



Number	Description
1	Inlets (the side labeled LINE)
2	Top cover
3	Outlets (the side labeled LOAD)
4	Front panel with the LED display
5	Rear panel

Models with Cable Glands

This diagram shows an in-line monitor whose inlets and outlets are in the form of cable glands. The total number of inlets and outlets varies depending on the model you purchased.



Number	Description
1	Inlets (the side labeled LINE)
2	Top cover
3	Outlets (the side labeled LOAD)
4	Front panel with the LED display
5	Rear panel

Flexible Cord Installation Instructions

An in-line monitor may require you to install flexible cords on both of its inlets and outlets unless the model has been implemented with factory-installed flexible cords, such as PX-3423.

WARNING! DO NOT perform wiring assembly for this product unless you are an experienced, licensed electrician. Assembly or attempted assembly by inexperienced or unlicensed electricians may result in electrical shock, fire, personal injury, and death. If you are not a qualified electrician with appropriate licensing and insurance - STOP NOW. This is work you cannot and should not attempt. Raritan is not responsible for any consequential damages to equipment or loss of data due to improper installation.

FOR QUALIFIED ELECTRICIANS: Read the instructions in their entirety before starting the installation. You must follow all wiring instructions, ensure compliance with national and local safety and electrical codes, and follow all other electrical safety requirements with regard to over-current protection. **STOP** and contact Raritan Technical Support if you are unsure of any answers, or have additional questions.

The following instructions are for Raritan products manufactured to accept user-installed flexible cords. These products are visually identified by the cable gland used to hold the flexible cord.



Flexible Cord Selection

- The preferred flexible cable is type SOOW, 600V, 90°C or 105°C. Consult Raritan before using a different flexible cable type.
- The rated ampacity of the flexible cord must be greater than or equal to the Raritan product's rated ampacity marked on its nameplate. In the United States, relevant ampacity ratings for flexible cords can be found in NEC(2011) section 400.5.
- The number of wires in the flexible cord must match the number of terminals (including the ground terminal) inside the Raritan product. See **Wiring of 3-Phase In-Line Monitors** (on page 198) for exceptions.
- If a plug is to be attached to the flexible cord, the length of the flexible cord must not exceed 4.5 meters - as specified in UL 60950-1 (2007) and NEC 645.5 (2011).
- The flexible cord may be permanently connected to power subject to local regulatory agency approval. In the United States, relevant electrical regulations can be found in NEC (2011) sections 400.7(A)(8), 400.7(B), 368.56 and table 400.4.

Plug Selection

If a plug is to be attached to the flexible cord, the plug's rated ampacity is chosen as follows:

- In the United States, the plug's rated ampacity must be 125% greater than the Raritan product's rated ampacity. In some Raritan products, such as 35A 3-phase delta wired PDUs, an exactly 125% rated plug is not available. In these cases, choose the closest plug that is more than 125%. For example, a 50A plug is the closest fit for a 35A 3-phase PDU.
- For all other locations, subject to local regulatory agency policy, the plug's rated ampacity is the same as the Raritan products rated ampacity.

Receptacle Selection

For Raritan in-line monitors, any receptacle fitted to the outlet flexible cord must have identical ratings as the plug attached to the inlet flexible cord.

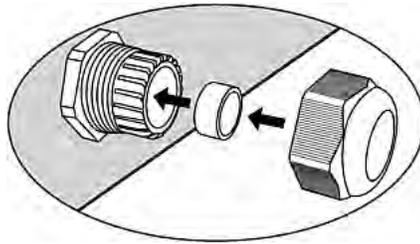
Derating a Raritan Product

Lower rated plugs, receptacles and flexible cords may be connected to a Raritan product. This results in a derated (reduced) ampacity rating for the product.

▶ **Derating guidelines:**

1. Choose the plug and use its rated ampacity to determine the derated ampacity.

- In North America, the derated ampacity is 80% of the plug's rated ampacity. For example, a 30A plug would result in a derated ampacity of 24A.
 - In other geographic locations, subject to local regulatory agency approval, the derated ampacity is the plug's rated ampacity. For example, using a 16A plug would result in a derated ampacity of 16A.
2. The derated ampacity must be marked on the Raritan product so the new reduced rating can be easily identified.
 3. For in-line monitors, the receptacles used must have the same voltage and ampacity rating as the plug chosen in step 1.
 4. The flexible cord must have a rated ampacity greater than or equal to the derated ampacity. Since the new flexible cord may be smaller diameter, a check must be performed to insure the cable gland nut, when tightened, will securely hold the flexible cord so that it cannot be twisted, pulled or pushed in the cable gland. A sealing ring, for small diameter flexible cords, may have been included with the Raritan product, or one can be requested from Raritan, to reduce the inside diameter of the cable gland.



Wiring of 3-Phase In-Line Monitors

3-phase in-line monitors contain 4-pole wiring terminal blocks (L1, L2, L3, N) to monitor 5-wire (4P+PE) 3-phase wye connections. Delta wired 4-wire (3P+PE) 3-phase connections are also permitted (no wire connected to the terminal block neutral "N"). No additional hardware or firmware configuration is required to specify whether the connection is 5-wire wye or 4-wire delta.

In-Line Monitor Unused Channels

It is not necessary to wire up all channels of multi-channel in-line monitors. The inlet and outlet openings of unused channels must be completely closed off. "Goof plugs" for this purpose may be a good choice if they are available in your country or region.

Step by Step Flexible Cord Installation

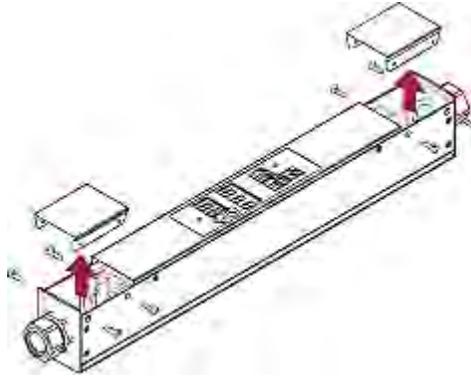
The following items are required to complete the installation:

- Flexible cord(s).
- Insulated ring terminals (one for each wire) and appropriate crimp tool.
- Plug(s) and receptacle(s) (for in-line monitors)
- Torque screwdriver, torque nut driver and torque wrench to tighten the wiring terminal block screws, ground nut and cable gland nut.

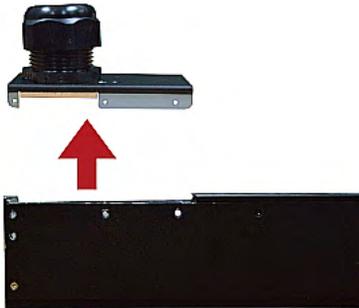
▶ **To install a flexible cord:**

1. Open the PDU's access panel (or in-line monitor top panel) to expose the power wiring terminal block(s).

One-channel in-line monitor



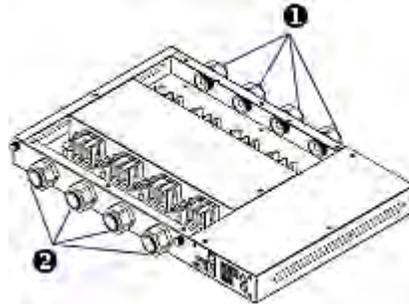
Zero U PDU



Make sure to locate the ground wire mounting stud(s). There is a separate ground wire mounting stud for each terminal block. Each flexible cord **MUST** have its green (or green/yellow) ground wire bonded to a ground wire mounting stud.



For in-line monitors, make sure to identify the inlet terminal blocks (rear of monitor) and outlet terminal blocks (front of monitor). Each inlet terminal block has a corresponding outlet terminal block.

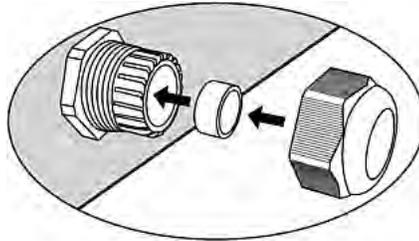


Number	Description
①	Inlets (labeled LINE)
②	Outlets (labeled LOAD)

2. Strip off the outer jacket of the flexible cord and remove any jute, paper or other fillers. Use the following to help determine how much jacket to remove:
 - In the finished assembly, the outer jacket should protrude inside the Raritan product.
 - The wires will have ring terminals crimped onto them.
 - In the finished assembly, the wires should have some slack and not be taught.
 - In the finished assembly, if the flexible cord slips in the cable gland placing a strain on the cord's wires, the ground wire must be the last wire to take the strain.
3. Crimp an insulated ring terminal onto each wire. A non-insulated ring terminal may be used for the ground wire. Inspect each crimp to insure it is secure and verify no exposed wire protrudes from the rear of an insulated ring terminal.
4. Loosen the cable gland nut and push the flexible cord assembly through the gland.



Temporarily hand tighten the gland nut and verify the cord cannot be twisted or pushed or pulled in the gland. Do not proceed if hand tightening results in a loose cord. In some models, especially in-line monitors, the flexible cord's diameter may be too small for the cable gland. A sealing ring for smaller diameter line cords may have been included with the Raritan product, or can be requested from Raritan, to reduce the inside diameter of the cable gland.



5. Fasten the ring terminal of the green (or green/yellow) ground wire to the chassis's threaded ground stud in this order:
 - a. Place the lock washer on the stud.
 - b. Place the ground wire ring terminal on the stud.
 - c. Place the nut on the stud and tighten with a torque wrench. The appropriate torque settings vary according to the nut size.

Nut size	Torque setting (N-m)	Tolerance
M3	0.49	10%
M4	1.27	8%
M5	1.96	5%
M6	2.94	3.5%
M8	4.9	2%

- d. Check the ground wire connection. It should be secure and not move or rotate.

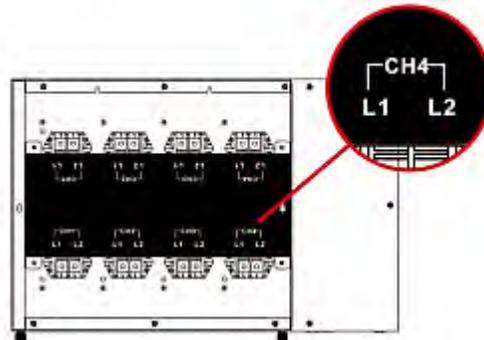


6. Fasten the ring terminals of all remaining wires to the terminal block and tighten each using a torque screwdriver. The appropriate torque settings vary according to the screw size.

Screw size	Torque setting (N-m)	Tolerance
M3	0.49	10%
M4	1.27	8%
M5	1.96	5%
M6	2.94	3.5%
M8	4.9	2%

Make sure each ring terminal is firmly fastened and cannot be twisted by hand. Use the following guidelines to help terminal block wiring.

- In single-phase Raritan products with world-wide ratings, the terminals are labeled L1 and L2. L1 is the phase wire. L2 is either the neutral (120/230V installations) or another phase wire (208V installations).



- In all 3-phase products, L1 is phase A, L2 is phase B, L3 is phase C and N is neutral.
 - For Raritan in-line monitors, where there is a one to one correspondence between plug and receptacle, maintain the same wire colors for inlet and outlet flexible cords.
7. Make final adjustments to the cable gland and verify the jacket of the flexible cord extends into the Raritan product. Hand tighten the gland nut and finish tightening with a torque wrench. Appropriate torque settings vary according to the cable gland size.

Cable gland size	Torque setting (N-m)
M12x1.5	0.7 to 0.9
M16x1.5	2.0 to 3.0
M20x1.5	2.7 to 4.0

Cable gland size	Torque setting (N·m)
M25x1.5	5.0 to 7.5
M32x1.5	7.5 to 10.0
M40x1.5	7.5 to 10.0
M50x1.5	7.5 to 10.0
M63x1.5	7.5 to 10.0

Note: The cable gland size is marked on the cable gland body.

After tightening, examine the flexible cord and cable gland for the following:

- Make sure you can see a few remaining threads between the cable gland body and cable gland nut. The gland nut must not bottom out on the gland body.
 - Make sure the flexible cord does not move in the cable gland when it is twisted, pushed or pulled.
8. Re-install the PDU wiring access panel or in-line monitor cover plate. This completes internal wiring of the Raritan product.
 9. For in-line monitors, fasten the receptacles to the outlet flexible cords following the manufacturer's instructions.
 10. Complete the wiring of the inlet flexible cord by performing one of these steps:
 - Assemble the plug following the manufacturer's instructions.
 - Permanently attach and strain relief the flexible cord to a junction box following applicable electrical codes.

In-line Monitor's LED Display

The LED display of an in-line monitor is the same as a regular Dominion PX model. See **LED Display** (on page 33).

Automatic Mode

Unlike regular Dominion PX models, the in-line monitor's LED display only cycles through the current readings of each outlet in the Automatic Mode.

Manual Mode

You can switch between voltage, active power and current readings of the selected outlet in the Manual Mode on an in-line monitor. To enter the Manual Mode, press the Up or Down button.

► **To operate the LED display of an in-line monitor:**

1. Press the Up or Down button until the desired outlet number is selected in the two-digit row.
 - Pressing the Up button moves up one selection.
 - Pressing the Down button moves down one selection.
2. Current of the selected outlet is shown in the three-digit row. It appears in this format: XX.X (A).
3. If desired, you can press the Up and Down buttons simultaneously to switch between current and voltage readings.
 - The voltage appears in this format: XXX (V). It is displayed for about five seconds, after which the current reading re-appears.
4. To switch to the active power readings, press the Up or Down button until the unbalanced load is selected in the two-digit row, such as 1U. Then press Up and Down buttons simultaneously to switch to the active power mode, such as 1P. Now you can press the Up or Down button to switch between the active power of different outlets/inlets.
 - The active power appears in this format: X.XX (W). It is displayed for about five seconds, after which the current reading re-appears.

To exit from the active power mode, do NOT press any button until the LED display returns to the Automatic Mode.

Note: The LED display returns to the Automatic Mode after 10 seconds elapse since the last time any button was pressed.

Tip: A quick way to distinguish between voltage, current, and power is the placement of the decimal point in the display. Voltage has no decimal point, active power has a decimal point between the first and second digits, and current has a decimal point between the second and third digits.

In-line Monitor's Web Interface

An in-line monitor's web interface is similar to a regular Dominion PX model's web interface.

See **Using the Web Interface** (on page 39) for login instructions and additional information.

Menus

An in-line monitor is NOT implemented with the overcurrent protection mechanism and outlet-switching function, so its menu items are slightly different from those of a regular Dominion PX PDU. The following list shows each menu with their own set of menu items.

Details
Outlet Details
PDU Details
Outlet Setup
Alerts
Alert Configuration
Alert Policies
Alert Policy Editor
Alert Destinations
User Management
Change Password
Users & Groups
User/Group System Permissions
Device Settings
PDU Setup
Network
Security
Certificate
Date/Time
Authentication
SMTP Settings
SNMP Settings
Event Log
FIPS Setting
External Sensors
External Sensors Details
External Sensors Setup

Maintenance
Device Information
View Event Log
Update Firmware
Bulk Configuration
Unit Reset
Diagnostics
Network Interface
Network Statistics
Ping Host
Trace Route to Host
Device Diagnostics
Help
About Dominion PX

Home Page

The power status of each outlet on an in-line monitor is displayed in the Monitors section of the Home page, including:

- Voltage (Volts)
- RMS current (Amps)
- Active power (Watts)
- Active energy (WattHours)

The screenshot shows the Raritan web interface for a Dominion PX device. The navigation bar includes links for Home, Details, Alerts, User Management, Device Settings, External Sensors, Maintenance, Diagnostics, and Help. The main content area is titled "Home > PDU Status" and features a "Monitors" section with a table of power monitoring data.

Name	Voltage	RMS Current	Active Power	Active Energy
Inlet1 Outlet 1	109 Volts	0.14 Amps	9 Watts	145 WattHours
Inlet2 Outlet 2	0 Volts	0.00 Amps	0 Watts	0 WattHours
Inlet3 Outlet 3	0 Volts	0.00 Amps	0 Watts	0 WattHours
Inlet4 Outlet 4	0 Volts	0.00 Amps	0 Watts	0 WattHours

SNMP and CLP Interfaces

Same as regular Dominion PX models, an in-line monitor allows remote access through either SNMP or CLP interface. See ***Using SNMP*** (on page 165) and ***Using the CLP Interface*** (on page 180).

Appendix A Specifications

In This Chapter

Maximum Ambient Operating Temperature	209
Dominion PX Serial RJ-45 Port Pinouts	209
Dominion PX Feature RJ-12 Port Pinouts.....	209

Maximum Ambient Operating Temperature

The maximum ambient operating temperature (TMA) for the Dominion PX varies between 40 to 60 degrees Celsius, depending on the model and certification standard (CE or UL). If necessary, contact Raritan Technical Support for this information for your model.

Specification	Measure
Max Ambient Temperature	40 to 60 degrees Celsius

Dominion PX Serial RJ-45 Port Pinouts

RJ-45 Pin/signal definition			
Pin No.	Signal	Direction	Description
1	DTR	Output	Reserved
2	GND	—	Signal Ground
3	+5V	—	Power for CIM (200mA, fuse protected)
4	TxD	Output	Transmit Data (Data out)
5	RxD	Input	Receive Data (Data in)
6	N/C	N/C	No Connection
7	GND	—	Signal Ground
8	DCD	Input	Reserved

Dominion PX Feature RJ-12 Port Pinouts

RJ-12 Pin/signal definition			
Pin No.	Signal	Direction	Description

RJ-12 Pin/signal definition			
1	+12V	—	Power (500mA, fuse protected)
2	GND	—	Signal Ground
3	RS485 (Data +)	bi-directional	Data Line +
4	RS485 (Data -)	bi-directional	Data Line -
5	GND	—	Signal Ground
6	1-wire		Used for Feature Port

Appendix B Equipment Setup Worksheet

Dominion PX Series Model _____

Dominion PX Series Serial Number _____

OUTLET 1	OUTLET 2	OUTLET 3
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE
OUTLET 4	OUTLET 5	OUTLET 6
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE

Appendix B: Equipment Setup Worksheet

OUTLET 7	OUTLET 8	OUTLET 9
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE
OUTLET 10	OUTLET 11	OUTLET 12
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE
OUTLET 13	OUTLET 14	OUTLET 15
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE

OUTLET 16	OUTLET 17	OUTLET 18
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE
OUTLET 19	OUTLET 20	OUTLET 21
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE

Appendix B: Equipment Setup Worksheet

OUTLET 22	OUTLET 23	OUTLET 24
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE

Types of adapters

Types of cables

Name of software program

Appendix C Enabling or Disabling the Power CIM

You may connect the Dominion PX device to a Raritan access product (KVM switch) via a power CIM, such as D2CIM-PWR. Serial port support of the power CIM must be enabled in order to enable communications to the KVM switch. By default, serial port support for the power CIM is enabled.

If no connection to a Raritan KVM switch is required, the serial port support for the power CIM can be disabled. Note that after disabling the serial port support for the power CIM, the KVM switch cannot receive any data from the Dominion PX or control it even if a power CIM is in place.

► To enable or disable the connected power CIM:

1. Use a terminal emulation program to access the CLP interface. See *With HyperTerminal* (on page 181).
2. Type the command `configurepowercim` and press Enter.

```
Welcome!  
At the prompt type one of the following commands:  
- "clp"      : Enter Command Line Protocol  
- "config"   : Perform initial IP configuration  
- "unblock"  : Unblock currently blocked users  
192.168.84.121 command: configurepowercim
```

3. Type `yes` to enable the power CIM or `no` to disable it, and press Enter.

```
Welcome!  
At the prompt type one of the following commands:  
- "clp"      : Enter Command Line Protocol  
- "config"   : Perform initial IP configuration  
- "unblock"  : Unblock currently blocked users  
192.168.84.121 command: configurepowercim  
Enable Power CIM (yes/no) [yes]: yes
```

4. Wait until the CLP interface completes the operation and shows the welcome message again.

```
Welcome!  
At the prompt type one of the following commands:  
- "clp"      : Enter Command Line Protocol  
- "config"   : Perform initial IP configuration  
- "unblock"  : Unblock currently blocked users  
192.168.84.121 command: configurepowercim  
Enable Power CIM (yes/no) [yes]: yes  
Enabled Power CIM ...
```

Appendix D Integration



Product	Direct Access Interfaces		Access Through CC-SG Interfaces		Connectivity	Max # of PX Units Supported
	Association	Control	Association	Control		
Dominion SX	>= 3.1: SX GUI; < 3.1: None	RSC into PX serial port	CC GUI	CC GUI	CSCSPCS-1 or CSCSPCS-10	Max = number of serial ports

Product	Direct Access Interfaces		Access Through CC-SG Interfaces		Connectivity	Max # of PX Units Supported
	Association	Control	Association	Control		
Dominion KX-I	KX Manager	RRC/MPC	CC-GUI	CC-GUI	P2CIM-PWR	4; 8 in KX 1.3 or higher.
Dominion KX-II	KX GUI	RRC/MPC, JAC	CC-GUI	CC GUI	D2CIM-PWR	4; 8 in KX 1.3 or higher.
Dominion KX2-101	KX-GUI	RRC/MPC, JAC	CC-GUI	CC-GUI	DKX2-101-SPDUC	1
Dominion KSX 2	KSX GUI	RRC/MPC, JAC	CC-GUI	CC-GUI / KSX GUI	Straight CAT5 cable	

Product	Direct Access Interfaces		Access Through CC-SG Interfaces		Connectivity	Max # of PX Units Supported
	Association	Control	Association	Control		
Paragon II (UST)	Paragon Manager, OSD	OSD	IP-Reach + OSD	IP-Reach + OSD	P2CIM-PWR	Max = number of channel ports
Paragon II (USTIP)	Paragon Manager, OSD	RRC, OSD	PIISC + Paragon Manager	CC GUI	P2CIM-PWR	Max = number of channel ports

Association: Associate the target with power outlet

Control: Power On/Off, and Power Recycle the device

CSCSPCS-1: An adapter which still needs a Cat5 straight through cable to connect

NOTE: Connecting any power CIM except the for the D2CIM-PWR (e.g. P2CIM-PWR) to the PX serial port switches all the outlets ON, even if they were previously OFF.

In This Chapter

Power IQ Configuration	218
Dominion KX II Power Strip Configuration	220
Dominion KX I Power Strip Configuration	224
Paragon II	229
Dominion SX.....	232
Dominion KSX	235
CommandCenter Secure Gateway	236

Power IQ Configuration

Raritan'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, see either of the following:

- Power IQ User Guide: Available on the Raritan website's **Firmware and Documentation section** (<http://www.raritan.com/support/firmware-and-documentation/>).
- Power IQ Online Help: Available on the **Product Online Help section** (<http://www.raritan.com/support/online-help/>).

*Note: Power IQ must use SNMP v3 to manage or control the Dominion PX running in the FIPS mode. See **Impact on the Raritan Product Integration** (on page 157).*

Adding PDUs to Power IQ Management

Once Power IQ is configured, add Dominion PX or other PDUs to its management. Power IQ can then gather data from these PDUs.

You can also add PDUs to Power IQ by uploading a CSV file containing the information. See Adding PDUs in Bulk with CSV Files in the Power IQ User Guide.

Use this procedure to add a Raritan EMX to Power IQ.

► **To add PDUs to Power IQ management:**

1. In the PDUs tab, click Add.
2. Enter the IP address of the PDU.
3. If the PDU is in a daisy-chained configuration or console server configuration, enter the PDU's position number in the chain or serial port number in the Proxy Index field.

Note: If the PDU is not in this type of configuration, leave the Proxy Index field blank.

4. Enter an asset tag number or other asset management code in the External Key field. **Optional.**
5. Enter data in Custom Field 1 and Custom Field 2. **Optional.** The labels may have been changed in Power IQ to identify these fields.

6. If the PDU is a Dominion PX, enter a valid Username and Password for the PDU in the Dominion PX Credentials section. Re-enter the password in the Password Confirm field.
7. Select the SNMP Version.
 - For SNMP version 1/2c PDUs, enter an SNMP Community String that has at least READ permissions to this PDU. This enables polling the PDU for data. Enter an SNMP community string that has both READ and WRITE permissions to the PDU to enable power control, outlet renaming, and buffered data retrieval.
 - For SNMP version 3 PDUs, enter the Username and select an Authorization Level. The authorization levels are:
 - noAuthNoPriv - No Authentication Passkey, No Encoding Passkey
 - authNoPriv - Authentication Passkey, No Encoding Passkey
 - authPriv - Authentication Passkey, Encoding Passkey
 - a. Depending on the Authorization Level selected, you must enter additional credentials for Authorization and Privacy.
 - b. Authorization Protocol: Select MD5 or SHA.
 - c. Enter the PDU's Authorization Passkey, then re-enter the passkey in the Authorization Passkey Confirm field.
 - d. Privacy Protocol: Select DES or AES.
 - e. Enter the PDU's Privacy Passkey, then re-enter the passkey in the Privacy Passkey Confirm field.

Note: You must enable the SNMP agent on all PDUs added to Power IQ.

8. Select "Validate and wait for discovery to complete before proceeding" to check credentials and view the discovery process status as you add this PDU. **Optional.** See Validating PDU Credentials in the Power IQ User Guide.
9. Click Add.

Note: PDU discovery is complete once the PDU model type is determined. SNMP fields such as contact or location values are not determined until this device is polled for the first time.

Once added, the PDU appears in the PDU list. Power IQ begins polling the PDU for sensor data. You can configure how often Power IQ polls PDU. See Configuring Polling Intervals in the Power IQ User Guide.

Dominion KX II Power Strip Configuration

Dominion KX II integration requires D2CIM-PWR and straight CAT5 cable.

For more information on Dominion KX II, see either of the following:

- Dominion KX II User Guide: Available on the Raritan website's **Firmware and Documentation section** (<http://www.raritan.com/support/firmware-and-documentation/>).
- Dominion KX II Online Help: Available on the **Product Online Help section** (<http://www.raritan.com/support/online-help/>).

Configuring Rack PDU (Power Strip) Targets

The KX II allows you to connect rack PDUs (power strips) to KX II ports. KX II rack PDU configuration is done from the KX II Port Configuration page.

Connecting a Rack PDU

Raritan PX series rack PDUs (power strips) are connected to the Dominion device using the D2CIM-PWR CIM.

► **To connect the rack PDU:**

1. Connect the male RJ-45 of the D2CIM-PWR to the female RJ-45 connector on the serial port of the rack PDU.
2. Connect the female RJ-45 connector of the D2CIM-PWR to any of the available female system port connectors on the KX II using a straight through Cat5 cable.
3. Attach an AC power cord to the target server and an available rack PDU outlet.
4. Connect the rack PDU to an AC power source.
5. Power on the device.



Naming the Rack PDU in the KX II or LX (Port Page for Power Strips)

Note: PX rack PDUs (power strips) can be named in the PX as well as in KX II and LX.

Once a Raritan remote rack PDU is connected to the KX II or LX, it will appear on the Port Configuration page. Click on the power port name on that page to access it. The Type and the Name fields are prepopulated.

Note: The (CIM) Type cannot be changed.

The following information is displayed for each outlet on the rack PDU: [Outlet] Number, Name, and Port Association.

Use this page to name the rack PDU and its outlets. Names can be up to 32 alphanumeric characters and can include special characters.

Note: When a rack PDU is associated with a target server (port), the outlet name is replaced by the target server name, even if you assigned another name to the outlet.

► To name the rack PDU and outlets:

Note: CommandCenter Secure Gateway does not recognize rack PDU names containing spaces.

1. Enter the Name of the rack PDU (if needed).
2. Change the [Outlet] Name if desired. (Outlet names default to the outlet #.)

3. Click OK.

Home > Device Settings > Port Configuration > Port

Port 17

Type:
PowerStrip

Name:

Outlets

Number	Name	Port Association
1	<input type="text" value="Dominion-Port1(1)"/>	Dominion- Port7
2	<input type="text" value="Outlet 2"/>	
3	<input type="text" value="Outlet 3"/>	
4	<input type="text" value="Outlet 4"/>	
5	<input type="text" value="Outlet 5"/>	
6	<input type="text" value="Outlet 6"/>	
7	<input type="text" value="Outlet 7"/>	
8	<input type="text" value="Outlet 8"/>	

Associating Outlets with Target Servers on KX II and LX

The Port page opens when you click on a port on the Port Configuration page. From this page, you can make power associations, change the port name to something more descriptive, and update target server settings if you are using the D2CIM-VUSB CIM. The (CIM) Type and the (Port) Name fields are prepopulated; note that the CIM type cannot be changed.

A server can have up to four power plugs and you can associate a different rack PDU (power strip) with each. From this page, you can define those associations so that you can power on, power off, and power cycle the server from the Port Access page.

To use this feature, you will need:

- Raritan remote rack PDU(s)
- Power CIMs (D2CIM-PWR)

► **To make power associations (associate rack PDU outlets to KVM target servers):**

Note: When a rack PDU is associated to a target server (port), the outlet name is replaced by the target server name (even if you assigned another name to the outlet).

1. Choose the rack PDU from the Power Strip Name drop-down list.
2. For that rack PDU, choose the outlet from the Outlet Name drop-down list.
3. Repeat steps 1 and 2 for all desired power associations.
4. Click OK. A confirmation message is displayed.

► **To change the port name:**

1. Type something descriptive in the Name field. For example, the name of the target server would be a likely candidate. The name can be up to 32 alphanumeric characters and can include special characters.
2. Click OK.

Removing Power Associations

When disconnecting target servers and/or rack PDUs from the device, all power associations should first be deleted. When a target has been associated with a rack PDU and the target is removed from the device, the power association remains. When this occurs, you are not able to access the Port Configuration for that disconnected target server in Device Settings so that the power association can be properly remove.

► **To remove a rack PDU association:**

1. Select the appropriate rack PDU from the Power Strip Name drop-down list.

2. For that rack PDU, select the appropriate outlet from the Outlet Name drop-down list.
3. From the Outlet Name drop-down list, select None.
4. Click OK. That rack PDU/outlet association is removed and a confirmation message is displayed.

► **To remove a rack PDU association if the rack PDU has been removed from the target:**

1. Click Device Settings > Port Configuration and then click on the active target.
2. Associate the active target to the disconnected power port. This will break the disconnected target's power association.

Finally, associate the active target to the correct power port.

Dominion KX I Power Strip Configuration

The Dominion KX (with the latest firmware) supports up to eight KX I devices, and requires P2CIM-PWR and straight CAT5 cable. You can associate up to four outlets to a target server. All four outlets can be from separate Dominion PX devices, if needed.

Setup Preparation

You must have a power strip and the P2CIM-PWR Computer Interface Module (CIM). By default the P2CIM-PWR is *not* included with Raritan power strips.

To receive the P2CIM-PWR CIM with the power strip, you must order the power strip with a part number that ends in PK (for example, PCR8-15-PK). Alternatively, the CIM can be ordered separately from the power strip. Raritan devices must be ordered from Raritan or an authorized Raritan reseller.

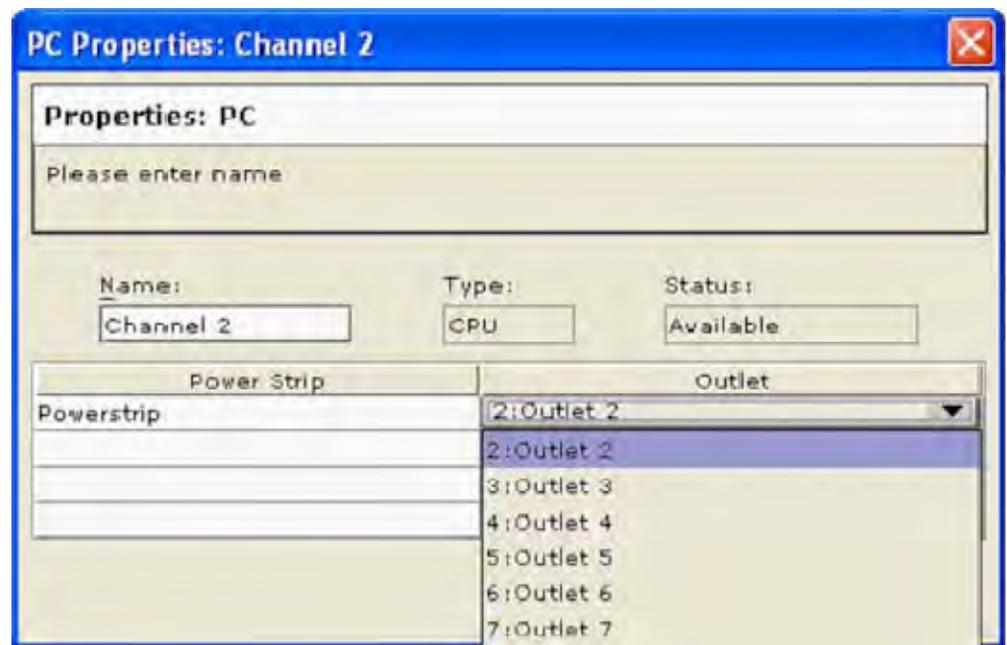
Connecting the Power Strip

1. Connect the male RJ-45 of the P2CIM-PWR to the female RJ-45 connector on the serial port power strip.
2. Connect the female RJ-45 connector of the P2CIM-PWR to any of the available female system port connectors on the Dominion KX using a straight through Cat 5 cable.
3. Power on the power strip.
4. Power on the device.

Configuring the Power Strip

Once the power strip has been added, Dominion KX Manager will automatically recognize that it is connected. The Device Tree in the left panel of the window will change the appropriate target icon to indicate that a power strip is connected to that port.

1. Select the power strip icon, right-click on it, and then click Properties. When the Power Strip Properties dialog appears, type a name for the new power strip and click OK.
2. In the Devices Tree, select the target server(s) powered through the power strip. Right-click on the server icon and click Properties. The PC Properties window appears.



3. Click on one of the Power Strip rows in the table and a list of available power strips connected to the Dominion KX appears. Click on the appropriate power strip.
4. Click on the Outlet drop-down that is associated the selected power strip. A list of available outlets is displayed. Select the outlet to which the device is connected.

Repeat these steps for all devices plugged into multiple outlets. Once outlets have been assigned, Remote Power Management to the associated server will be available in the associated client software (see Multi-Platform Client and Raritan Remote Client).

Note: Be sure to assign the correct outlets to each channel. If more than one outlet is physically associated with a different server, you could accidentally switch the wrong server off.

KX Manager Application

Use Raritan's KX Manager application to configure associations.

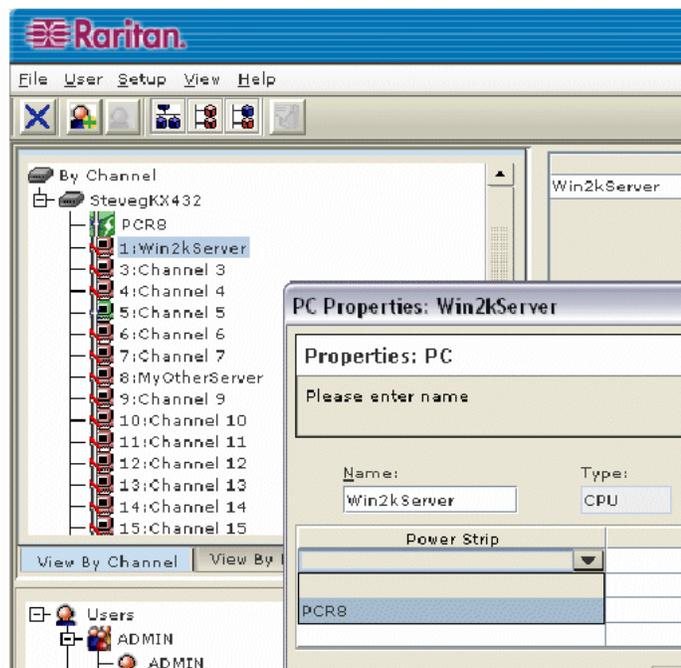
► **To configure associations:**

1. Select the target.
2. Edit the Properties and choose the outlets to associate. The outlets are automatically renamed to the associated target server's name.
3. RRC for control.
4. Select the target.
5. Select On, Off, or Recycle power from the pop-up menu.

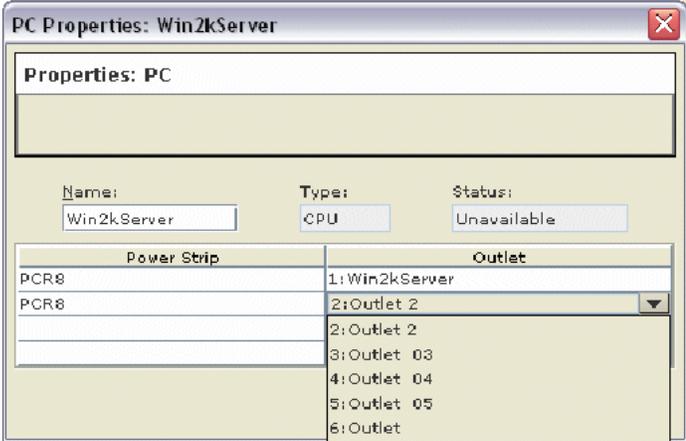
See the **KX User Guide** for details.

Associating Outlets with a Target Server

1. Select a target server. Then select Properties from pop-up menu.
2. Select up to eight Dominion PX devices from drop-down list.



3. Select up to a total of four outlets from the Dominion PX devices.

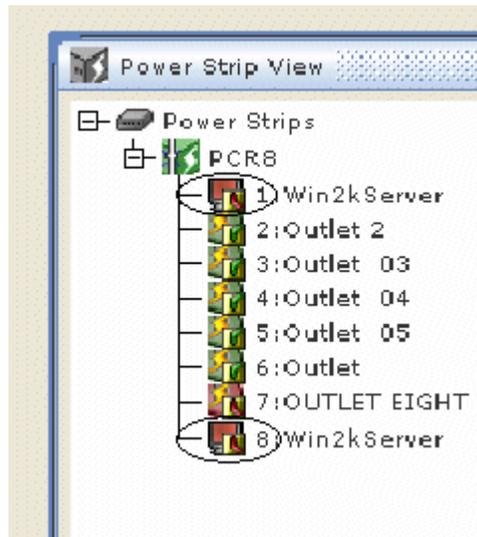


4. Notice the target icon change to indicate power.



5. Notice the outlet icon change to indicate association.

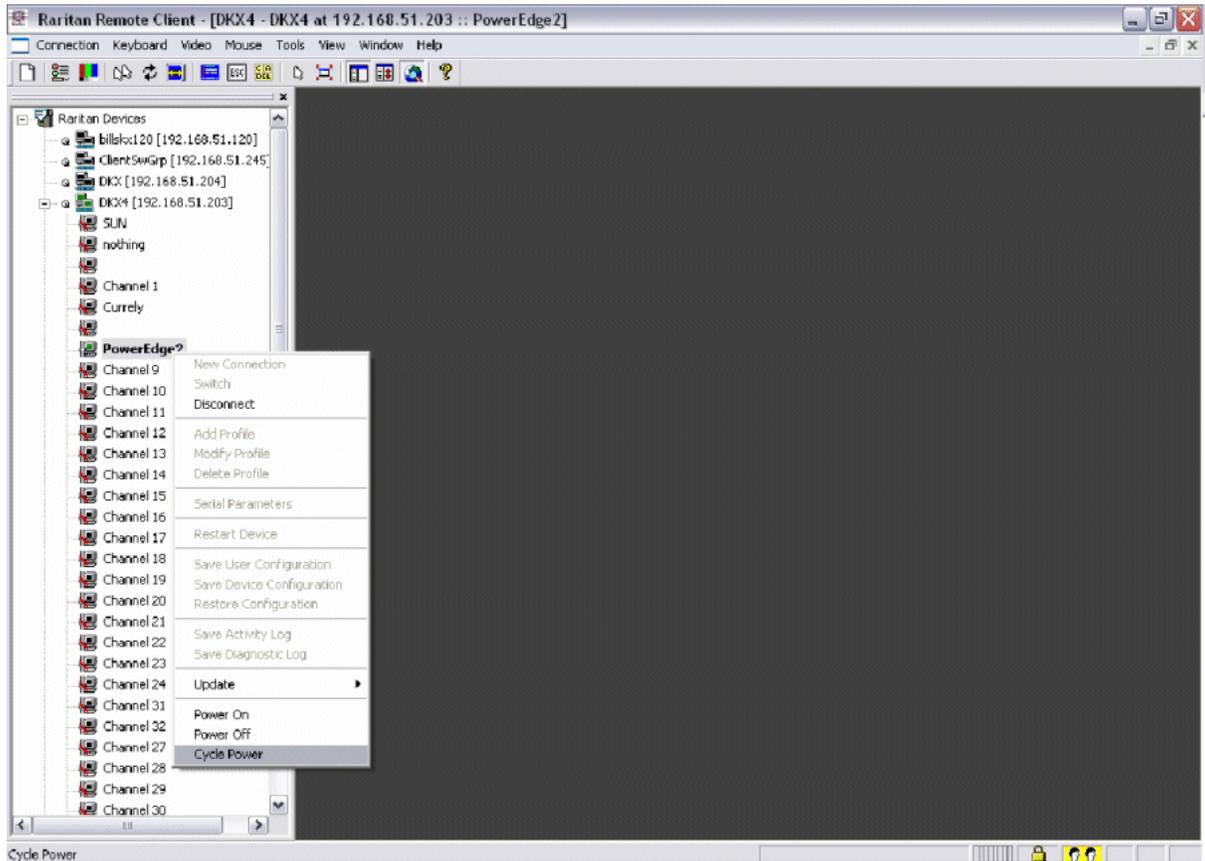
6. Notice the outlet name automatically changes to the target's name.



Controlling a Target Server's Power

1. Select the target server associated with outlets.

2. Select from Power On, Power Off, or Cycle Power options.



Paragon II

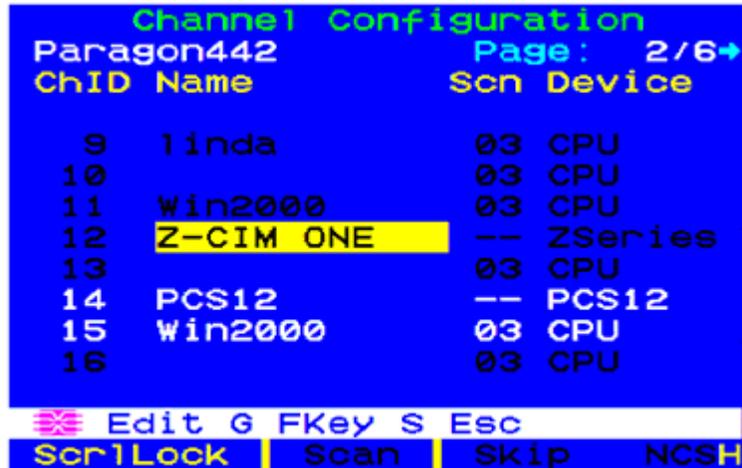
Paragon II integration requires P2CIM-PWR and straight CAT5 cable. You can associate up to four outlets to a target server, and all four outlets can be from separate Dominion PX devices, if necessary.

For more information on Paragon II, see either of the following:

- Paragon II User Guide: Available on the Raritan website's **Firmware and Documentation section** (<http://www.raritan.com/support/firmware-and-documentation/>).
- Paragon II Online Help: Available on the **Product Online Help section** (<http://www.raritan.com/support/online-help/>).

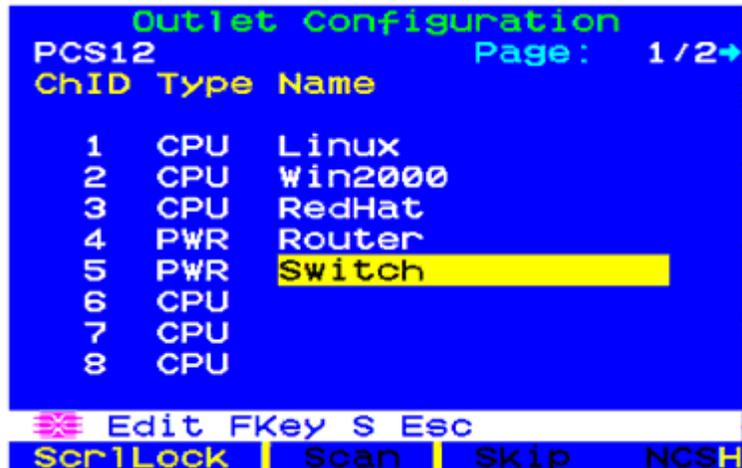
Adding a Dominion PX in Paragon II

Add a Dominion PX device exactly as you would add any second-tier device. Your Paragon II auto-detects the Dominion PX device and changes the device type to PCR8, PCS12, PCS20, DPX16, or DPX24. On the OSD screen, press F5 to enter the Channel Configuration page. Select the channel and change the channel name from the default name to an identifying name for the Dominion PX device.



Associating Outlets with a Target Server

On the OSD screen, press the F5 key to enter the Channel Configuration page and select the channel. Press G to enter the Outlet Configuration page, and associate each outlet with appropriate IT devices.



Controlling a Target Server's Power

After associating the outlets with target servers, you can turn on, turn off or power cycle a target by controlling the outlets.

► To control a target server's power:

1. Select a target server from the Selection Menu or Selection Menu by Name page, and press F3 to control power.
 - If no outlets are associated with the server, the message "No Outlets / Access Denied" appears.
 - If no permissions to outlets associated with the server exist, the message "No Outlets / Access Denied" appears.
 - Paragon automatically switches to the channel, so that the server is displayed in the background. If the switch fails, the message Switch fail appears.
 - If the switch is successful, all outlets associated with the server are displayed and so are the following power control options.
 - Power Off (X)
 - Power On (O)
 - Recycle Power (R)
 - Select All (A)
2. Select the outlet and press X, O, or R. If there are multiple associated outlets, you can press A to select all outlets and then press X, O, or R.
 - If O, execute on command.
 - If X or R, "Are you sure (yes/no)?" is displayed. Users must type `yes` (case insensitive) in order for command to execute. The full word, "yes" must be typed to execute the command.

Controlling an Outlet's Power

Use the Selection Menu, except for Selection Menu by Name, to navigate to individual Dominion PX ports and control power.

► To control an outlet's power:

1. Select the Dominion PX device from the Selection Menu.
2. The Outlet Selection page opens, and the following message should appear.
 - Power Off (X)
 - Power On (O)
 - Recycle Power (R)
3. Select an outlet and press X, O, or R:

- If there is no permission to the outlet, the message "No Outlets / Access Denied" appears.
- If O, execute on command.
- If X or R, "Are you sure (yes/no)?" is displayed. Users must type `yes` (case insensitive) in order for command to execute. The full word, "yes" must be typed to execute the command.

Paragon Manager Application

Use Raritan's Paragon Manager application to configure associations. Note that Paragon Manager cannot be used to control power.

► **To associate outlets with target servers using Paragon Manager:**

1. In Paragon Manager, select the target server.
2. Drag and drop it on the desired outlets shown in the Power Strip View panel.
3. The outlets are renamed to the associated target's name.

*Note: For more information on Paragon Manager, see the Paragon Manager User Guide, which can be downloaded from the Raritan website's **Firmware and Documentation section** (<http://www.raritan.com/support/firmware-and-documentation/>).*

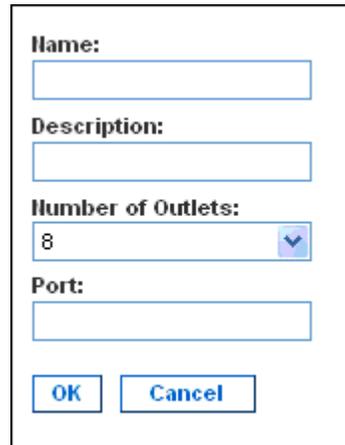
Dominion SX

By connecting to a Dominion SX device, you can associate one or more outlets on a Dominion PX device to specific Dominion SX ports.

Configuring a Dominion PX on Dominion SX

1. Choose Setup > Power Strip Configuration.

2. Click Add. The Power Strip Configuration screen appears.



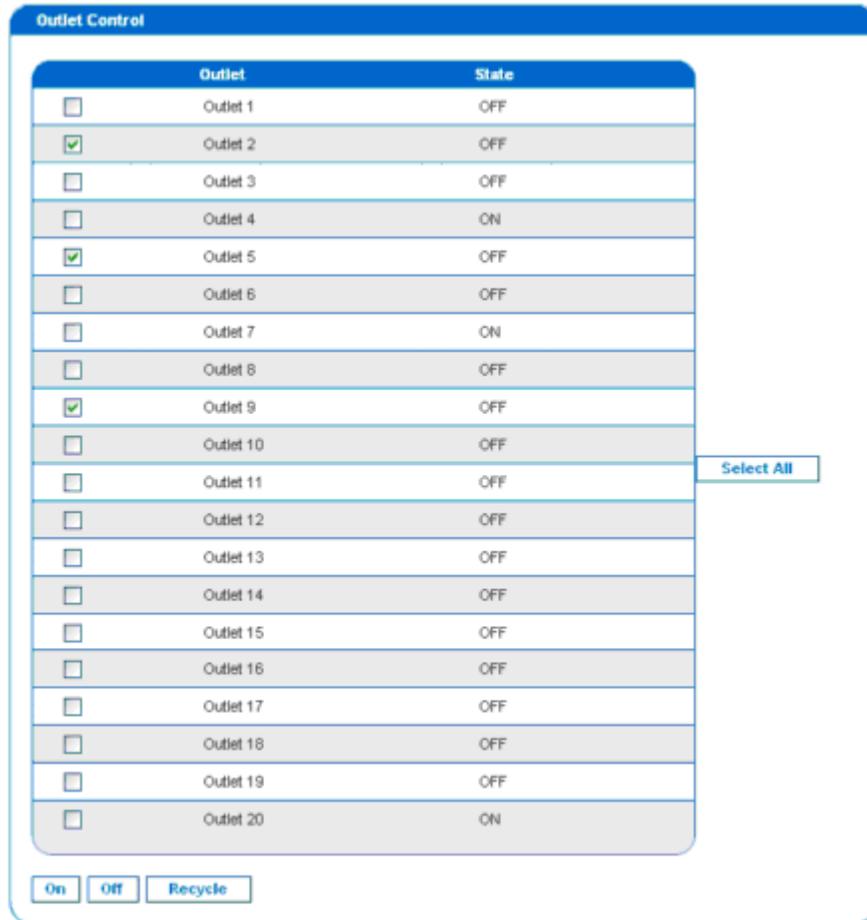
The image shows a configuration dialog box for a power strip. It contains four input fields: 'Name', 'Description', 'Number of Outlets', and 'Port'. The 'Number of Outlets' field is a dropdown menu currently set to '8'. At the bottom are 'OK' and 'Cancel' buttons.

Name: <input type="text"/>
Description: <input type="text"/>
Number of Outlets: <input type="text" value="8"/>
Port: <input type="text"/>
<input type="button" value="OK"/> <input type="button" value="Cancel"/>

3. Type a name and description in the Name and Description fields.
4. Select the number of outlets from the Number of Outlets drop-down menu.
5. Type the port number in the Port field.
6. Click OK.

Power Control

1. Choose Power Control > Power Strip Power Control. The Outlet Control screen appears.



2. Check the box of outlet number you wish to control, and click On/Off buttons to power on/off the selected outlet(s).
3. A confirmation message appears, indicating successful operation.

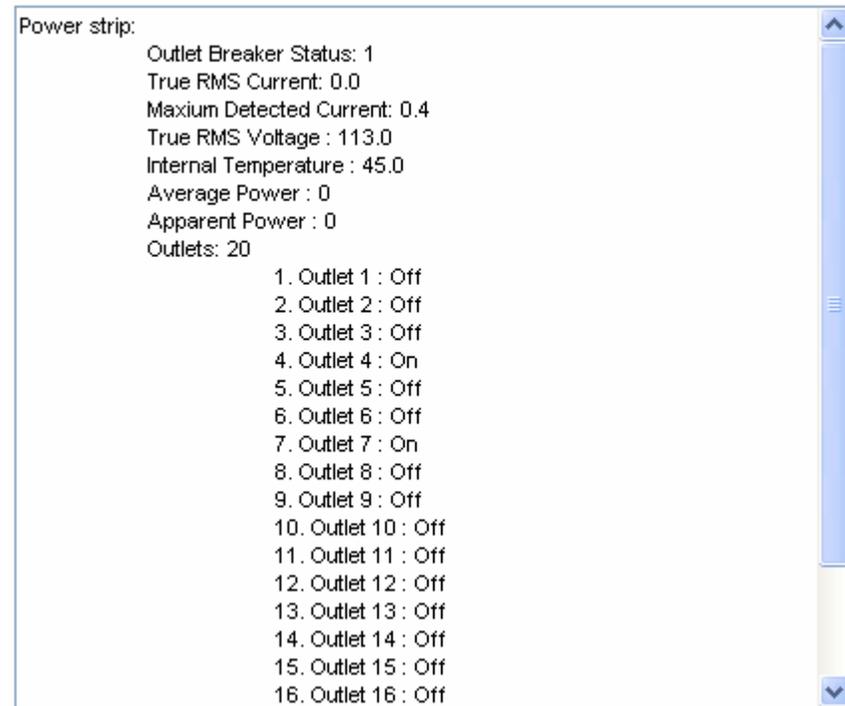
Outlet 19: The power operation has been sent.

The system shall reflect successful operations shortly.

Checking Power Strip Status

1. Choose Power Control > Power Strip Status.

DPX Status:



2. A status box appears, displaying details of the controlled Dominion PX, including power state of each outlet on the device.

Dominion KSX

Dominion KSX does not support connectivity with Dominion PX. However, Dominion PX can be managed as a serial target on one of KSX's serial ports, interacting through CLP interface.

Dominion KSX 2 supports Dominion PX integration.

CommandCenter Secure Gateway

You can manage a Dominion PX from a CommandCenter Secure Gateway (CC-SG) if it is connected through any of the following Raritan products:

- Dominion SX
- Dominion KX
- Paragon II

See the **CC-SG Administrators Guide** for more details.

Note: If you have to reboot or power OFF the Dominion PX device while it is integrated with a Raritan product under CC-SG management you should PAUSE MANAGEMENT of the integrated product until the Dominion PX device fully powers ON again. Failure to do so may result in the outlets being deleted from CC-SG's view and your power associations becoming lost when the Dominion PX device is back online.

Direct Control from CC-SG 4.0 or Later

CommandCenter Secure Gateway 4.0 or later can discover Dominion PX units on the local network and can provide direct control over their outlet states (ON, OFF, and recycle).

*Note: Currently the CommandCenter Secure Gateway (CC-SG) CANNOT manage or control the Dominion PX running in the FIPS mode, but a new release of CC-SG (version 5.3) scheduled for the second quarter of 2012 will implement its management or control. See **Impact on the Raritan Product Integration** (on page 157).*

Appendix E Using the IPMI Tool Set

The IPMI tool set is command-line that allows users to display channel information, print sensor data, and set LAN configuration parameters. The following explains the available IPMI commands.

Note: The open source IPMI tool can be downloaded from sourceforge, and compiled on Linux system . Then users can interact with the Dominion PX via IPMI protocol through this tool. An example at the Linux command shell is given as: \$ ipmitool -I lan -H 192.168.51.58 -U admin -a channel info

In This Chapter

Channel Commands	237
Event Commands	238
LAN Commands	239
Sensor Commands	241
OEM Commands	242
IPMI Privilege Levels	250
IPMI in the FIPS Mode	251

Channel Commands

authcap <channel number> <max priv>

Displays information about the authentication capabilities of the selected channel at the specified privilege level. Possible privilege levels are:

1. Callback level
2. User level
3. Operator level
4. Administrator level
5. OEM Proprietary level

Example

```
$ ipmitool -I lan -H 192.168.51.58 -U admin -a channel  
authcap 14 5
```

See **IPMI Privilege Levels** (on page 250) for additional information about IPMI privileges.

info [channel number]

Displays information about the selected channel. If no channel is given it displays information about the currently used channel:

Example

```
$ ipmitool -I lan -H 192.168.51.58 -U admin -a channel
info
```

getaccess <channel number> [userid]

Configures the given userid as the default on the given channel number. When the given channel is subsequently used, the user is identified implicitly by the given userid.

Example

```
$ ipmitool -I lan -H allen-dpxpcr20-20 -U admin -P
raritan1 channel getaccess 14 63
```

**setaccess <channel number> <userid>[callin=on|off] [ipmi=on|off]
[link=on|off] [privilege=level]**

Configures user access information on the given channel for the given userid.

Example

```
$ ipmitool -I lan -H allen-dpxpcr20-20 -U admin -P
raritan1 channel setaccess 14 63 privilege=5
```

getciphers <all | supported> <ipmi | sol> [channel]

Displays the list of cipher suites supported for the given application (ipmi or sol) on the given channel.

Example

```
$ ipmitool -I lan -H allen-dpxpcr20-20 -U admin -P
raritan1 channel getciphers ipmi 14
```

Event Commands

The Event commands allow you to send pre-defined events to a Management Controller.

<predefined event number>

Sends a pre-defined event to the System Event Log. The Currently supported values for are:

- Temperature: Upper Critical: Going High
- Voltage Threshold: Lower Critical: Going Low
- Memory: Correctable ECC Error Detected

Note: These pre-defined events usually do not produce "accurate" SEL records for a particular system because they will not be correctly tied to a valid sensor number. However, they are sufficient to verify correct operation of the SEL.

Example

```
$ ipmitool -I lan -H allen-dpxpcr20-20 -U admin -P
raritan1 event 1
```

file <filename>

Event log records specified in filename is added to the System Event Log. The format of each line in the file is as follows:

<{EvM Revision} {Sensor Type} {Sensor Num} {Event Dir/Type} {Event Data 0} {Event Data 1} {Event Data 2}>[# COMMENT]

Note: The Event Dir/Type field is encoded with the event direction as the high bit (bit 7) and the event type as the low 7 bits.

Example

```
0x4 0x2 0x60 0x1 0x52 0x0 0x0 # Voltage threshold: Lower
Critical: Going Low
```

LAN Commands

The LAN commands allow you to configure the LAN channels.

print <channel>

Prints the current configuration for the given channel.

set <channel> <parameter>

Sets the given parameter on the given channel. Valid parameters are:

- *ipaddr* <x.x.x.x> Sets the IP address for this channel.
- *netmask* <x.x.x.x> Sets the netmask for this channel.
- *macaddr* <xx:xx:xx:xx:xx:xx> Sets the MAC address for this channel.
- *defgw ipaddr* <x.x.x.x> Sets the default gateway IP address.
- *defgw macaddr* <xx:xx:xx:xx:xx:xx> Sets the default gateway MAC address.
- *bakgw ipaddr* <x.x.x.x> Sets the backup gateway IP address.
- *bakgw macaddr* <xx:xx:xx:xx:xx:xx> Sets the backup gateway MAC address.
- *password* <pass> Sets the null user password.
- *snmp* <community string> Sets the SNMP community string.
- *user* Enables user access mode for userid 1 (issue the `user` command to display information about userids for a given channel).
- *access* <on/off> Set LAN channel access mode.
- *ipsrc* Sets the IP address source:
 - none* unspecified
 - static* manually configured static IP address
 - dhcp* address obtained by DHCP
 - bios* address loaded by BIOS or system software
- *arp respond* <on/off> Sets generated ARP responses.
- *arp generate* <on/off> Sets generated gratuitous ARPs.
- *arp interval* <seconds> Sets generated gratuitous ARP interval.
- *auth* <level,...> <type,...> Sets the valid authtypes for a given auth level.
 - Levels:* callback, user, operator, admin
 - Types:* none, md2, md5, password, oem
- *cipher_privs* <privlist> Correlates cipher suite numbers with the maximum privilege level that is allowed to use it. In this way, cipher suites can be restricted to users with a given privilege level, so that, for example, administrators are required to use a stronger cipher suite than normal users.

The format of *privlist* is as follows. Each character represents a privilege level and the character position identifies the cipher suite number. For example, the first character represents cipher suite 1 (cipher suite 0 is reserved), the second represents cipher suite 2, and so on. *privlist* must be 15 characters in length.

Characters used in privlist and their associated privilege levels are:

- X Cipher Suite Unused
- c CALLBACK
- u USER
- O OPERATOR
- a ADMIN
- O OEM

Sensor Commands

The Sensor commands allow you to display detailed sensor information.

list

Lists sensors and thresholds in a wide table format.

Example

```
$ ipmitool -I lan -H allen-dpxpcr20-20 -U admin -a sensor
list
```

get <id> ... [<id>]

Prints information for sensors specified by name.

Example

```
$ ipmitool -I lan -H allen-dpxpcr20-20 -U admin -P
raritan1 sensor get "R.14 Current"
```

thresh <id> <threshold> <setting>

This allows you to set a particular sensor threshold value. The sensor is specified by name. Valid thresholds are:

- *unr* Upper Non-Recoverable
- *ucr* Upper Critical
- *unc* Upper Non-Critical
- *lnc* Lower Non-Critical
- *lcr* Lower Critical
- *lnr* Lower Non-Recoverable

Example

```
$ ipmitool -I lan -H allen-dpxpcr20-20 -U admin -P
raritan1 sensor thresh "R.14 Current" unr 10.5
```

OEM Commands

You can use the OEM commands to manage and control the operation of the Dominion PX device.

OEM Net-Fn is as defined below:

```
#define IPMI_NETFN_OEM_PP          0x3C
```

The table lists each OEM command and gives its ID. The sections that follow explain each command in greater detail.

Command Name	Id
Set Power On Delay Command	0x10
Get Power On Delay Command	0x11
Set Receptacle State Command	0x12
Get Receptacle State Command	0x13
Set Group State Command	0x14
Set Group Membership Command	0x15
Get Group Membership Command	0x16
Set Group Power On Delay Command	0x17
Get Group Power On Delay Command	0x18
Set Receptacle ACL	0x19
Get Receptacle ACL	0x1A
Set Sensor Calibration	0x1B
Test Actors	0x1C
Test Sensors	0x1D
Set Power Cycle Delay Command	0x1E
Get Power Cycle Delay Command	0x1F

A Note about Group Commands

When sending Group commands, a valid group number (0 through 23, or 255) must be used. Only the group number itself can be sent, alpha-numeric expressions for group numbers are incorrect, and cause the command to be ignored.

For example, sending the following is incorrect:

```
#ipmitool -H 192.168.80.43 -U admin -P pass raw 0x3c 0x14
grp2 0
```

The Dominion PX ignores this command.

A Note about Outlet Numbers

An outlet command uses decimal numerals to represent outlets. Each decimal numeral must be converted into a binary one consisting of 8 numeric digits for indicating 8 outlets. Note that the lowest-numbered outlet is located on the rightmost digit of 8 digits.

- The first decimal numeral represents outlets 1 to 8, and its outlet sequence in a binary numeral is shown below:

8 - 7 - 6 - 5 - 4 - 3 - 2 - 1

For example:

- 0000 0001 refers to outlet 1.
- 0000 0101 refers to outlets 1 and 3.

- The second decimal numeral represents outlets 9 to 16, and its outlet sequence in a binary numeral is shown below:

16 - 15 - 14 - 13 - 12 - 11 - 10 - 9

For example:

- 0000 1001 refers to outlets 9 and 12.
- 0000 1100 refers to outlets 11 and 12.

- The third decimal numeral represents outlets 17 to 24, and its outlet sequence in a binary numeral is shown below:

24 - 23 - 22 - 21 - 20 - 19 - 18 - 17

For example:

- 0001 0101 refers to outlets 17, 19, and 21.
- 0001 0111 refers to outlets 17, 18, 19 and 21.

Below is the outlet conversion table from decimal to binary numerals:

Decimal	Binary	Decimal	Binary
1	0000 0001	13	0000 1101

Decimal	Binary	Decimal	Binary
2	0000 0010	14	0000 1110
3	0000 0011	15	0000 1111
4	0000 0100	16	0001 0000
5	0000 0101	17	0001 0001
6	0000 0110	18	0001 0010
7	0000 0111	19	0001 0011
8	0000 1000	20	0001 0100
9	0000 1001	21	0001 0101
10	0000 1010	22	0001 0110
11	0000 1011	23	0001 0111
12	0000 1100	24	0001 1000

Example

To group outlets 2, 10, 12, 19, and 21, first convert these outlets to 3 decimal numerals:

- Outlet 2 = 0000 0010 (binary) = 2 (decimal)
- Outlets 10 and 12 = 0000 1010 (binary) = 10 (decimal)
- Outlets 19 and 21 = 0001 0100 (binary) = 20 (decimal)

Add these decimal numerals to the end of the Set Group Membership command and the command looks like this:

```
#ipmitool -H 192.168.57.155 -U admin -P pass raw 0x3c 0x15
0 1 2 10 20
```

For details about the command, see **Set Group Membership Command** (on page 247).

Set Power On Delay Command

The global power on delay defines how much time has to pass between two power on actions.

Request Data	1	delay in seconds the delay is the minimum time after which a receptacle is switched on after a previous receptacle has been switched on.
Response Data	1	Completion Code

Get Power On Delay Command

Request Data	-	-
Response Data	1	Completion Code
	2	delay in seconds

Set Receptacle State Command

This command is used to switch on/off and recycle individual receptacles.

Request Data	1	# of receptacle [7 - 5] reserved [4 - 0] # of receptacle, 0 based, highest valid # depends on device model
	2	new state [7 - 2] reserved [1] 1b = recycle, ignoring [0], 0b = get new state from [0] [0] 1b = power on, 0b = power off
Response Data	1	Completion Code

Get Receptacle State Command

Request Data	1	# of receptacle [7 - 5] reserved [4 - 0] # of receptacle, 0 based, highest valid # depends on device model
Response Data	1	Completion Code
	2	current receptacle state and visual state [7] reserved [6] 1b = blinking, 0b = steady [5] 1b = LED green on, 0b = off [4] 1b = LED red on, 0b = off [3] 1b = enqueued to be switched on, 0b = not enqueued [2] 1b = in power cycle delay phase, 0b = not delayed [1] 1b = released because of soft breaker, 0b = norm [0] 1b = power on, 0b = power off

Get Receptacle State and Data Command

Request Data	1	# of receptacle [7 - 5] reserved [4 - 0] # of receptacle, 0 based, highest valid # depends on device model
Response Data	1	Completion Code
	2	current receptacle state and visual state [7] reserved [6] 1b = blinking, 0b = steady [5] 1b = LED green on, 0b = off [4] 1b = LED red on, 0b = off [3] 1b = enqueued to be switched on, 0b = not enqueued [2] 1b = in power cycle delay phase, 0b = not delayed [1] 1b = released because of soft breaker, 0b = norm [0] 1b = power on, 0b = power off
	3	Number of bytes of data = 2 or 6
	4	Apparent Power
	5	Active Power
	6-9	Active Energy, LSB First

Set Group State Command

This command is used to switch on/off all receptacles belonging to a group. There is no Get Group State Command. Getting the state of a receptacle has to be carried out with Get Receptacle State Command.

Request Data	1	# of group [7 - 5] reserved [4 - 0] group #, valid numbers: 0 - 23, 255
	2	new state [7 - 1] reserved [0] 1b = power on, 0b = power off
Response Data	1	Completion Code

Set Group Membership Command

Request Data	1	# of group [7 - 5] reserved [4 - 0] group #, valid numbers: 0 - 23, 255
	2	[7 - 1] reserved [0] 1b = enable group, 0b = disable group
	3	[7] 1b = receptacle 7 belongs to group ... [0] 1b = receptacle 0 belongs to group
	4	[7] 1b = receptacle 15 belongs to group ... [0] 1b = receptacle 8 belongs to group
	5	[7] 1b = receptacle 23 belongs to group ... [0] 1b = receptacle 16 belongs to group
Response Data	1	Completion Code

Get Group Membership Command

Request Data	1	# of group [7 - 5] reserved [4 - 0] group #, valid numbers: 0 - 23, 255
Response Data	1	Completion Code
	2	[7 - 1] reserved [0] 1b = group is enabled, 0b = group is disabled
	3	[7] 1b = receptacle 7 belongs to group ... [0] 1b = receptacle 0 belongs to group
	4	[7] 1b = receptacle 15 belongs to group ... [0] 1b = receptacle 8 belongs to group
	5	[7] 1b = receptacle 23 belongs to group ...

		[0] 1b = receptacle 16 belongs to group
--	--	---

Set Group Power On Delay Command

Request Data	1	# of group [7 - 5] reserved [4 - 0] group #, valid numbers: 0 - 23, 255
	2	delay in seconds This delay overwrites the global delay for all receptacles in that group. The delay applies not only when using the Set Group State Command but also when using Set Receptacle State Command.
Response Data	1	Completion Code

Get Group Power On Delay Command

Request Data	1	# of group [7 - 5] reserved [4 - 0] group #, valid numbers: 0 - 23, 255
Response Data	1	Completion Code
	2	delay in seconds

Set Receptacle ACL

ACLs define who is authorized to change the state of a receptacle. ACLs are stored for each individual outlet. A single ACL entry defines whether a certain user id or privilege level is allowed or denied to issue control commands for the outlet. ACL are evaluated top to bottom, hence order of ACL entries is important. If there is no ACL entry at all, receptacle ACLs are disabled, i.e. any user id has access.

Request Data	1	# of receptacle
	2	number of ACL entries to follow
	3 +N	ACL entry [7] 0b = deny, 1b = allow [6] 0b = user id, 1b = privilege level [5 - 0] user id or privilege level depending on [6]
Response Data	1	Completion Code

Get Receptacle ACL

Request Data	1	# of receptacle
Response Data	1	Completion Code
	2	number of ACL entries to follow
	3	ACL entry
	+N	[7] 0b = deny, 1b = allow [6] 0b = user id, 1b = privilege level [5 - 0] user id or privilege level depending on [6]

Test Actors

Used for hardware testing during production

Request Data	1	[7 - 2] reserved [1] Beeper test, 0b - disable, 1b - enable [0] 7 segment display test, 0b - disable, 1b - enable
Response Data	1	Completion Code

Test Sensors

Used for hardware testing during production

Request Data	1	-
Response Data	1	Completion Code
	2	[7 - 2] reserved [1] down button, 0b - not pressed, 1b - pressed [0] up button, 0b - not pressed, 1b - pressed

Set Power Cycle Delay Command

Request Data	1	# of receptacle (0xFF for global unit delay)
	2	Delay (seconds), 1-255 for unit and receptacle, 0 fallback to unit delay (receptacle only)
Response Data	1	Completion Code

Get Power Cycle Delay Command

Request Data	1	# of receptacle (0xFF for global unit delay)
Response Data	1	Completion Code
	2	Delay (seconds), 1-255, 0 if not set (receptacle only)

Note: Values greater than 255 cannot be sent to the Dominion PX via IPMI. To set the Power Cycle Delay to longer than 255 seconds, use the web interface.

IPMI Privilege Levels

The IPMI privilege level that you select determines:

	IPMI Privilege Level:					
	No Access	Callback	User	Operator	Administrator	OEM
Authentication Settings	No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No
Change Password	No	No	No	No	Yes	Yes
Date/Time Settings	No	No	No	Yes	Yes	Yes
Firmware Update	No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No
Log Settings	No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No
Log View	No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No
Network Dyn/DSN Settings	No	No	No	No	Yes	Yes
Power Control Setting	No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No
SNMP Setting	No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No
SSH/Telnet Access	No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No
SSL Certificate	No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No

	IPMI Privilege Level:					
	No Access	Callback	User	Operator	Administrator	OEM
Management						
Security Settings	No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No
Unit Reset	No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No
User/Group Management	No	No	No	No	Yes	Yes
User Group Permissions	No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No

IPMI in the FIPS Mode

In the FIPS mode, you must meet the requirements below to use the IPMI.

- Only IPMI v2.0 is supported.
- FIPS approved algorithms for IPMI:
 - Authentication algorithms:
 - RAKP-HMAC-SHA1
 - RAKP-HMAC-SHA256
 - Integrity algorithms:
 - HMAC-SHA1-96
 - HMAC-SHA256-128
 - Encryption algorithms:
 - AES-CBC-128
- ipmitool commands:
 - You must use the *lanplus* interface.
 - Example:


```
$ ipmitool -I lanplus -H allen-dpxpcr20-20 -U admin -P raritan1 sensor get "R.14 Current"
```
 - The parameter used with the *-C* option for ciphersuite must be 3. This is because the *-C 3* option corresponds to RAKP-HMAC-SHA1 authentication, HMAC-SHA1-96 integrity and AES-CBC-128 encryption algorithms.

Example:

Appendix E: Using the IPMI Tool Set

```
$ ipmitool -I lanplus -U admin -P raritan1 -C 3 -H  
192.168.50.13 mc info
```

Appendix F Additional PDU Information

In This Chapter

Default Hysteresis Values for Thresholds	253
Event Types.....	253
MAC Address	255
Altitude Correction Factors	255
Data for BTU Calculation.....	256

Default Hysteresis Values for Thresholds

This table describes the default hysteresis values for each type of measurement. Values must recede past the threshold by the hysteresis value before the Dominion PX de-asserts the condition. You can disable the hysteresis feature for outlet current while the feature for other measurements continue to apply. Or you can change the default hysteresis on appropriate threshold pages for each measurement.

Measurement	Lower Critical	Lower Non-Critical	Upper Critical	Upper Non-Critical
Outlet RMS Current (Amps)	+0.9	+0.9	-0.9	-0.9
Unit/Line RMS Voltage (Volts)	+5	+5	-5	-5
Unit/Line RMS Current (Amps)	-	-	-1	-1
Circuit Breaker Current (Amps)	-	-	-1	-1
PDU Temperature (Degrees Celsius)	+1	+1	-1	-1
Environmental Temperature (Degrees Celsius)	+2	+2	-2	-2
Environmental Humidity (%)	+1	+1	-1	-1

Event Types

Event Type	Examples
Outlet Control	Outlet(#) switched on by user Outlet(#) switched off by user Outlet(#) cycled by user
Outlet/Unit/Environmental Sensors	Assertion: Environmental Temperature (#) above upper non-critical threshold Deassertion: Environmental Temperature (#) above upper critical threshold
User/Group Administration	User added successfully User successfully changed User successfully deleted User password successfully changed Group added successfully Group successfully changed Group successfully deleted
Security Relevant	User login failed
User Activity	User logged in successfully User logged out User session timeout Note: The user activity entries in the event log always show the IP address of the computer that logged in or out. Entries with an IP address of 127.0.0.1 (the loopback IP address) represent a serial connection and a CLP session.
Device Operation	Device successfully started
Device Management	The Device update has started
Virtual Device Management	Master PDU lost connectivity with SlaveIPAddress

MAC Address

A label is affixed to a Dominion PX device, near the LED display, showing both the serial number and MAC address of the PDU.



If necessary, you can find the PDU's IP address through the MAC address by using commonly-used network tools. Contact your LAN administrator for assistance.

Altitude Correction Factors

If a Raritan differential air pressure sensor is attached to your device, the altitude you enter for the device can serve as an altitude correction factor. That is, the reading of the differential air pressure sensor will be multiplied by the correction factor to get a correct reading.

This table shows the relationship between different altitudes and correction factors.

Altitude (meters)	Altitude (feet)	Correction factor
0	0	0.95
250	820	0.98
425	1394	1.00
500	1640	1.01
740	2428	1.04
1500	4921	1.15
2250	7382	1.26
3000	9842	1.38

Data for BTU Calculation

If you need to calculate the heat (BTU/hr) generated by the Dominion PX device, use the following power data in the BTU calculation formula.

Model name	Maximum power (Watt)
PX-nnnn, DPXS, DPXR, DPCS and DPCR series	24

The letter "n" in the model names represents a number.

Appendix G LDAP Configuration Illustration

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

- a. Determine user accounts and groups intended for the Dominion PX
- b. Create user groups for the Dominion PX on the AD server
- c. Configure LDAP authentication on the Dominion PX device
- d. Configure user groups on the Dominion PX device

In This Chapter

Step A. Determine User Accounts and Groups	257
Step B. Configure User Groups on the AD Server	258
Step C. Configure LDAP Authentication on the Dominion PX Device..	259
Step D. Configure User Groups on the Dominion PX Device.....	262

Step A. Determine User Accounts and Groups

Determine the user accounts and groups that are authenticated for accessing the Dominion PX. In this example, we will create two user groups with different permissions. Each group will consist of two user accounts available on the AD server.

User groups	User accounts (members)
PX_User	usera
	pxuser2
PX_Admin	userb
	pxuser

Group permissions:

- The PX_User group will have neither system permissions nor outlet permissions.
- The PX_Admin group will have full system and outlet permissions.

Step B. Configure User Groups on the AD Server

You must create the groups for the Dominion PX on the AD server, and then make appropriate users members of these groups.

In this illustration, we assume:

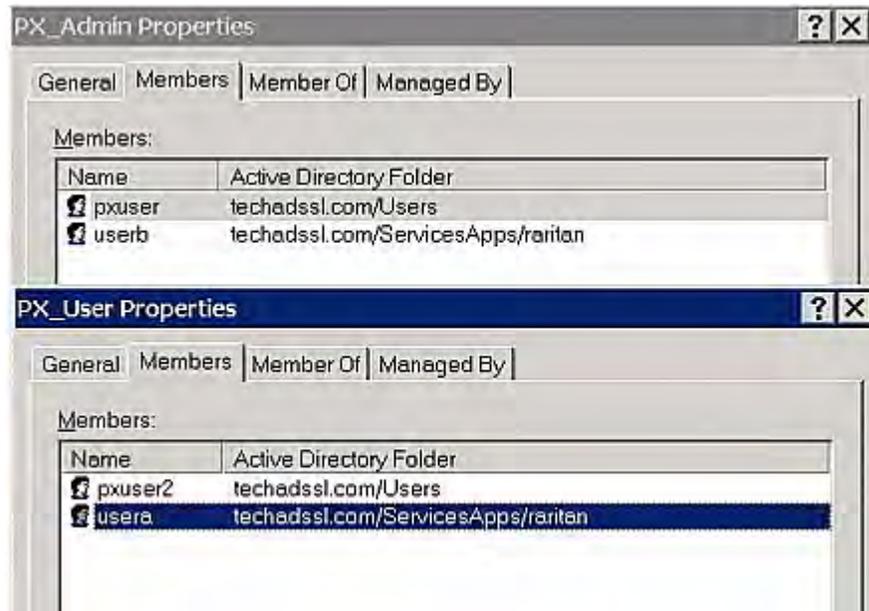
- The groups for the Dominion PX are named *PX_Admin* and *PX_User*.
- User accounts *pxuser*, *pxuser2*, *usera* and *userb* already exist on the AD server.

► **To configure the 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 Dominion PX Device

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

In the illustration, we assume:

- The DNS server settings have been configured properly. See **Modifying the Network Settings** (on page 56) and **Role of a DNS Server** (on page 57).
- 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 SSL.
- The AD server uses the default TCP port 389.
- Anonymous bind is used.
- There is no backup AD server.
- The FIPS mode is disabled.

► **To configure LDAP authentication:**

1. Choose Device Settings > Authentication. The Authentication Settings page opens.
2. Select the LDAP radio button to enable the LDAP section of the page.
3. Provide the Dominion PX with the information about the AD server.
 - Type of external LDAP server - Select "Microsoft Active Directory" from the drop-down list.
 - User LDAP Server - Type the domain name *techadssl.com* or IP address *192.168.56.3*.

Important: Without the SSL 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 SSL encryption is enabled.

- Backup User LDAP Server - Leave the field empty because a backup AD server is unavailable.
- SSL Enabled - Have the checkbox deselected since the SSL encryption is not applied in this example.
- Port - Ensure the field is set to 389.
- SSL Port and Certificate File - Skip the two fields since the SSL encryption is not enabled.
- Bind with credentials - Make sure this checkbox is deselected since anonymous bind is used.
- Bind DN and Password - Skip these two fields because anonymous bind is used.

- Base DN of user LDAP server - Type `dc=techadssl,dc=com` as the starting point where your search begins on the AD server.
- Name of login-name attribute - Type `sAMAccountName` because the LDAP server is Microsoft Active Directory.
- Name of user-entry objectclass - The field is optional. The object class information is helpful for filtering out additional objects in a large directory structure. In this example, we leave it blank.
- 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.

[Home](#) > [Device Settings](#) > [Authentication Settings](#)

Authentication Settings

Local Authentication *

LDAP

Type of external LDAP server
 *

User LDAP Server
 *

Backup User LDAP Server
 *

SSL Enabled *

Port
 *

SSL Port
 *

Certificate File

Anonymous bind *

Bind with credentials *

Bind DN
 *

Password
 *

Base DN of user LDAP server
 *

Name of login-name attribute
 *

Name of user-entry objectclass
 *

User Search Subfilter
 *

Active Directory Domain
 *

*Note: For more information on LDAP configuration, see **Setting Up LDAP Authentication** (on page 114).*

4. Click Apply. The LDAP authentication is activated.

Note: If the Dominion PX clock and the LDAP server clock are out of sync, the certificates are considered expired and users are unable to authenticate using LDAP. To ensure proper synchronization, administrators should configure the Dominion PX and the LDAP server to use the same NTP server.

Step D. Configure User Groups on the Dominion PX Device

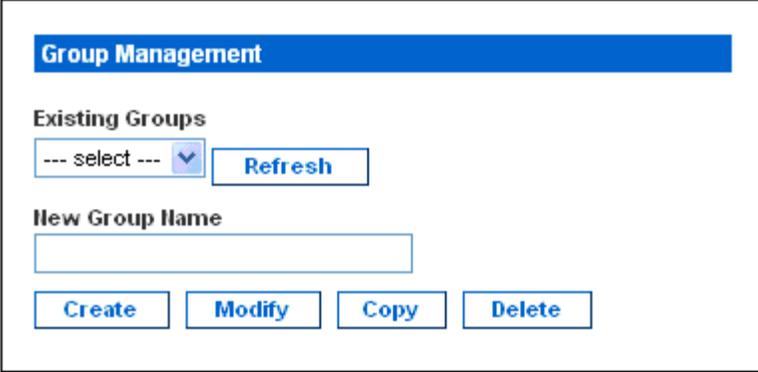
A user group on the Dominion PX device determines the system and outlet permissions. You must create the user groups identical to those created for the Dominion PX on the AD server or authorization will fail. Therefore, we will create the user groups *PX_User* and *PX_Admin* on the PDU.

In this illustration, we assume:

- The *PX_User* group members can neither configure the Dominion PX nor access the outlets.
- The *PX_Admin* group members have the Administrator permissions so they can both configure the Dominion PX and access the outlets.

► **To create the same user groups on the Dominion PX device:**

1. Choose User Management > Users & Groups. The User/Group Management page opens. This window is divided into a User Management panel and a Group Management panel.



The screenshot shows a web interface titled "Group Management". Under the heading "Existing Groups", there is a dropdown menu with the text "--- select ---" and a "Refresh" button. Below this is a section for "New Group Name" with an empty text input field. At the bottom of the section are four buttons: "Create", "Modify", "Copy", and "Delete".

2. In the Group Management panel, type *PX_User* in the New Group Name field.
3. Click Create. The *PX_User* group is created.
4. Repeat Steps 2 to 3 for creating the *PX_Admin* group.

► **To set the system permissions for each group:**

1. Choose User Management > User/Group System Permissions. The User/Group System Permissions page opens.

2. Select PX_User from the Group drop-down list. The permissions that apply to this group appear. Since this is the first time you are setting the system permissions for this group, all permissions are set to No.
3. Set the permissions as necessary. Click on the drop-down list to select a permission level for each permission listed. In this example, all system permissions are set to No (or Deny).

Home > User Management > User/Group System Permissions

User/Group System Permissions

Show permissions for:

User (not in a group)

Group

[Setup Outlet Access Permissions](#)

	Permission
Authentication Settings :	No
Bulk Configuration :	No
Change Password :	No
Date/Time Settings :	No
Environmental Sensor Configuration :	No
Firmware Update :	No
IPMI Privilege Level :	No Access
Log Settings :	No
Log View :	No
Network Settings :	No
Outlet Group Configuration :	No
SIIMP Settings :	No
SIIMP v3 Access :	Deny
SSH/Telnet Access :	No
SSL Certificate Management :	No
Security Settings :	No
Server Status via IPMI :	No
Unit & Outlet Configuration :	No
Unit Reset :	No
User/Group Management :	No
User/Group Permissions :	No

4. Click Apply. The permissions are applied to the PX_User group.

- Repeat Steps 2 to 4 to set the permissions for the PX_Admin group. In this example, all system permissions are set to Yes (or Read-Write).

Home > User Management > User/Group System Permissions

User/Group System Permissions

Show permissions for:

User (not in a group):

Group:

[Setup Outlet Access Permissions](#)

	Permission
Authentication Settings :	Yes ▾
Bulk Configuration :	Yes ▾
Change Password :	Yes ▾
Date/Time Settings :	Yes ▾
Environmental Sensor Configuration :	Yes ▾
Firmware Update :	Yes ▾
IPMI Privilege Level :	Administrator ▾
Log Settings :	Yes ▾
Log View :	Yes ▾
Network Settings :	Yes ▾
Outlet Group Configuration :	Yes ▾
SNMP Settings :	Yes ▾
SNMP v3 Access :	Read-Write ▾
SSH/Telnet Access :	Yes ▾
SSL Certificate Management :	Yes ▾
Security Settings :	Yes ▾
Server Status via IPMI :	Yes ▾
Unit & Outlet Configuration :	Yes ▾
Unit Reset :	Yes ▾
User/Group Management :	Yes ▾
User/Group Permissions :	Yes ▾

► **To set the outlet permissions for each group:**

- Choose User Management > User/Group Outlet Permissions. The User/Group Outlet Permissions page opens.
- Select PX_User from the Group drop-down list. The permissions that apply to this group appear. Since this is the first time you are setting the outlet permissions for this group, all permissions are set to No.

3. Set the permissions as necessary. Click on the drop-down list to select a permission level for each outlet. In this example, all outlet permissions are set to No.

Home > User Management > User / Group Outlet Permissions

User / Group Outlet Permissions

Show outlet permissions for:

User (not in a group)

Group

[Setup User / Group Permissions](#)

	Permission
Outlet 1:	No
Outlet 2:	No
Outlet 3:	No
Outlet 4:	No
Outlet 5:	No
Outlet 6:	No
Outlet 7:	No
Outlet 8:	No

4. Click Apply. The permissions are applied to the PX_User group.

- Repeat Steps 2 to 4 to set the permissions for the PX_Admin group. In this example, all outlet permissions are set to Yes.

Home > User Management > User / Group Outlet Permissions

User / Group Outlet Permissions

Show outlet permissions for:

User (not in a group)

Group

[Setup User / Group Permissions](#)

	Permission
Outlet 1:	<input type="text" value="Yes"/>
Outlet 2:	<input type="text" value="Yes"/>
Outlet 3:	<input type="text" value="Yes"/>
Outlet 4:	<input type="text" value="Yes"/>
Outlet 5:	<input type="text" value="Yes"/>
Outlet 6:	<input type="text" value="Yes"/>
Outlet 7:	<input type="text" value="Yes"/>
Outlet 8:	<input type="text" value="Yes"/>

Appendix H Resetting the PDU Settings

You can reset the Dominion PX settings, including the administrator password, at the local serial console.

To establish a serial connection, see **Connecting the Dominion PX to a Computer** (on page 17).

In This Chapter

Resetting to Factory Defaults	267
Resetting the Administrator Password	268

Resetting to Factory Defaults

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

Important: Exercise caution before resetting the Dominion PX to its factory defaults. This erases existing information and customized settings, such as user profiles and threshold values.

You must have the "Unit & Outlet Configuration" and "Unit Reset" permissions to perform a reset.

When resetting to factory defaults, do *not* use a DB9-to-USB adapter to connect the Dominion PX serial cable to your PC. This may result in misinterpreted characters at the special prompt. Connect the Dominion PX serial cable to a PC with a DB9 serial port instead.

► **To reset to factory defaults:**

1. Connect a computer to the Dominion PX device. See **Connecting the Dominion PX to a Computer** (on page 17).
2. Launch a terminal emulation program such as HyperTerminal, Kermit, or PuTTY, and open a window on the Dominion PX. Make sure the serial port settings use this configuration:
 - Bits per second = 9600
 - Data bits = 8
 - Stop bits = 1
 - Parity = None
 - Flow control = None
3. If the window is blank, press Enter. The Welcome message appears.
4. Type `clp` at the command prompt and press Enter.

5. Type your user name and password to log in to the CLP interface when prompted. See **With HyperTerminal** (on page 181).
6. Type the following command and press Enter.

```
clp:/-> set /system1 FactoryDefaults=true
```
7. Wait until the Welcome message appears, indicating that the reset is completed.

Note: HyperTerminal is available on Windows operating systems prior to Windows Vista. For Windows Vista or later versions, you may use PuTTY, which is a free program you can download from the Internet. See PuTTY's documentation for details on configuration.

Resetting the Administrator Password

If you lose the password for the "admin" user, you can reset the password at the local serial console.

► **To reset the administrator password:**

1. Connect a computer to the Dominion PX device. See **Connecting the Dominion PX to a Computer** (on page 17).
2. Launch a terminal emulation program such as HyperTerminal, Kermit, or PuTTY, and open a window on the Dominion PX. Make sure the serial port settings use this configuration:
 - Bits per second = 9600
 - Data bits = 8
 - Stop bits = 1
 - Parity = None
 - Flow control = None
3. If the window is blank, press Enter. The Welcome message appears.
4. At the command prompt, type `resetadminpassword`, and press Enter.
5. Type the new password for the "admin" user when prompted, and press Enter.
6. Type the same new password again when prompted, and press Enter.
7. The message "Password changed successfully" appears, indicating that the administrator password has been changed successfully.

Index

<

<predefined event number> • 241

1

1U Products • 5

1U Size • 2

2

2U Products • 5

2U Size • 2

A

A False Circuit Breaker Trip Trap • 170

A Note about Group Commands • 245

A Note about Measurement Units • 176

A Note about Outlet Numbers • 245

A Note about the Non-Critical Temperature Threshold Alarm • 38

A Note about Untriggered Alerts • 91, 142, 173

About Contact Closure Sensors • 27

About the CLP Interface • 180

Access Security Control • 97

Adding a Dominion PX in Paragon II • 232

Adding PDUs to Power IQ Management • 220

Additional PDU Information • 255

All Outlets Control • 51

Altitude Correction Factors • 61, 257

Applicable Models • xiii

Assigning or Changing the ID Number • 122, 131

Associating Outlets with a Target Server • 228, 232

Associating Outlets with Target Servers on KX II and LX • 225

Attributes • 185

authcap <channel number> <max priv> • 239

Automatic Mode • 35, 206

B

Balancing Loads • 95

Beeper • 38

Before You Begin • 15

Before You Begin Tool-less Mounting: • 9

Blue LED • 31

C

Changing ID Numbers of Environmental Sensors • 131, 174

Changing the Default Action • 102

Changing the Default Policy • 98, 99

Changing Your Password • 42

Channel Commands • 239

Checking Power Strip Status • 237

Circuit Breaker • 36

Circuit Breaker Details Page • 96

Circuit Breaker Orientation Limitation • 6, 8, 10, 12, 13

Circuit Breaker Status • 49

Closing a Serial Connection • 184

CommandCenter Secure Gateway • 238

Components of an Alert • 132

Configuring a Contact Closure Sensor • 28, 29, 129

Configuring a Dominion PX on Dominion SX • 234

Configuring and Using Alert Notifications • 62, 91, 131

Configuring Environmental Sensors • 119, 122, 127

Configuring Rack PDU (Power Strip) Targets • 222

Configuring the Dominion PX • 17, 56

Configuring the FIPS Mode • xiv, 157, 174

Configuring the Firewall • 20, 98

Configuring the Hysteresis • 173

Configuring the Local Event Log • 145, 147

Configuring the NFS Logging • 148

Configuring the Power Strip • 227

Configuring the SMTP Logging • 149

Configuring the SMTP Settings • 62, 132, 149

Configuring the SNMP Logging • 150

Configuring the SNMP Settings • xiv, 63

Configuring the SNMP Traps • 134, 135, 169

Configuring the Syslog Forwarding • 150

Configuring the Thresholds for Environmental Sensors • 193

Configuring Unbalanced Load Thresholds • 95

Configuring Users for Encrypted SNMP v3 • 167

Connecting a Rack PDU • 222

- Connecting Environmental Sensors (Optional) • 25, 118
- Connecting the Dominion PX to a Computer • 17, 18, 269, 270
- Connecting the Dominion PX to a Power Source • 16
- Connecting the Dominion PX to Your Network • 18
- Connecting the Power Strip • 226
- Connecting Third-Party Detectors/Switches to DPX-CC2-TR • 27
- Connection Ports • 32
- Contact Closure Sensor LEDs • 29
- Controlling a Target Server's Power • 230, 233
- Controlling an Outlet's Power • 233
- Copying a Dominion PX Configuration • 74
- Copying a User Group • 83
- Copying a User Profile • 77
- Copying Configurations with Bulk Configuration • 72
- Creating a Certificate Signing Request • 109
- Creating a User Group • 80
- Creating a User Profile • 39, 75
- Creating Alert Destinations • 133
- Creating Alert Policies • 136, 139
- Creating Alerts • 137, 138
- Creating Firewall Rules • 98, 99
- Creating Group Based Access Control Rules • 101, 102, 103

D

- Data for BTU Calculation • 258
- Default Asterisk • 48
- Default Hysteresis Values for Thresholds • 143, 255
- Deleting a User Group • 84
- Deleting a User Profile • 78
- Deleting Firewall Rules • 101
- Deleting Group Based Access Control Rules • 104
- Deleting Outlet Group Devices • 155
- Derating a Raritan Product • 199
- Describing the Sensor Location • 124, 126
- Diagnostics • 158
- Direct Control from CC-SG 4.0 or Later • xiv, 238
- Disabling Outlet Switching • 173
- Disabling the PDU's Ping Response • 108
- Displaying Additional Details • 51
- Displaying Basic Device Information • 52, 54

- Displaying Model Configuration Information • 53
- Dominion KSX • 237
- Dominion KX I Power Strip Configuration • 226
- Dominion KX II Power Strip Configuration • 222
- Dominion PX Feature RJ-12 Port Pinouts • 211
- Dominion PX Serial RJ-45 Port Pinouts • 211
- Dominion SX • 234

E

- Editing or Deleting Outlet Groups • 155
- Enabling Data Retrieval • 64, 173
- Enabling Login Limitations • 105
- Enabling or Disabling the Power CIM • 25, 217
- Enabling SNMP • xiv, 64, 165
- Enabling Strong Passwords • 107
- Enabling the Feature • 101, 102
- Enabling the Firewall • 98
- Enabling Unbalanced Load Detection • 34, 94
- Enabling User Blocking • 105
- Environmental Sensors • 118
- Equipment Setup Worksheet • 16, 213
- Event Commands • 240
- Event Types • 146, 255
- Example • 178, 246
 - When Hysteresis is Useful • 144
 - When to Disable Hysteresis • 144
- Example 1 - Help Information for the Show Command • 194
- Example 1 - No Attributes • 185, 191
- Example 2 - Getting In-Depth Help Information • 195
- Example 2 - Name Attribute • 186, 192
- Example 3 - CurrentReading Attribute • 192
- Example 3 - powerState Attribute • 186
- Example with Missing Numbers • 175
- Example without Missing Numbers • 175
- Examples • 185
- Examples of Showing In-Depth Outlet Information • 187

F

- file <filename> • 241
- Filling Out the Equipment Setup Worksheet • 16
- FIPS Limitations • 58, 63, 64, 77, 112, 114, 117, 156, 166, 168, 174
- Flexible Cord Installation Instructions • xiv, 198
- Flexible Cord Selection • 199

For Zero U Models Using Tool-less Button Mounting • 9
 Forcing HTTPS Encryption • xiv, 97, 108
 Full Disaster Recovery • 71

G

Gathering Information for LDAP Configuration • 113
 get <id> ... [<id>] • 243
 Get Group Membership Command • 249
 Get Group Power On Delay Command • 250
 Get Power Cycle Delay Command • 252
 Get Power On Delay Command • 247
 Get Receptacle ACL • 251
 Get Receptacle State and Data Command • 248
 Get Receptacle State Command • 247
 getaccess <channel number> [userid] • 240
 getciphers <all | supported> <ipmi | sol> [channel] • 240
 Grouping Outlets Together • 153

H

Home Page • 209
 How to Configure an Alert • 132
 How to Connect Differential Air Pressure Sensors • 30
 How to Disable the Hysteresis • 143

I

Identifying Environmental Sensors • 119
 Identifying Other Dominion PX Devices • 152
 Identifying Sensor Types • 190
 Impact on the Raritan Product Integration • 157, 220, 238
 info [channel number] • 240
 Initial Network and Time Configuration • xiv, 19, 59, 98
 In-Line Monitor Unused Channels • 200
 In-line Monitors • 35, 196
 In-line Monitor's LED Display • 206
 In-line Monitor's Web Interface • 207
 Installation and Configuration • 15
 Installing a Certificate • 111
 Integration • 157, 218
 Introduction • 1
 IPMI in the FIPS Mode • xiv, 157, 253
 IPMI Privilege Levels • 239, 252

K

KX Manager Application • 228

L

LAN Commands • 241
 Layout • 172
 LDAP Configuration Illustration • 117, 259
 LED Display • 33, 206
 Line Details Page • 96
 Line Loads Display • 48
 list • 243
 Logging in to the CLP interface • 181
 Logging in to the Web Interface • 39
 Login • 39

M

MAC Address • 17, 257
 Managing Environmental Sensors • 119, 121
 Managing the Dominion PX • 52
 Manual Mode • 35, 36, 207
 Maximum Ambient Operating Temperature • 16, 211
 Measurement Accuracy • 52
 Menus • xiv, 42, 208
 Models with Cable Glands • 197
 Models with Power Sockets • 197
 Modifying a User Group • 83
 Modifying a User Profile • 78
 Modifying the LAN Interface Settings • 59
 Modifying the Network Service Settings • xiv, 58, 180, 183
 Modifying the Network Settings • 56, 261
 Monitoring Line and Circuit Breaker Status • 93
 Monitoring Unbalanced Loads • 94
 More Information about AD Configuration • 117
 Mounting 1U or 2U Models • 13
 Mounting Zero U Models Using Button Mount • 10
 Mounting Zero U Models Using Claw-Foot Brackets • 12
 Mounting Zero U Models Using L-Brackets • 8

N

Naming and Configuring Outlets • 85, 86, 88, 90
 Naming the Dominion PX Device • 55, 56

Naming the Rack PDU in the KX II or LX (Port Page for Power Strips) • 223
Navigation Path • 44
Network Interface Page • 159
Network Statistics Page • 159

O

OEM Commands • 244
Outlet Grouping • 151
Outlet Permissions • 79
Outlet Sensor Properties • 186
Outlets • 32
Outlets List • 50
Overview • 196

P

Package Contents • 5, 15
Panel Components • 31
Paragon II • 231
Paragon Manager Application • 234
Ping Host Page • 161
Plug Selection • 199
Power Control • 236
Power Cord • 31
Power Cycling an Outlet • 50, 86, 88, 90
Power IQ Configuration • xiv, 220
Preparing the Installation Site • 15
print <channel> • 241
Product Features • xiv, 3
Product Models • 1
Product Photos • 1
PSoC Firmware Upgrade Failure • 47, 70

Q

Querying an Outlet Sensor • 189
Querying the PDU's Serial Number • 194

R

Rackmount Safety Guidelines • 6
Rack-Mounting the PDU • 6
Receptacle Selection • 199
Refresh • 48
Reset Button • 36
Reset to Defaults • 47
Resetting the Administrator Password • 270
Resetting the Button-Type Circuit Breaker • 37
Resetting the Dominion PX Device • 66, 194
Resetting the Handle-Type Circuit Breaker • 37

Resetting the PDU Settings • 269
Resetting to Factory Defaults • 36, 194, 269
Restarting the SNMP Agent after Adding Users • 168
Retrievable Data • 65
Retrieving and Interpreting Sensor Readings • xiv, 176
Retrieving Energy Usage • 173
Role of a DNS Server • 57, 261

S

Safety Guidelines • ii
Safety Instructions • iii, 16
Sample Alerts • 140
Sample Environmental Alert 1 • 141
Sample Environmental Alert 2 • 142
Sample Outlet-Level Alert • 140
Sample Unit-Level Alert • 141
Saving a Device Diagnostics File • 162
Saving a Dominion PX Configuration • xiv, 73
Sensor Commands • 243
Sensor Measurement Accuracy • 127
set <channel> <parameter> • 242
Set Group Membership Command • 246, 249
Set Group Power On Delay Command • 250
Set Group State Command • 248
Set Power Cycle Delay Command • 251
Set Power On Delay Command • 246
Set Receptacle ACL • 250
Set Receptacle State Command • 247
setaccess <channel number>
 <userid>[callin=on|off] [ipmi=on|off]
 [link=on|off] [privilege=level] • 240
Setting Data Retrieval • 65, 173
Setting Outlet Thresholds and Hysteresis • 88, 90, 92
Setting PDU Thresholds and Hysteresis • 38, 90, 91
Setting the Date and Time • 22, 59
Setting the FIPS Mode • xiv, 21, 156
Setting the Global Default Outlet State • 85
Setting the Global Power Cycling Delay • 86, 88
Setting the Outlet Permissions • 79, 82, 84
Setting the Outlet Power-On Sequence • 87
Setting the Sequence Delay • 189
Setting the System Permissions • 78, 79, 80, 84
Setting Up a Digital Certificate • 108
Setting Up and Managing Outlets • 84
Setting Up Event Logging • 144, 169

- Setting Up External User Authentication • xiv, 112
- Setting Up LDAP Authentication • 57, 114, 263
- Setting Up Power Thresholds and Hysteresis • 91, 172
- Setting Up RADIUS Authentication • 117
- Setting Up User Groups • 76, 80
- Setting Up User Login Controls • 104
- Setting Up User Profiles • xiv, 75
- Setting User Permissions Individually • 77, 79
- Setup Preparation • 226
- Showing Environmental Sensor Information • 190
- Showing In-Depth Outlet Information • 186
- Showing Outlet Information • 184
- SNMP and CLP Interfaces • 210
- SNMP Gets and Sets • 171
- SNMP Sets and Configurable Objects • 172
- Specifications • 6, 211
- Specifying the Device Altitude • 61
- Standard Rackmount • 7
- States of Managed Sensors • 128
- Status Messages • 47
- Status Panel • xiv, 45, 158
- Step A. Determine User Accounts and Groups • 259
- Step B. Configure User Groups on the AD Server • 260
- Step by Step Flexible Cord Installation • 201
- Step C. Configure LDAP Authentication on the Dominion PX Device • 261
- Step D. Configure User Groups on the Dominion PX Device • 264
- Successful Messages • 47
- Suggestion for SNMP Trap Configuration • 134, 135, 170
- Switching an Outlet • 188
- Syntax • 184
- System Permissions • 79

T

- Test Actors • 251
- Test Sensors • 251
- The Dominion PX MIB • 171, 174
- Three-Digit Row • 34
- thresh <id> <threshold> <setting> • 243
- Trace Route to Host Page • 161
- Turning an Outlet Off • 189
- Turning an Outlet On • 188
- Turning an Outlet On or Off • 50, 90

- Turning an Outlet On, Off, or Cycling the Power • 50, 90
- Two-Digit Row • 34

U

- Unavailable Options • 47
- Unmanaging Environmental Sensors • 122, 130
- Unpacking the Product and Components • 15
- Unsuccessful Messages • 47
- Updating the Firmware • 67, 74
- Using Online Help • 163
- Using Rack Units for the Z Coordinate Value • 126
- Using SNMP • 65, 69, 77, 150, 165, 210
- Using the CLP Interface • 58, 180, 210
- Using the Help Command • 194
- Using the Home Page • 48
- Using the IPMI Tool Set • 239
- Using the PDU • 31
- Using the Web Interface • 39, 207

V

- Viewing and Controlling Outlet Groups • 154
- Viewing Outlet Details • 89
- Viewing Sensor Readings and States • 127
- Viewing the Local Event Log • 147

W

- Web Interface Elements • 42
- What is Threshold Hysteresis? • 91, 92, 142
- What's New in the Dominion PX User Guide • xiv
- Wiring of 3-Phase In-Line Monitors • 199, 200
- With HyperTerminal • 181, 217, 270
- With SSH or Telnet • 183

Z

- Zero U Products • 5
- Zero U Size • 2

▶ **U.S./Canada/Latin America**

Monday - Friday
8 a.m. - 6 p.m. ET
Phone: 800-724-8090 or 732-764-8886
For CommandCenter NOC: Press 6, then Press 1
For CommandCenter Secure Gateway: Press 6, then Press 2
Fax: 732-764-8887
Email for CommandCenter NOC: tech-ccnoc@raritan.com
Email for all other products: tech@raritan.com

▶ **China**

Beijing

Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +86-10-88091890

Shanghai

Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +86-21-5425-2499

GuangZhou

Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +86-20-8755-5561

▶ **India**

Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +91-124-410-7881

▶ **Japan**

Monday - Friday
9:30 a.m. - 5:30 p.m. local time
Phone: +81-3-3523-5991
Email: support.japan@raritan.com

▶ **Europe**

Europe

Monday - Friday
8:30 a.m. - 5 p.m. GMT+1 CET
Phone: +31-10-2844040
Email: tech.europe@raritan.com

United Kingdom

Monday - Friday
8:30 a.m. to 5 p.m. GMT
Phone +44(0)20-7090-1390

France

Monday - Friday
8:30 a.m. - 5 p.m. GMT+1 CET
Phone: +33-1-47-56-20-39

Germany

Monday - Friday
8:30 a.m. - 5:30 p.m. GMT+1 CET
Phone: +49-20-17-47-98-0
Email: rg-support@raritan.com

▶ **Melbourne, Australia**

Monday - Friday
9:00 a.m. - 6 p.m. local time
Phone: +61-3-9866-6887

▶ **Taiwan**

Monday - Friday
9 a.m. - 6 p.m. GMT -5 Standard -4 Daylight
Phone: +886-2-8919-1333
Email: support.apac@raritan.com