



Dominion PX

User Guide
Release 1.2.5

Copyright © 2008 Raritan, Inc.

DPX-01-E

October 2008

255-80-6080-00

Safety Guidelines

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 2008 Raritan, Inc., CommandCenter®, Dominion®, Paragon® and the Raritan company logo are trademarks or registered trademarks of Raritan, Inc. All rights reserved. Java® is a registered trademark of Sun Microsystems, Inc. Internet Explorer® is a registered trademark of Microsoft Corporation. Netscape® and Netscape Navigator® are registered trademarks of Netscape Communication Corporation. All other trademarks or registered trademarks 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.



To avoid potentially fatal shock hazard and possible damage to Raritan equipment:

SYSTEMS SHOULD BE CONFIGURED ONLY BY A KNOWLEDGEABLE PERSON.

IT IS ESSENTIAL THAT THIS EQUIPMENT IS CONNECTED TO AN ELECTRICAL SUPPLY THAT HAS A PROTECTIVE GROUND CONDUCTOR

WARNING: TO ISOLATE THIS EQUIPMENT DISCONNECT POWER SUPPLY PLUG.

ATTENTION: AFIN D'ISOLER TOTALEMENT CET APPAREIL DEBRANCHER FICHE D'ALIMENTATION.

CAUTION: USE ONLY IN DRY LOCATIONS.

ATTENTION: UTILISER UNIQUEMENT DANS DES EMPLACEMENTS SECS.

Do not use a 2-wire power cord in any product configuration.

Test AC outlets at your computer and monitor for proper polarity and grounding.

Use only with grounded outlets at both the computer and monitor. When using a backup UPS, power the computer, monitor and appliance off the supply.

The installation socket outlet used for the power supply to this equipment must be installed near the equipment and must be easily accessible.

When installing this product, it is essential that the distribution circuit supplying the product is protected by a branch circuit protection device with a maximum rating to suit the product maximum rating.

This power distribution unit is intended for power supply provision to equipment only. Secondary (Satellite) power strips shall not be connected to the receptacles

This product has been designed to conform to the latest safety requirements. In addition to compliance with standards for general use, it has been factory configured for use in rack mounting environments aiding the installer to provide systems compliant with relevant standards.

Provide an earthing connection before the mains plug is connected to the mains. And, when disconnecting the earthing connection, be sure to disconnect after pulling out the mains plug from the mains.

Contents

Safety Guidelines	ii
--------------------------	-----------

Chapter 1 Introduction	1
-------------------------------	----------

Product Models	1
Product Photos	1
Zero U Size	1
1U Size	2
2U Size	2
Product Features	3
Package Contents.....	4
Zero U Products.....	4
1U Products	5
2U Products	5

Chapter 2 Rack-Mounting the Dominion PX	6
--	----------

Rack Mount Safety Guidelines	6
Standard Rack Mounting	6
For Zero U Models Using L-Bracket	9
For Zero U Models Using Tool-less Button Mounting.....	10
Before You Begin Tool-less Mounting:.....	10
To Mount.....	10

Chapter 3 Installation and Configuration	12
---	-----------

Before You Begin.....	12
Unpack the Dominion PX and Components	12
Prepare the Installation Site	12
Fill Out the Equipment Setup Worksheet	12
Connecting the Dominion PX to a Computer.....	13
Connecting the Dominion PX to Your Network.....	14
Configuring the Dominion PX for Network Connectivity	15
Resetting to Factory Defaults	18

Chapter 4 Using the Dominion PX	20
--	-----------

Front Panel	20
Connection Ports	20
Blue LED.....	21

Back Panel.....	21
Power Cord.....	21
Outlets	21
LED Display	22
Circuit Breaker	24
Beeper	24
Measurement Accuracy	25

Chapter 5 Using the Web Interface 26

Logging into the Web Interface.....	26
Log In.....	26
Change Your Password.....	29
Using the Web Interface	30
Menus.....	30
Navigation Path	31
Status Panel	32
Status Messages	34
Unavailable Options	34
Reset to Defaults	35
Refresh	35
Using the Home Window	35
Line Loads Display	36
Circuit Breaker Status.....	36
Outlets List.....	37
All Outlets Control.....	38
Monitoring Line and Circuit Breaker Status	39
Line Details Page	39
Circuit Breaker Details Page	40
Setting Up User Profiles	41
Create a User Profile	41
Copy a User Profile	43
Modify a User Profile	44
Delete a User Profile	44
Set User Permissions Individually	44
Setting Up User Groups.....	45
Create a User Group	46
Set System Permissions.....	46
Set Outlet Permissions	48
Copy a User Group.....	49
Modify a User Group	49
Delete a User Group.....	50
Setting Up Access Controls	50
Force HTTPS Encryption.....	50
Configure the Firewall.....	51
Create Group Based Access Control Rules	54
Set Up User Login Controls.....	57
Setting Up a Digital Certificate.....	60
Create a Certificate Signing Request	61
Install a Certificate	63

Contents

Setting Up External User Authentication	63
Gather Information for LDAP Configuration	64
Setup LDAP Authentication	65
Setting Up RADIUS Authentication	67
Setting Up Outlets and Power Thresholds	68
Set Default Outlet State	69
Set Dominion PX Thresholds	70
Set Outlet Power-Up Sequence	71
Name Outlets	72
Set Outlet Thresholds	73
View Outlet Details	74
Power Cycle an Outlet	75
Turn Outlet On or Off	75
Environmental Sensors	75
Connect Environmental Sensors	76
Map Environmental Sensors	76
Configure Environmental Sensors and Thresholds	79
View Sensor Readings	80
Configuring and Using Alert Notifications	80
Components of an Alert	81
How to Configure an Alert	81
Sample Alerts	89
Setting Up Event Logging	92
Configure Local Event Log	93
View Internal Event Log	95
Configure NFS Logging	96
Configure SMTP Logging	97
Configure SNMP Logging	98
Configure Syslog Forwarding	98
Managing the Dominion PX	99
Displaying Basic Device Information	99
Displaying Model Configuration Information	101
Displaying Connected Users	101
Naming the Dominion PX	102
Modifying the Network Settings	103
Modifying the Communications, Port and Bandwidth Settings	104
Modifying the LAN Interface Settings	105
Setting the Date and Time	106
Configuring the SMTP Settings	107
Configuring the SNMP Settings	108
Enabling Data Retrieval	109
Resetting the Dominion PX	110
Updating the Firmware	112
Copying Configurations with Bulk Configuration	113
Outlet Grouping	116
Identifying Other Dominion PX Units	116
Grouping Outlets Together	117
Viewing and Controlling Outlet Groups	118
Editing or Deleting Outlet Groups	119
Deleting Outlet Group Devices	119

Chapter 6 Integration	121
Dominion KX	122
KX Manager Application (Dominion KX-I only).....	122
Associate Outlets with a Target.....	123
Control a Target's Power	124
Dominion KX-II.....	125
Paragon II	125
Paragon Manager Application	126
Add a Dominion PX Unit in Paragon II	126
Associate Outlets with a Target.....	127
Control a Target's Power	127
Control an Outlet's Power.....	128
Dominion SX	128
Configure a Dominion PX Power Unit on Dominion SX	128
Power Control.....	129
Check Power Strip Status.....	130
Dominion KSX.....	130
CommandCenter Secure Gateway.....	131
Direct Control from CC-SG 4.0.....	131
Appendix A Equipment Setup Worksheet	132
Appendix B Using the CLP Interface	136
About the CLP Interface	136
Logging into the CLP interface	136
With HyperTerminal.....	137
With SSH or Telnet.....	138
Showing Outlet Information	139
Syntax.....	139
Attributes.....	139
Examples.....	140
Turning an Outlet On or Off	140
Syntax.....	141
Querying an Outlet Sensor	141
Appendix C Using SNMP	142
Enabling SNMP.....	142
Configure Users for Encrypted SNMP v3.....	144
Configuring SNMP Traps.....	145
SNMP Gets and Sets.....	146
The Dominion PX MIB	147
Disabling Switching	148

Appendix D Using the IPMI Tool Set 149

Channel Commands	149
authcap <channel number> <max priv>	149
info [channel number]	150
getaccess <channel number> [userid]	150
setaccess <channel number> <userid>[callin=on off] [ipmi=on off] [link=on off] [privilege=level].....	150
getciphers <all supported> <ipmi sol> [channel]	150
Event Commands	150
<predefined event number>	151
file <filename>	151
LAN Commands.....	151
print <channel>	151
set <channel> <parameter>	152
Sensor Commands	153
list	153
get <id> ... [<id>].....	153
thresh <id> <threshold> <setting>.....	154
OEM Commands	154
A Note About Group Commands.....	155
Set Power Set Delay Command.....	155
Get Power On Delay Command.....	155
Set Receptacle State Command	155
Get Receptacle State Command.....	156
Set Group State Command	156
Set Group Membership Command.....	157
Get Group Membership Command	157
Set Group Power On Delay Command	158
Get Group Power On Delay Command.....	158
Set Receptacle ACL	159
Get Receptacle ACL.....	159
Set Sensor Calibration.....	159
Test Actors.....	160
Test Sensors.....	160
Set Power Cycle Delay Command	160
Get Power Cycle Delay Command.....	160

IPMI Privilege Levels 161

Appendix E Event Types **163**

Appendix F Specifications **164**

Environmental Specifications..... 164
Dominion PX Serial RJ-45 Port Pinouts 164
Dominion PX Feature RJ-12 Port Pinouts 164

Index **167**

Chapter 1 Introduction

The Dominion PX unit is an intelligent power distribution unit that allows you to reboot remote servers and other network devices and to monitor power in the data center through Raritan's KVM switches and Secure Console Servers. From the office or from anywhere, the Dominion PX unit will power on, power off, or reboot remote equipment, as well as monitor current, voltage, power, and temperature.

The Dominion PX offers the ability to recover systems remotely in the event of system failure and/or system lockup. It eliminates the need to perform manual intervention or dispatch field personnel, reduces downtime and mean time to repair, and increases productivity.

In This Chapter

Product Models.....	1
Product Photos	1
Product Features	3
Package Contents	4

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.

See <http://www.raritan.com> or your local reseller for a list of available models.

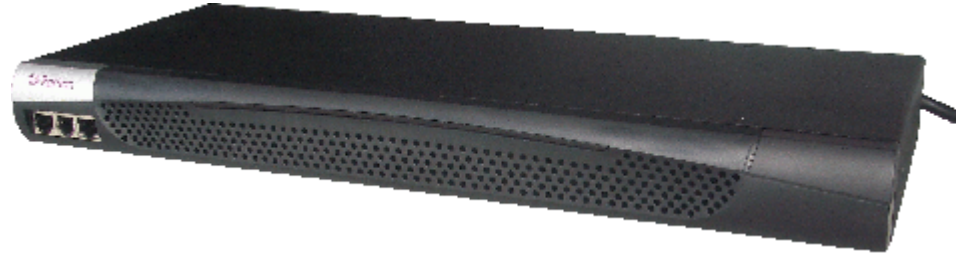
Product Photos

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

Zero U Size



1U Size



2U Size



Product Features

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

- The ability to control outlets collectively and individually
- The ability to power on, power off, and reboot the devices connected to each outlet
- The ability to group outlets from multiple Dominion PX 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

- The ability to monitor the internal CPU temperature of the Dominion PX
- The ability to monitor environmental factors such as external temperature and humidity
- An audible alarm (beeper) and a visual alarm (blinking LED) to indicate current overload
- Configurable alarm thresholds
- Support for SNMP v1, v2, and V3
- The ability to send traps using SNMP protocol
- The ability to retrieve outlet specific data using SNMP, including outlet state, current, voltage, and power
- The ability to retrieve a history of sampled data at all levels (unit, circuit breaker, outlet, etc) via SNMP
- The ability to configure and set values through SNMP, including unit and outlet threshold levels
- The ability to save one unit's configuration settings and then deploy those settings to other Dominion PX units
- Fully shrouded local branch circuit breakers on products rated over 20A to protect connected equipment against overload and short circuits
- Integration with Raritan's Paragon II, CommandCenter Secure Gateway (CC-SG), and Dominion access devices
- Line current and circuit breaker monitoring
- A combination of outlet types (e.g., C13 + C19) in select models

Select models may be available without switching. Please check with your reseller or distributor.

Package Contents

The following describes the equipment and other material included in each product package.

Zero U Products

- Dominion PX unit including power cord
- Bracket for Zero U and screws
- Tool-less mounting bracket for Zero U units
- Null-modem cable with RJ-45 and DB9F connectors on either end

1U Products

- Dominion PX unit including power cord
- 1U bracket pack and screws
- Null-modem cable with RJ-45 and DB9F connectors on either end

2U Products

- Dominion PX unit including power cord
- 2U bracket pack and screws
- Null-modem cable with RJ-45 and DB9F connectors on either end

Chapter 2 Rack-Mounting the Dominion PX

In This Chapter

Rack Mount Safety Guidelines	6
Standard Rack Mounting	6
For Zero U Models Using L-Bracket.....	9
For Zero U Models Using Tool-less Button Mounting	10

Rack Mount 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 appliances (see Appendix A: Specifications).

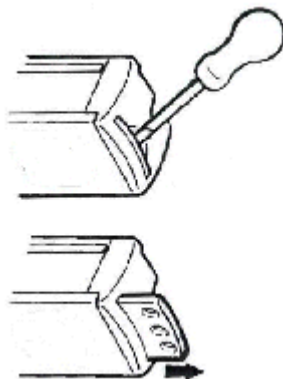
Ensure sufficient airflow through the rack environment.

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.

Standard Rack Mounting

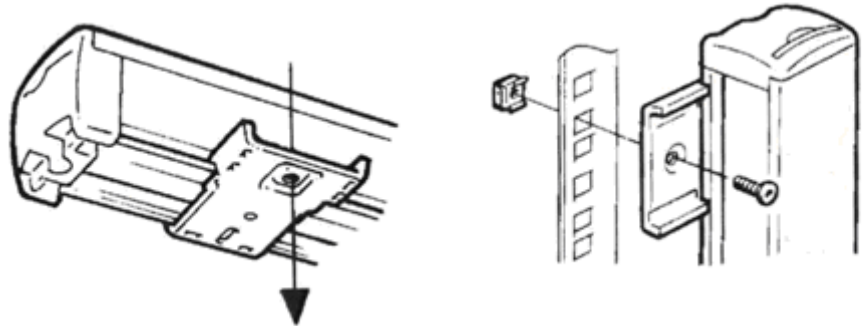


The Zero U units are provided with high grade engineering polycarbonate isolation hardware to allow fixing in a variety of positions within the rack.

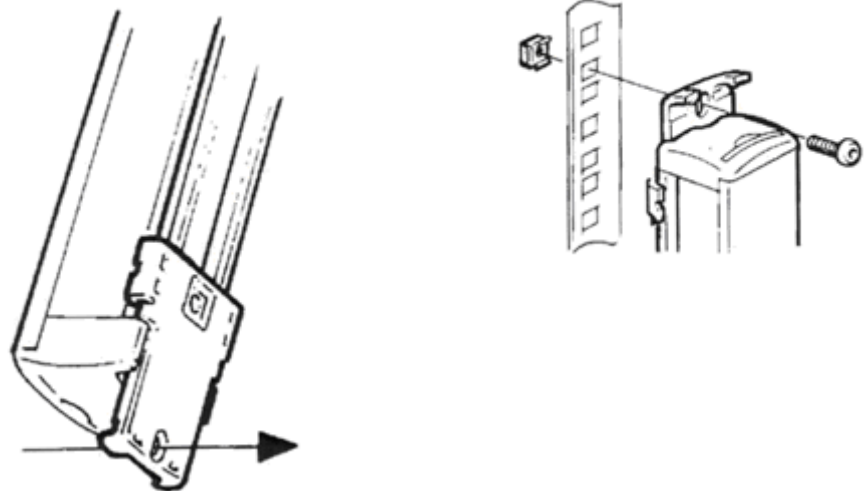
For panel/flush mount, pull out fixing brackets are available on each end cap to allow mounting on suitable rails.

See other options shown below.

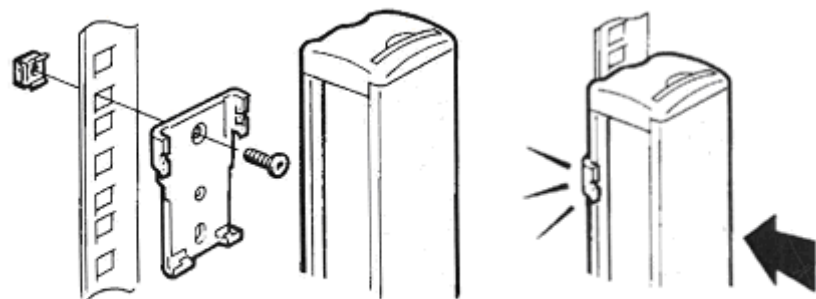
Side Fixing

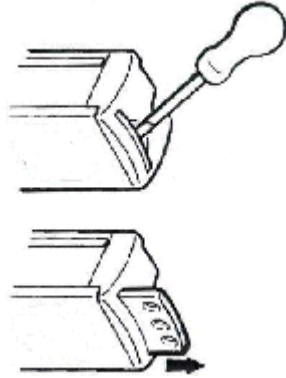


End Fixing

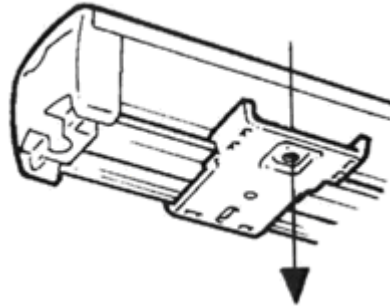


Blind Fixing





Side Fixing

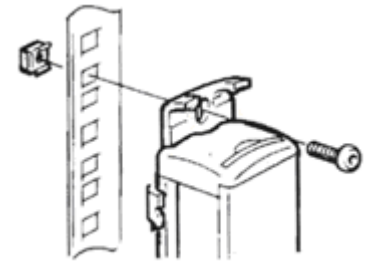
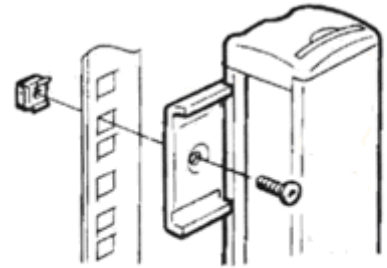


End Fixing

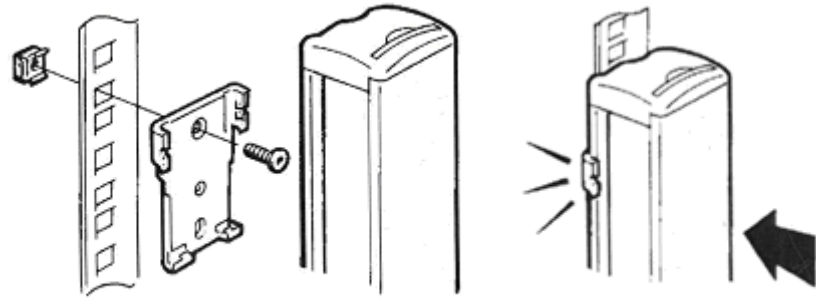
The Zero U units are provided with high grade engineering polycarbonate isolation hardware to allow fixing in a variety of positions within the rack.

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

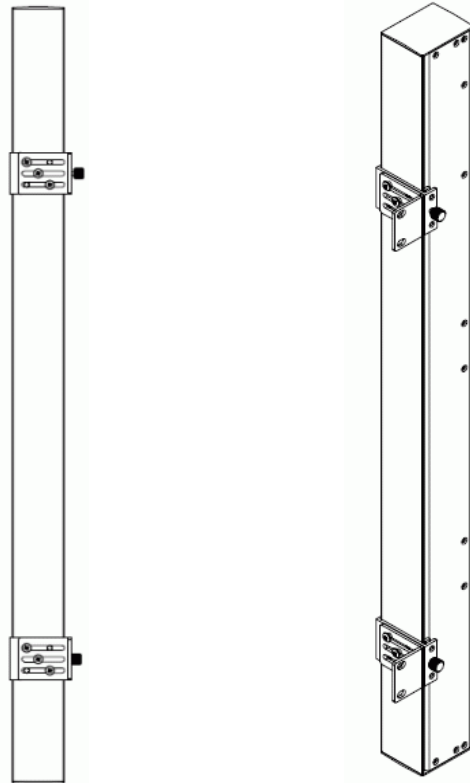
See other options shown below.



Blind Fixing



For Zero U Models Using L-Bracket



1. Align the base-plates on the back of the Dominion PX unit and tighten the thumb screws to secure them in place.
2. Unscrew the large buttons in the center of the base plates.
3. Align the L-Brackets with the base plates so that the five screw-holes line up through the L-Bracket's slots. The rack-mount side of the plates should face either the left or right side of the Dominion PX.
4. Fasten the L-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 to the rack through the L-Brackets.

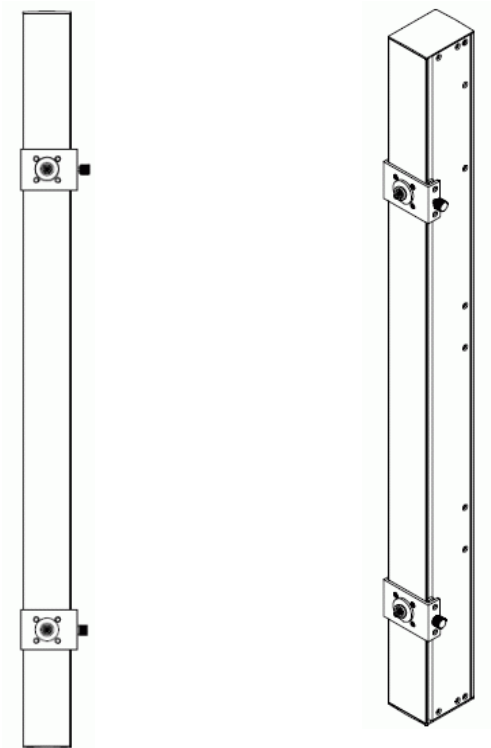
For Zero U Models Using Tool-less Button Mounting

The Zero U units ship with tool-less mounting brackets consisting of an adjustable base-plate with a large button on one side. These work by attaching to the back side of a Zero U Dominion PX (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 in this way.

Before You Begin Tool-less Mounting:

- Ensure that you have sufficient space in the cabinet to mount the Dominion PX. Approximately one inch of clearance is required at each end (top and bottom) of the unit.
- It may help to mark the back of the Dominion PX 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.

To Mount



1. Slide the baseplates onto the rear of the Dominion PX unit. Leave at least 24 inches between the buttons for stability, and turn the thumbscrews until the plate grasps the Dominion PX lightly.
2. Align the large mounting buttons the mounting holes in the cabinet, fixing one in place and adjusting the other.
3. Tighten the thumbscrews on both baseplates to secure the mounting buttons in their position.
4. Ensure that both buttons can engage their mounting holes simultaneously.
5. Press the Dominion PX forward, pushing the mounting buttons through the mounting holes, then letting the Dominion PX drop about 5/8". This will secure the Dominion PX in place and complete the installation.

Tool-less mounting buttons attach to the rear of the Dominion PX Zero-U unit. Fix the bottom button in place then adjust the other to align with the mounting holes.

Chapter 3 Installation and Configuration

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

In This Chapter

Before You Begin	12
Connecting the Dominion PX to a Computer	13
Connecting the Dominion PX to Your Network	14
Configuring the Dominion PX for Network Connectivity	15
Resetting to Factory Defaults	18

Before You Begin

Before beginning the installation, perform the following activities:

Unpack the Dominion PX and Components

1. Remove the Dominion PX unit and other equipment from the box in which they were shipped. See Package Contents for a complete list of the contents of the box.
2. Compare the unit and 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.

Prepare the Installation Site

1. Make sure the installation area is clean and free of extreme temperatures and humidity.
2. Allow sufficient space around the Dominion PX for cabling and outlet connections.
3. Review the Safety Instructions listed in the beginning of this user guide.

Fill Out the Equipment Setup Worksheet

An Equipment Setup Worksheet is provided in **Appendix B** (see "Equipment Setup Worksheet" on page 132). Use this worksheet to record the model, serial number, and use of each device connected to the Dominion PX.

As you add and remove devices, keep the worksheet up to date.

Connecting the Dominion PX to a Computer

You must connect the Dominion PX to a computer to configure it, using a serial connection between the Dominion PX and the computer. If you plan to use this connection to log into the CLP command line interface, leave the cable connected after the configuration is complete.

The computer must have a communications program such as HyperTerminal or PuTTY. You will need the null-modem cable and connectors that were shipped with the Dominion PX.

1. Take the null-modem cable and connect the end with the RJ-45 connector to the port labeled Serial on the front of the Dominion PX. See the pictures for the location of this port on your Dominion PX.





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

2. Plug the other end of the null-modem cable with the DB9 connector into the serial port (COM) of the computer.

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).

1. Take a standard Category 5e UTP cable and connect one end to the LAN port on the front of the Dominion PX. See **Connecting the Dominion PX to a Computer** (on page 13) for the location of this port on your size Dominion PX.
2. Connect the other end of the cable to your LAN.

Configuring the Dominion PX for Network Connectivity

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

1. Go to the computer that you connected to the Dominion PX and open a communications program such as HyperTerminal or PuTTY. Make sure its 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.

2. Point the communications program at the serial port connecting the Dominion PX, and open a terminal window.
3. Press the Enter key 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
192.168.0.192 command:

```

4. Type config and press Enter to begin the configuration process. You are prompted to select an IP configuration method.

```

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
192.168.0.192 command: config
IP autoconfiguration (none/dhcp/bootp) [none]:

```

5. You must assign the Dominion PX an IP address. There are two ways to do this:
 - Auto configuration - Select an autoconfiguration 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 Dominion PX 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 IP address is 192.168.0.192. The default IP configuration method is DHCP, and the default IP address will be replaced by the address assigned by DHCP or BOOTP, or the static IP address you entered, as soon as 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. The default IP address for static (none) configuration is 192.168.0.192.*

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
192.168.0.192 command: config
IP autoconfiguration (none/dhcp/bootp) [none]: dhcp
Enable IP Access Control (yes/no) [no]: _
```

6. By default, IP access control is NOT enabled. This disables the Dominion PX firewall. Leave the firewall disabled for the present; later you will enable the firewall from the Web interface and create firewall rules. See **Configure the Firewall** (on page 51).

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.

7. 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
192.168.0.192 command: config
IP autoconfiguration (none/dhcp/bootp) [none]: dhcp
Enable IP Access Control (yes/no) [no]: no
LAN interface speed (auto/10/100) [auto]:
```

8. 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
192.168.0.192 command: config
IP autoconfiguration (none/dhcp/bootp) [none]: 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]:

```

9. 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, 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. You are prompted to confirm the information you just entered.

```

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
192.168.0.192 command: config
IP autoconfiguration (none/dhcp/bootp) [none]: 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]:
Are the entered values correct? Enter y for Yes, n for No or c to Cancel _

```

10. All the configuration parameters have now 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 completes the configuration and displays a message when the configuration is done.
 - If one or more parameters are not correct, type n and press Enter. You are returned to the IP configuration prompt as shown in the screenshot of Step 4, and given the opportunity to correct each piece of information. When the information is correct, type y and press Enter to complete the configuration and return to the opening prompt.

- If you want to terminate the configuration process, type `c` and press Enter. The configuration is cancelled and you are returned to the opening prompt.
11. If you entered `y` to confirm the configuration, a message appears when the configuration is complete. You will be returned to the opening prompt. You are now ready to begin using your Dominion PX.

```
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
192.168.0.192 command: config
IP autoconfiguration (none/dhcp/bootp) [none]: 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]:
Are the entered values correct? Enter y for Yes, n for No or c to Cancel y

Configuring device ...
Done.
```

Note: The IP address configured takes about 15 seconds to take effect for the device connected via serial line, or even longer if configured over DHCP.

Resetting to Factory Defaults

Important: Exercise caution before resetting a DPX to its factory defaults. This wipes out any information you have entered, including user profiles, user groups, thresholds, alert policies, and so on.

For security reasons, the Dominion PX may be reset only to factory defaults at the local serial console. To do this:

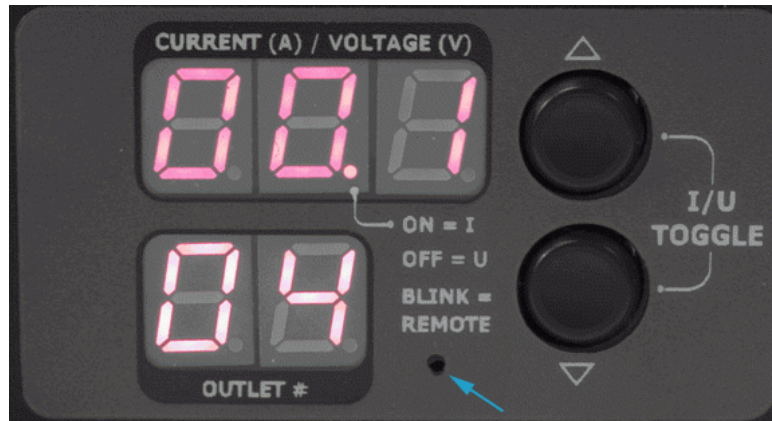
1. Connect a computer to the serial port of the Dominion PX.
2. Using a terminal emulation program such as HyperTerminal, Kermit, or PuTTY (at a speed of 9600 bps), open a window on the DPX. Make sure serial port settings are configured as followed:
 - Baud rate (bits per second) = 9600
 - Data bits = 8
 - Stop bits = 1
 - Parity = None
 - Flow control = None
1. Press (and release) the Reset button of DPX while pressing the Esc key several times in rapid succession. A prompt (`=>`) should appear after about one second.

- Execute the defaults command to reset the DPX to its factory defaults.

Note: Type "help" to show a list of available commands and a short description of each one.

HyperTerminal is available on many Windows OS. But HyperTerminal is not available on Windows Vista. PuTTY is a free program you can download from the internet. See PuTTY's documentation for details on configuration.

The pictures show the location of the reset hole.



Chapter 4 Using the Dominion PX

This chapter explains how to use the Dominion PX unit. It describes the LEDs and ports on the front and back panels of the Dominion PX, and explains how to use the display panel. It also explains how the circuit breaker works and when the beeper sounds.

In This Chapter

Front Panel	20
Back Panel	21
Circuit Breaker	24
Beeper	24
Measurement Accuracy	25

Front Panel

The front panel of the 1U and 2U Dominion PX units features a blue LED to the right and three connection ports to the left, while the front panel of the Zero U model features power outlets to connect devices to Dominion PX, a display panel, and three connection ports.

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: Take the null-modem cable that was shipped with the Dominion PX unit, connect the end with the RJ-45 connector to the port labeled Serial on the front of the Dominion PX, and connect the end with the DB9F connector to the serial (COM) port on the computer. 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.
Feature	For use with Raritan provided environmental sensors.
LAN	Connecting the Dominion PX to your company's network: Connect a standard Category 5e UTP cable to this port and connect the other end to your network. This connection is necessary to administer the Dominion PX remotely using the Web interface. There are two small LEDs under the LAN port. Green indicates a physical link and activity, and yellow indicates communication at 10/100 BaseT speeds.

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

Blue LED

Only 1U and 2U models have a blue LED on the front panel. The blue LED on the right side of the front panel is lit solid as soon as the Dominion PX unit is plugged in.

Back Panel

The back panel of the 1U and 2U Dominion PX units consists of, from left to right, a power cord, power outlets to connect devices to the Dominion PX, and a display panel; the Zero U models do not have a back panel.

Power Cord

The power cord that connects the Dominion PX to a power source is located on the far left of the back panel or on the end of the unit if the unit is a Zero U type. No devices can be rewired by the user.

Note: Each Dominion PX model should be plugged into an appropriately rated outlet for its type.

There is no power switch on the Dominion PX. On products rated at over 20A there are branch circuit breakers that are fully shrouded to prevent accidental operation. To power cycle the unit, remove the power cord from the power source and then re-connect it.

Outlets

The number of outlets on the back panel depends upon the Dominion PX model. To the upper left of each outlet is a small LED. The units are shipped from the factory with all outlets powered ON. The table below explains how to interpret the different LED states.

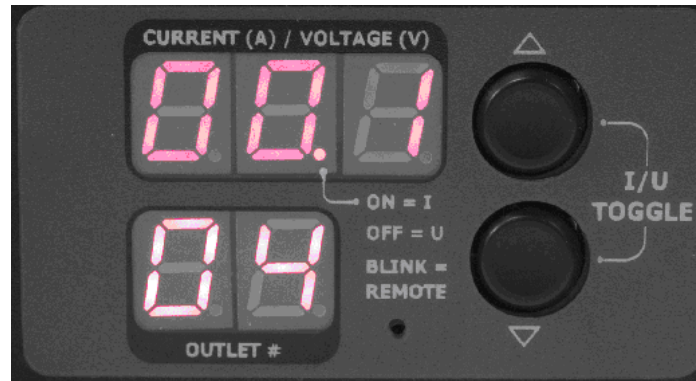
LED State	Outlet Status	What it Means
Not lit (Light grey)	Unit OFF	The outlet is not connected to power or the control circuitry's power supply is broken.
Red	ON and LIVE	The outlet is ON (relay closed) and LIVE (voltage present).
Red flashing	ON and LIVE	The outlet is ON and LIVE, but there is overload and the current has crossed the non-critical threshold.
Green	OFF and LIVE	The outlet is OFF (relay open) and LIVE.

LED State	Outlet Status	What it Means
Green flashing	OFF and NOT LIVE	The outlet is OFF and Circuit Breaker is OFF
Yellow flashing	ON and NOT LIVE	The outlet is ON but NOT LIVE (circuit breaker open or other high voltage rail error).
Cycling through Red, Green and Yellow	n/a	The Dominion PX has just been plugged in and its management software is loading. OR A firmware upgrade is being performed on the unit

Note: When a Dominion PX unit is powered on, the power-on self-test and software loading takes a few moments. As the unit boots up, the outlet LEDs cycle through red, green and yellow. When the software has completed loading, the outlet LEDs display a steady color and the meter illuminates.

LED Display

The LED display is located adjacent to the outlets on the Zero U model, and on the back right of the 1U and 2U models. The following picture shows the LED display.



The LED display consists of:

- An upper row displaying three digits
- A lower row displaying two digits
- Up and Down buttons

*Note: The small hole between the lower row and the Down button is the reset hole. The Dominion PX unit can be reset to its factory default values using this hole when connected to the serial port. See **Resetting to Factory Defaults** (on page 18) for details. Pressing this Reset hole will **ONLY** restart the unit.*

Lower Row

The lower row shows the outlet number.

Upper Row

The upper row shows the current, voltage, and power readings for the outlet indicated in the lower row. During the firmware upgrade process, the upper row displays “FuP” to indicate that a Firmware Upgrade is being performed on the unit.

► To Operate the LED Display:

1. Use the Up and Down buttons to select an outlet. Pressing the Up button moves up one outlet number. Pressing the Down button moves down one outlet number.
2. When an outlet is selected, the outlet number appears in the lower row and the current in the upper row. Current is displayed in the format: XX.X (A)
3. To display the voltage for the selected outlet, press the Up and Down buttons simultaneously. The voltage reading will replace the current for about five seconds, after which the current will re-appear.
4. To display the active power for the selected outlet, first press the Up and Down button simultaneously to display the voltage, and then again to display the active power. Active Power appears in the format: X.XX in volt-amps (VA).

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, current has a decimal point between the first and second digits, and power has a decimal point between the second and third digits.

You can view current and voltage for the entire Dominion PX unit using the Up and Down buttons to select outlet number 00. If left alone, the display will cycle through the current for each outlet.

Circuit Breaker

The Dominion PX includes branch circuit breakers that automatically trip when a power overload is detected. The Dominion PX uses circuit breakers with Type C Trip Characteristic. If the circuit breaker switches off the voltage rail, the lower row of the display panel will jump to the lowest outlet number affected by the circuit breaker error, and the upper row will display these three letters, which mean circuit breaker error:

CbE

Note: Dominion PX models that are embedded with circuit breakers are those units rated over 20 Amp, including DPCS12-30L, DPCS20-30L, DPCS20A-32, DPCS20A-30L6, DPCR20-30L, and DPCR20A-32.

You will still be able to switch between outlets on the Dominion PX's display panel. Outlets affected by the error will show CbE. Unaffected outlets will show the current and voltage readings as described above.

To reset the breakers in the event of an overload:

- On the 1U and 2U products unclip, the front molding to access the breaker(s).
- On the Zero U product, access the breaker(s) by lifting the hinged cover over the breaker element.

Beeper

The Dominion PX includes a beeper. It will ring if any of the circuit breakers is tripped or if the control board temperature sensor exceeds 80 degrees Celsius (or 176 degrees Fahrenheit).

The beeper will cease ringing when the broken circuit breaker conditions disappear or the control board temperature sensor drops below 70 degrees Celsius (or 158 degrees Fahrenheit).

The temperature thresholds are factory defaults and can be user-configurable.

It takes a maximum of three seconds for the beeper to start ringing right after the circuit breaker is tripped.

Measurement Accuracy

- Voltage (per outlet): Range 0-255V, +/-5%, 3 digits, resolution 1V
- Current (per outlet): Range 0-25A, +/-5%, 3 digits, resolution 0.1A

Chapter 5 Using the Web Interface

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

In This Chapter

Logging into the Web Interface	26
Using the Web Interface	30
Using the Home Window	35
Monitoring Line and Circuit Breaker Status.....	39
Setting Up User Profiles	41
Setting Up User Groups	45
Setting Up Access Controls.....	50
Setting Up a Digital Certificate.....	60
Setting Up External User Authentication	63
Setting Up Outlets and Power Thresholds	68
Environmental Sensors	75
Configuring and Using Alert Notifications.....	80
Setting Up Event Logging.....	92
Managing the Dominion PX.....	99
Outlet Grouping	116

Logging into the Web Interface

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

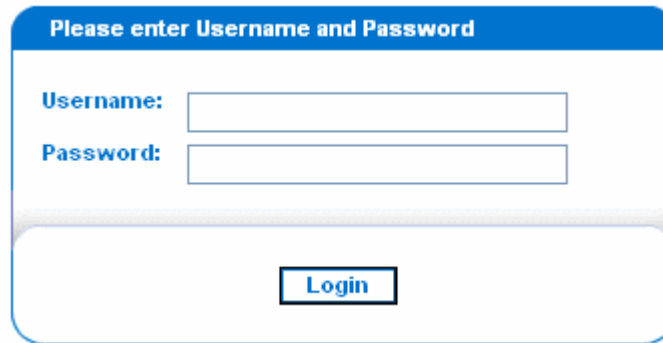
Once you have logged in, you can create user profiles for your other users. These profiles define their login names and passwords. (See **Creating a User Profile** (see "Create a User Profile" on page 41) for instructions on creating a user profile.)

Log In

► **To log into the Web interface:**

1. Open a browser such as Microsoft Internet Explorer or Mozilla Firefox and point it at this URL:
`https://<ip address>`

where <ip address> is the IP address of the Dominion PX. A Login dialog appears.

A login dialog box with a blue header bar containing the text "Please enter Username and Password". Below the header, there are two input fields: "Username:" followed by a text box, and "Password:" followed by a text box. At the bottom center of the dialog is a button labeled "Login".

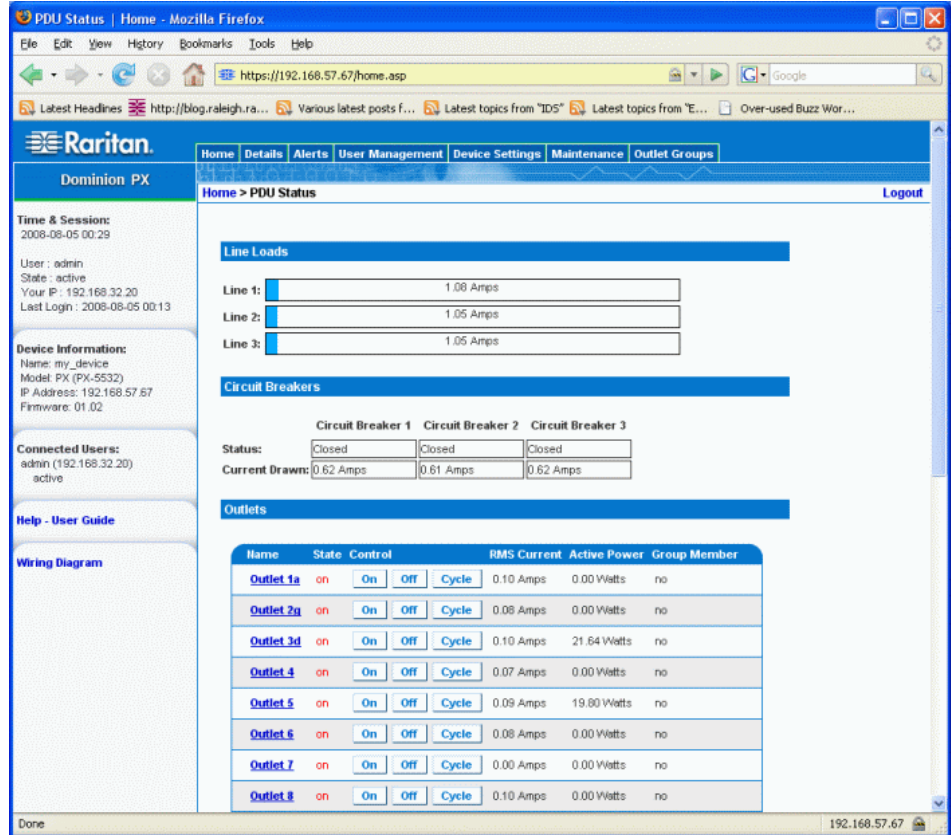
Please enter Username and Password

Username:

Password:

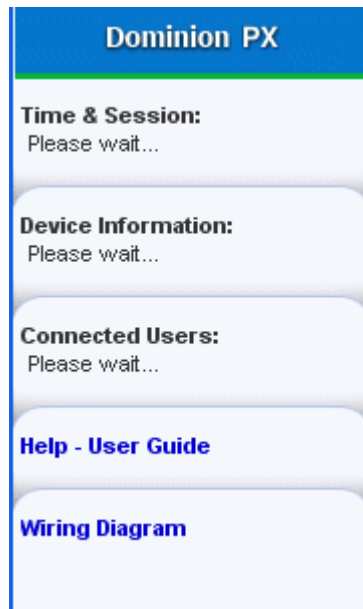
Login

2. Type your user name and password in the Username and Password fields. Both the user name and password are case sensitive, so make sure you capitalize the letters correctly.
3. Click Login. The Home window opens.



Note: The Home window shown above shows 20 outlets. If your Dominion PX has eight outlets, the Home window will show eight. Elements may appear differently, depending on model type and setup.

Java script must be enabled 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 will not display correctly.



Change Your Password

► **To change your password:**

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

The image shows a "Change Password" web form. It has a blue header with the text "Change Password". Below the header are three text input fields, each with a label above it: "Old Password", "New Password", and "Confirm New Password". At the bottom of the form is a blue button labeled "Apply".

2. Type your existing 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.

Using the Web Interface

Every window 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 options:

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
- Environmental Sensors
- Network
- Security
- Certificate
- Date / Time
- Authentication
- SMTP Settings

SNMP Settings

Event Log

Maintenance

Device Information

View Event Log

Update Firmware

Unit Reset

Outlet Groups

Outlet Group Details

Outlet Group Devices

Outlet Group Editor

► To select an option:

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

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

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

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

Navigation Path

When you select an option from a menu and navigate to a specific window, the system displays a navigation path across the top that shows the menu and option 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 window, click the window name in the navigation path. Every navigation path begins at the Home window, so a single click always takes you back to the Home window from anywhere in the interface. You can click the Home tab from any page to take you back to the Home window.

Status Panel

The Status panel appears on the left of every window 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, including:
 - Model name and number
 - IP address
 - Firmware version

- Information about all the users currently connected, including user name, IP address, and present state. Your active session is included in this list.
- A link to the User Guide on the Raritan Website.
- A link to wiring diagrams for select Dominion PX models.

Dominion PX

Time & Session:
2008-10-14 11:38

User : admin
State : active
Your IP : 192.168.43.181
Last Login : 2008-10-14 11:31

Device Information:
Name: Rack3_EM
Model: PX (DPCR8-15)
IP Address: 192.168.43.159
Firmware: 01.02.05

Connected Users:
admin (192.168.43.181)
active

[Help - User Guide](#)

[Wiring Diagram](#)

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 will be logged out and re-directed to the main login window automatically.

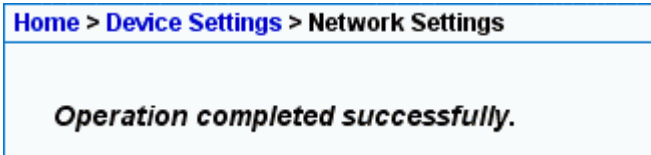
Important: Users still appear in the Connected Users list if they end their session by closing their browser window without logging off. Dominion PX will remove their names when their sessions reach the idle time limit.

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 window indicating whether or not the operation was successful. Be sure to check this message to confirm that an operation was successful.

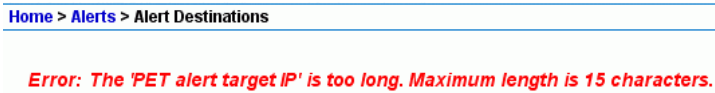
Successful messages

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



Unsuccessful messages

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



Unavailable Options

Sometimes certain actions will be unavailable. When this occurs, the appropriate buttons will be 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 will be grayed-out since you cannot Copy, Modify, or Delete the Admin user group. In Firefox, however, these buttons will appear normal, but be unclickable.

Reset to Defaults

Many windows 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, the next time you return to the window, you will still see 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 windows provide a Refresh button. If a window is open for a while, the information displayed may become "stale." Click this button periodically to reload the window and update the information displayed.

Using the Home Window

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

You can return to the Home window from any other window 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 will also change colors as the load crosses configured thresholds.

For more information on the status of each line, click the Details tab, then select Line Detail.

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 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, click the Details tab, then select CB Detail.

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

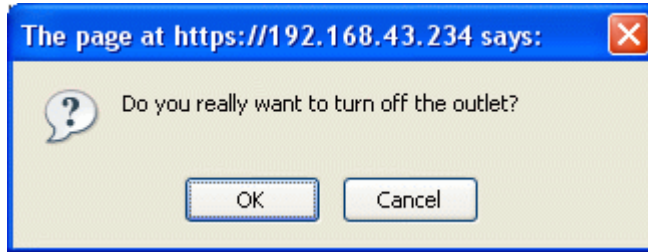
Outlets List

The Outlets List displays each outlet on the Dominion PX 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	2.66 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

Turn an Outlet On, Off, or Cycle the Power

To turn an outlet ON, OFF, or cycle the power to it, click the On, Off, or Cycle in the outlet row. You will be asked to confirm your action, click OK and the outlet will then switch ON, OFF, or will cycle its power. You can also turn an outlet on or off from the Outlet Details window.



Display Additional Details

To display additional details about an outlet, click the outlet name. This displays the Outlet Details window. This window gives the name and status of the outlet, as well as:

- RMS Current
- Power Factor
- Maximum RMS Current
- Voltage
- Active Power
- Apparent Power

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 comparable DC value.

All Outlets Control

The All Outlets Control panel at the bottom of the Home Window allows you to turn all outlets ON and OFF. Click On to turn all outlets ON, click Off to turn all outlets OFF. As with individual outlets, you must confirm the selection before it takes effect.

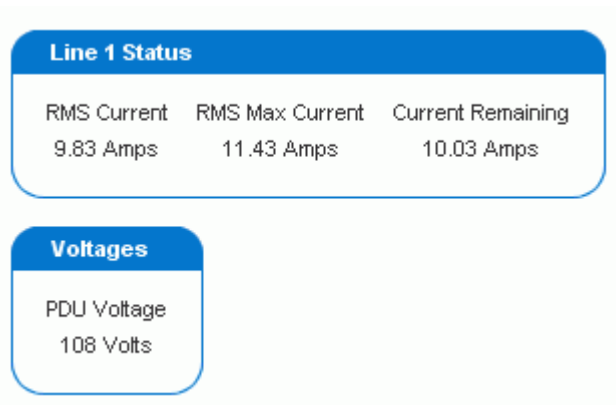


Note: Users must have permission to access all outlets in order to use All Outlets Control.

Monitoring Line and Circuit Breaker Status

Dominion PX provides detail pages for additional information on Line and Circuit Breaker status.

Line Details Page



To open the Line Details Page, choose Details > Line Details. The page opens and displays for each line the present current draw, the largest amount of current drawn since the Dominion PX'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, click the Details tab, then select CB Details.

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 last booted, and the amount of available current that the circuit breaker can handle.

Setting Up User Profiles

The Dominion PX is shipped with one built-in user profile: the admin profile, which is used for the original login. 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. The profile 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 at the same time using the login name from the same profile. You can change this so only one user at a time can use a specific login. This is done by choosing Device Settings > Security and selecting the Enable Single Login Limitation checkbox.

Create a User Profile

► **To create a user profile:**

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

User Management

Existing Users
 --- select ---

New User Name

Full Name

Password

Confirm Password

Use Password as Encryption Phrase ^{*}

SNMP v3 Encryption Phrase

Confirm SNMP v3 Encryption Phrase

Email Address

Mobile Number

User Group
 --- select ---

Enforce user to change password on next login ^{*}

Note: Before entering any information in the user profile, make sure the User Group is created and available for selection.

- 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 will enter to log into the Web interface.
Full Name	The user's first and last names.
Password Confirm Password	<p>The password the user will enter to log in. Type it first in the Password field and then again in the Confirm Password field.</p> <p>The password must be at least four characters long, and spaces are not permitted. The maximum password length is 32 characters.</p> <p>The password is case sensitive, so be sure to capitalize the same letters each time.</p>
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.
4. If you select None, the user is not assigned to a User Group. This means you have to set the user's permissions individually. Until you do this, the user is blocked from accessing any system functions and outlets. (See **Setting User Permissions Individually** (see "Set User Permissions Individually" on page 44).)
5. 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 one of his or her choice.
6. Click Create. The user profile is created.

Note: The Use Password as Encryption Phrase, SNMP v3 Encryption Phrase and Confirm SNMP Encryption Phrase apply only when using secure SNMP v3 communication. See the Using SNMP appendix for more details.

Copy a User Profile

You can create a new user profile with the same settings as an existing profile using the copy function. You can 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 window 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.

Modify a User Profile

Users with User/Group Management permissions can modify user profiles (see **Setting the System Permissions** (see "Set System Permissions" on page 46) for details on setting user permissions).

▶ **To modify a user profile:**

1. Choose User Management > Users & Groups. The User/Group Management window 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.
4. Click Modify. The user profile is modified.

Delete a User Profile

▶ **To delete a user profile:**

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

Set 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

▶ **To set the system permissions:**

1. Choose User Management > User/Group System Permissions. The User/Group System Permissions window opens (see **Setting the System Permissions** (see "Set System Permissions" on page 46)).
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

► **To set the outlet permissions:**

1. Choose User Management > User/Group Outlet Permissions. The User/Group Outlet Permissions window opens (see **Setting the Outlet Permissions** (see "Set Outlet Permissions" on page 48)).
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 affect on outlet permissions.

Setting Up User Groups

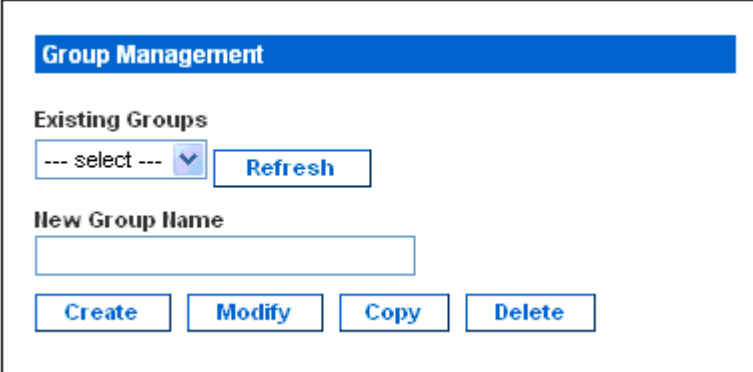
The Dominion PX is shipped with one User Group built in: the Admin User Group. This User Group provides full system and outlet permissions. It can be neither modified nor deleted.

When creating user profiles, the User Group field defaults to the Admin User Group. This means that if you do not change the entry in this field, the user will have full system and outlet permissions. To restrict the user's permissions, create a User Group with limited system and/or outlet permissions, and assign the user to that group.

Create a User Group

► **To create a User Group:**

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



The screenshot shows a web interface titled "Group Management". It features a blue header bar with the text "Group Management". Below the header, there is a section labeled "Existing Groups" which contains a dropdown menu with the text "--- select ---" and a "Refresh" button. Underneath, there is a section labeled "New Group Name" with an empty text input field. At the bottom of the panel, there are four buttons: "Create", "Modify", "Copy", and "Delete".

2. In the Group Management panel, type the name of the group in the New Group Name field.
3. Click Create. The User Group is created.

Set 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 > Users/Group System Permissions. The User/Group System Permissions window opens.

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 :	No ▼
Date/Time Settings :	Yes ▼
Environmental Sensor Configuration :	Yes ▼
Firmware Update :	Yes ▼
IPMI Privilege Level :	Operator ▼
Line & Circuit Breaker Configuration :	Yes ▼
Log Settings :	Yes ▼
Log View :	Yes ▼
Network Settings :	Yes ▼
Outlet Group Configuration :	No ▼
SNMP Settings :	No ▼
SNMP v3 Access :	Deny ▼
SSH/Telnet Access :	Yes ▼
SSL Certificate Management :	No ▼
Security Settings :	No ▼
Server Status via IPMI :	Yes ▼
Unit & Outlet Configuration :	No ▼
Unit Reset :	No ▼
User/Group Management :	Yes ▼
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 window 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 permission for the effects to apply. Check the individual task descriptions in this guide for details.

Set 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 > Users/Group Outlet Permissions. The User/Group Outlet Permissions window opens.

	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 field on this window is used to set individual user permissions. If you are setting group permissions, you may ignore this field.

Copy a User Group

You can create a new User Group with the same permissions as an existing User Group using the copy function. You can 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.

► To copy a User Group:

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

Modify a User Group

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

► To modify a User Group name:

1. Choose User Management > Users & Groups. The User/Group Management window 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.
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 described above and make any necessary changes.

Delete a User Group

► **To delete a User Group:**

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

Setting Up Access Controls

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

Force HTTPS Encryption

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

► **To require users to use HTTPS instead of HTTP when accessing the Dominion PX through the Web interface:**

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



2. Select the Force HTTPS for web access checkbox.
3. Click Apply. HTTPS is now required for browser access.

Note: Attempts using HTTP will be redirected back to HTTPS automatically only if the Force HTTPS for web access checkbox is selected.

Configure the Firewall

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

To configure the firewall, you must first enable the firewall, then set the default policy and create rules specifying which addresses to accept and which addresses to drop. Changes made to firewall rules take effect immediately. Any unauthorized IP activities will cease instantly.

*Note: The purpose of disabling the firewall by default is to prevent users from accidentally locking themselves out of the unit. See **Installation and Configuration** (on page 12).*

Enable the Firewall

► To enable the Dominion PX firewall:

1. Choose Device Settings > Security. The Security Settings window opens. The panel at the upper right is labeled IP Access Control.

IP Access Control

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

Enable IP Access Control *

Default policy

ACCEPT ▾ *

Rule #	IP/Mask	Policy
		ACCEPT ▾

2. Select the Enable IP Access Control checkbox. This enables the firewall.
3. Click Apply. The firewall is enabled.

Change the Default Policy

Once enabled, the firewall has a built-in default policy that accepts traffic from all IP addresses. This means that any IP addresses not dropped by a specific rule will be permitted to access the Dominion PX. You can change the default policy to DROP, in which case traffic from all IP addresses will be dropped except traffic allowed by a specific ACCEPT rule.

► To change the default policy:

1. Choose Device Settings > Security. The Security Settings window opens. The panel at the upper right is labeled IP Access Control.
2. Make sure the Enable IP Access Control checkbox is selected.
3. The default policy is shown in the Default Policy field. To change it, select the policy you want from the drop-down list in the field.
4. Click Apply. The new default policy is applied.

Create Firewall Rules

Firewall rules accept or drop traffic intended for the Dominion PX, based on the IP address of the host sending the traffic. When creating firewall rules, keep the following in mind:

- Rule order - The order of the rules is important. When traffic reaches the Dominion PX, the rules are executed in numerical order. The first rule that matches the IP address determines whether the traffic is accepted or dropped. Any subsequent rules matching the IP address have no effect on the traffic.
- Subnet mask - 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.

► To create firewall rules:

1. Choose Device Settings > Security. The Security Settings window opens. The panel at the upper right is labeled IP Access Control.
2. Make sure the Enable IP Access Control checkbox is selected.

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 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 #5 and #6, type 6. 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 rennumbers the 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 v *

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

ACCEPT v

Append
Insert
Replace
Delete

- Click Apply. The rules are applied.

Delete Firewall Rules

► **To delete a firewall rule:**

1. Choose Device Settings > Security. The Security Settings window opens.
2. Make sure the Enable IP 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 IP Access Control panel.
5. Click Apply. The rule is deleted.

Create Group Based Access Control Rules

Group based access control rules are similar to firewall rules, except they can be applied to members of specific User Groups. This enables you to give entire User Groups system and outlet permissions, based on their IP addresses or subnets.

To create group based access control rules, first enable the feature. Then set the default action, specify an IP address range, and associate the rule with a specific User group. Finally, indicate whether the rule will accept or drop traffic. Changes made will not affect users currently logged in until the next login.

Enable the feature

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

1. Choose Device Settings > Security. The Security Settings window 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. Click Apply. Group based access control rules are enabled.

Change the Default Action

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

► To change the default action:

1. Choose Device Settings > Security. The Security Settings window 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.

Create Group Based Access Control Rules

Group based access control rules accept or drop traffic intended for the Dominion PX, based on the user's group membership. Like firewall rules, the order of the rule 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 window 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 field. This rule applies to members of this group only. • Select ACCEPT or DROP from the drop-down list in the Policy field. • Click Append. <p>Do NOT enter a rule number. This system automatically numbers the rule.</p>

Action	Do this...
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 #5 and #6, type 6. • 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 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 Action field. • Click Replace. <p>This system replaces the existing rule with the one you just created.</p>

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

Delete Group Based Access Control Rules

► **To delete a firewall rule:**

1. Choose Device Settings > Security. The Security Settings window opens.
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.

Set Up User Login Controls

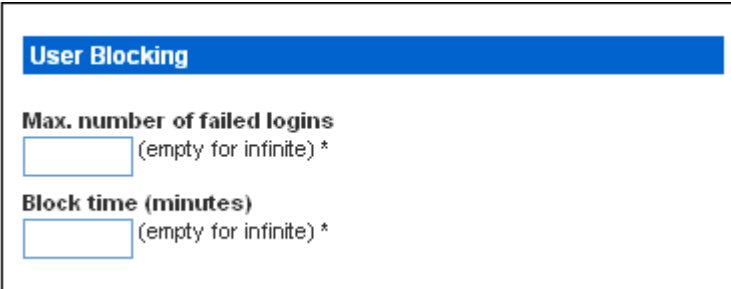
You can set up login controls to make it more difficult for hackers to access the Dominion PX and the devices connected to it. You can arrange to lock persons out after a specified number of failed logins, limit the number of persons who can log in at the same time using the same login, and force users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

Enable User Blocking

User blocking allows you to determine how many times a user can attempt to log into 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 window opens. Go to the User Blocking panel.



User Blocking

Max. number of failed logins
 (empty for infinite) *

Block time (minutes)
 (empty for infinite) *

2. Type a number in the Max. 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. 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.
4. Click Apply. The user blocking limits are applied.

Enable Login Limitations

Login limitations allow you to determine whether more than one person can use the same login at the same time, and whether or not users will be required to change passwords at regularly scheduled intervals.

► **To enable login limitations:**

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

Login Limitations

Enable Single Login Limitation *

Enable Password Aging *

Password Aging Interval (days)
 *

Idle Timeout (minutes)
 *

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 will be 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 Dominion PX, enter a time in minutes in the Idle Timeout field. The default value is 15 minutes.
5. Click Apply. The controls are applied.

Note: Raritan recommends keeping the idle timeout to 15 minutes or less. This reduces the number of idle sessions connected, and the number of simultaneous commands sent to Dominion PX.

Enable Strong Passwords

Forcing users to create strong passwords makes it more difficult for intruders to crack user passwords and access the Dominion PX unit. Strong passwords should be at least eight characters long and should contain upper and lowercase letters, numbers, and special characters (such as @ or &).

► To force users to create strong passwords:

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

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 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.

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).

Once the CA has processed the information in the CSR, it will provide you with a certificate, which you must install on the Dominion PX.

*Note: See **Forcing HTTPS Encryption** (see "Force HTTPS Encryption" on page 50) for instructions on forcing users to employ SSL when connecting to the Dominion PX.*

Create a Certificate Signing Request

► **To create a CSR:**

1. Choose Device Setting > Certificate. The first page of the SSL Server Certificate Management window 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)
1024 *

2. Provide the information requested. Type the following in the appropriate fields:

Field	Type this...
Common name	The name of your company
Organizational unit	The name of your department
Organization	The name of your organization within the department

Field	Type this...
Locality/City	The city where your company is located
State/Province	The state or province where your company is located
Country (ISO code)	The country where your company is located. Use the standard ISO code. For a list of ISO codes, go to this Web site: http://www.iso.org/iso/en/prods-services/iso3166ma/02iso-3166-code-lists/list-en1.ht
Email	An email address where you or another administrative user can be reached
Challenge Password Confirm Challenge Password	The password that will be required to access the Dominion PX. Type it first in the Challenge Password field and then again in the Confirm Challenge password field. The password is case sensitive, so be sure to capitalize the same letters each time.

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

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

Certificate Signing Request (CSR)
Certificate Upload

The following CSR is pending:

```

countryName           = US
stateOrProvinceName  = New York
localityName          = New York
organizationName      = National
organizationalUnitName = Sales Department
commonName            = XYZ Corproation
emailAddress          = me@xyz.corp
                    
```

SSL Certificate File

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

Install a Certificate

Once the CA has provided you with a digital certificate, you must install it on the Dominion PX.

▶ **To install a certificate:**

1. Make sure a certificate has been created prior to any further configuration. Next, choose Device Settings > Certificate. The second page of the Server Certificate Management window 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.

Setting Up External User Authentication

For security purposes, users attempting to log into the Dominion PX must be authenticated. You can use the local database of user profiles in the Dominion PX, or you can use the Lightweight Directory Access Protocol (LDAP) or the Remote Access Dial-In User Service (RADIUS) protocol.

By default, the Dominion PX is configured for local authentication. If you stay with this method, you do not have 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 system with information about the server.

Remember that you still must create user profiles for users who are authenticated externally, because the user profile determines the User Group to which the user belongs, and the User Group determines the user's system and outlet permissions.

Note: Users who log in with External Authentication cannot perform operations on Outlet Groups. Users must authenticate locally to do this.

Gather Information for LDAP Configuration.

Configuring Dominion PX to use LDAP authentication requires knowledge of your LDAP server and directory settings. Below is a list of settings you will need values for to configure LDAP authentication. If you are not familiar with these settings, ask your LDAP administrator to help you prepare this list.

▶ **You will need to know:**

- The IP Address of the LDAP server.
- (Optionally) The IP address of a backup or secondary LDAP server.
- If the Secure LDAP protocol (LDAP with SSL) is being used.
 - If Secure LDAP is in use, ask your LDAP administrator for the CA certificate file.
- The network port used by the LDAP server.
- The type of LDAP server used. It will be one of the following:
 - A generic LDAP server.
 - Novell Directory Service.
 - Microsoft Active Directory.
 - If using a Microsoft Active Directory server, ask your AD administrator for the name of the Active Directory Domain.
- 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).

Setup LDAP Authentication

► To set up LDAP authentication:

1. Choose Device Settings > Authentication. The Authentication Settings window opens. The LDAP parameters appear on the left side of the window.

Authentication Settings

Local Authentication *

LDAP

User LDAP Server

 *

Backup User LDAP Server

 *

SSL Enabled *

Port

 *

SSL Port

 *

Certificate File

Base DN of user LDAP server

 *

Type of external LDAP server

 *

Name of login-name attribute

 *

Name of user-entry objectclass

 *

User Search Subfilter

 *

Active Directory Domain

 *

2. Click the radio button labeled LDAP to enable the LDAP fields on the page.
3. Type the IP address of the LDAP server in the User LDAP Server field.

4. Type the IP address of the Backup LDAP server in the Backup User LDAP Server field. This server will be used if the primary server cannot be contacted. Note that the remaining fields share the same settings with the User LDAP server. **Optional.**
5. To encrypt traffic to and from the LDAP server, select the **SSL Enabled** checkbox.
6. By default, the Dominion PX uses the standard port 389 for LDAP or port 636 for secure LDAP (SSL). If you prefer to use non-standard ports, specify another port.

Note: The SSL port is enabled only if you click the checkbox in Step 3.

7. If you enabled SSL (secure LDAP), consult your authentication server administrator to get the CA certificate file in Base64 encoded X-509 format for the LDAPS server. Use the Browse button to navigate to the certificate file.
8. Type the base DN in the Base DN of user LDAP server field. The base distinguished name (DN) is the top level of the LDAP directory tree. It indicates where in the LDAP directory you want to begin searching for user credentials. 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.
9. Select the type of LDAP server from the Type of external LDAP server drop-down list. Your choices are:
 - Generic LDAP Server
 - Novell Directory Service
 - Microsoft Active Directory
10. 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)
11. If you selected Microsoft Active Directory, enter the domain name in the Active Directory Domain field.
12. Click **Apply**. LDAP authentication is now in place.

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

Setting Up RADIUS Authentication

► To set up RADIUS authentication:

1. Choose Device Settings > Authentication. The Authentication Settings window opens. The RADIUS parameters appear on the right side of the window.

	Server	Shared Secret	Auth. Port	Acc. Port	Timeout	Retries
1.	<input type="text"/>	<input type="text"/>	1812 *	1813 *	1 *	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 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 2 - 7 for each additional server.
9. Select an authentication protocol from the drop-down list in the Global Authentication Type field. Your choices are:
 - 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.

Setting Up Outlets and Power Thresholds

The Dominion PX is shipped with certain Dominion PX and outlet power thresholds already defined. You can change the default Dominion PX thresholds, and you can give each outlet a name and change its default thresholds.

When setting the thresholds, remember that you can set up alerts that are triggered whenever any of these thresholds are crossed. See [Setting Up Alerts](#).

Set Default Outlet State

Set a global default for the power state of the outlets when the Dominion PX unit is powered on. Setting an individual outlet's startup state to something other than Device Default (see Naming the Outlets) will override this default state for that outlet.

► To set the default outlet state:

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

PDU Setup

Default outlet state on device startup
 Last Known State ▼ *

PDU Power Cycling Delay
 * s

Power off period during outlet power cycling
 * s

Sequence Delay
 * ms

Data Retrieval

Enable Data Retrieval *

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

Thresholds

	lower		upper		
	critical	non-critical	non-critical	critical	
Voltage	102	108	127	132	Volts
Line Current			14.69	14.69	Amps
Temperature	18	20	65	80	degrees C

see also: [Model Configuration](#)

Outlet Sequencing

Outlet 1 (1) ▲
 Outlet 2 (2)
 Outlet 3 (3)
 Outlet 4 (4)
 Outlet 5 (5)
 Outlet 6 (6)
 Outlet 7 (7)
 Outlet 8 (8) ▼

⬆ First

⬆ Up

⬇ Down

⬇ Last

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

Set Dominion PX Thresholds

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

1. Choose Device Settings > PDU Setup. The PDU Setup window opens.
2. Type a number in the field labeled PDU Power Cycling Delay. When power to the Dominion PX is cycled (either manually or because of a temporary power loss), this number determines how many seconds Dominion PX will wait 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 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).

*Note: The number you enter here applies to all outlets on the Dominion PX. However, you can override this number for specific outlets (see **Setting the Outlet Thresholds** (see "Set Outlet Thresholds" on page 73)). You can power cycle an outlet from the Outlet Details window (see **Power Cycling an Outlet** (see "Power Cycle an Outlet" on page 75)).*

4. Type a number of seconds in the field labeled Sequence Delay in ms. This is the Dominion PX takes from outlet to outlet when powering ON, OFF or cycling all outlets. The default is 200 milliseconds.
5. Set the voltage, current, temperature, and (if applicable) circuit breaker current thresholds for the unit in the Thresholds panel. Enter critical or non-critical threshold for each setting.
6. When you are finished, click Apply. The delays and thresholds are applied.

Note: When there are a large number of outlets, especially when dealing with outlets grouped from other Dominion PX Units, you may want to set both the Power off period and the Sequence Delays to lower numbers in order to avoid a long wait before all the outlets are available again.

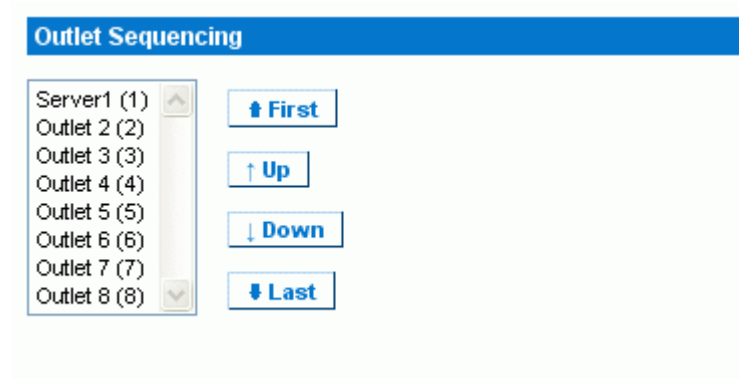
Users require the Unit & Outlet Configuration permission to see the contents of the PDU Setup page. Both the Unit & Outlet Configuration and the Line & Circuit Configuration permissions are required to adjust thresholds on the page.

Set Outlet Power-Up Sequence

You can set the order in which the unit's outlets power up. This is useful when devices have multiple power supplies that should be powered on together.

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

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



2. The current outlet power-up sequence appears in the list under Outlet Sequencing. To change the priority of an outlet, select it from the list and click one of four option buttons:
 - First moves the outlet to the top of the list and makes 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 and makes it the last outlet to receive power.
1. Click Apply. The new sequence is saved.

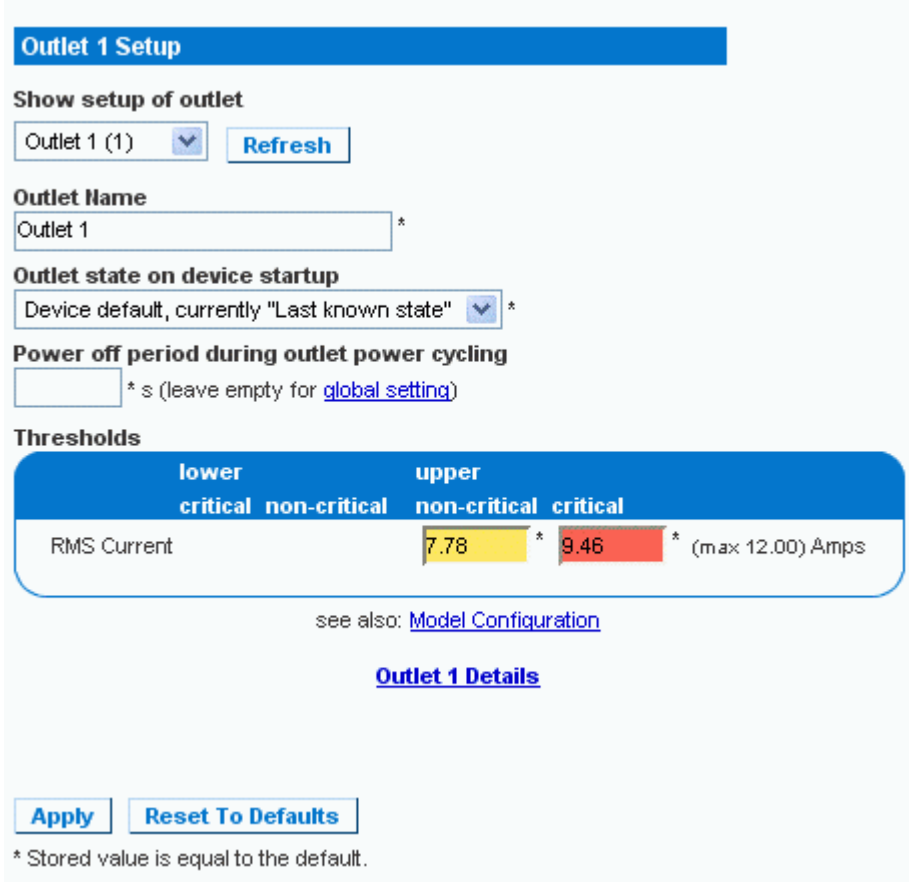
Note: If you use Outlet Grouping to group outlets together, you should adjust the Outlet Sequencing to ensure that all outlets from this Dominion PX that are part of the same group, power up consecutively.

Name Outlets

You can give each outlet a name to help you identify the device connected to it.

► **To name outlets:**

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



Outlet 1 Setup

Show setup of outlet

Outlet 1 (1)

Outlet Name
 Outlet 1 *

Outlet state on device startup
 Device default, currently "Last known state" *

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

Thresholds

	lower critical	non-critical	upper non-critical	critical	
RMS Current			7.78 *	9.46 *	(max 12.00) Amps

see also: [Model Configuration](#)

[Outlet 1 Details](#)

* Stored value is equal to the default.

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. This will determine if the outlet is ON or OFF when the Dominion PX powers up. If set to Device Default, the state for this outlet will be determined by the Default Outlet State in the PDU Setup page.
5. Click Apply. The new name is applied.

Set Outlet Thresholds

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

1. Choose Details > Outlet Setup. The Outlet Setup window opens.
2. Select an outlet from the Show setup of outlet drop-down list.
3. Type a number in the field labeled Power off period during outlet power cycling. When an outlet is power cycled, it is turned off and then back on. The number you enter here determines the length of time (in seconds) it takes for the outlet to turn back on after it is shut down during the power cycle. If left blank, this outlet will use the value set in the PDU Setup page as a default.

*Note: You can power cycle an outlet from the Outlet Details window. See **Power Cycling an Outlet** (see "Power Cycle an Outlet" on page 75).*

4. Set the RMS current thresholds for the outlet in the Thresholds panel.
5. When you are finished, click Apply. The setup details are applied.

View Outlet Details

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

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

Outlet 1 Details

Show details of outlet

Outlet 1a (1)

Outlet Name: Outlet 1a
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	

[Setup](#)

2. Select an outlet from the Show details of outlet drop-down list. The window 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

*Note: To display the Outlet Setup window, click the [Setup] link. See **Naming the Outlets** (see "Name Outlets" on page 72) for a picture of the Outlet Setup Window.*

Power Cycle an Outlet

Power Cycling an Outlet will turn 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 window opens.
2. Select an outlet from the Show details of outlet drop-down list. The outlet must be ON.
3. Click Cycle.

Note: You can also power cycle an outlet from the Home window.

*The length of time between the off and on states in a power cycle can be set on the Dominion PX as a whole, and for individual outlets. See **Setting the Dominion PX Thresholds** (see "Set Dominion PX Thresholds" on page 70) and **Setting the Outlet Thresholds** (see "Set Outlet Thresholds" on page 73).*

Turn Outlet On or Off

► **To turn an outlet on or off:**

1. Choose Details > Outlet Details. The Outlet Details window 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.

Note: You can also turn an outlet on or off from the Home window.

Environmental Sensors

In addition to monitoring its own internal temperature, Dominion PX can monitor the environment where environmental sensors are placed.

Connect Environmental Sensors

To enable Dominion PX to measure environmental factors, connect the cable of the environmental sensor to the Feature port of the unit.

To use multiple environmental sensors with the Environmental Sensor Hub, first connect the IN port (Port 1) of the sensor hub to the Feature port of the Dominion PX, then connect your environmental sensors to any of the four OUT ports of the hub.

Map Environmental Sensors

Once the sensors have been physically connected to the Dominion PX, they must be mapped to the unit's logical sensors before Dominion PX will recognize (and display) the readings from them.

► **To map the environmental sensors:**

1. Choose Device Settings > Environmental Sensors. The Environmental Sensors window opens. The page will list the logical Temperature and Humidity sensors first.

Environmental Humidity Sensor 8

Name
Humidity 8 *

Thresholds

	lower critical	non-critical	upper non-critical	critical	
Humidity	5 *	10 *	90 *	95 *	rel. %

Environmental Temperature Sensors

Description	Serial Number	Reading	Temperature 1 (1)	Temperature 2 (2)	Temperature 3 (3)	Temperature 4 (4)	Temperature 5 (5)	Temperature 6 (6)	Temperature 7 (7)	Temperature 8 (8)
DS2438 Temperature	FE7AB5000000	25.0 degrees C	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
DS2438 Temperature	6FC894000000	24.0 degrees C	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
			<input type="button" value="clear"/>	<input type="button" value="clear"/>	<input type="button" value="clear"/>	<input type="button" value="clear"/>	<input type="button" value="clear"/>	<input type="button" value="clear"/>	<input type="button" value="clear"/>	<input type="button" value="clear"/>

Environmental Humidity Sensors

Description	Serial Number	Reading	Humidity 1 (1)	Humidity 2 (2)	Humidity 3 (3)	Humidity 4 (4)	Humidity 5 (5)	Humidity 6 (6)	Humidity 7 (7)	Humidity 8 (8)
DS2438 Humidity	FE7AB5000000	18 rel. %	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
DS2438 Humidity	6FC894000000	16 rel. %	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
			<input type="button" value="clear"/>	<input type="button" value="clear"/>	<input type="button" value="clear"/>	<input type="button" value="clear"/>	<input type="button" value="clear"/>	<input type="button" value="clear"/>	<input type="button" value="clear"/>	<input type="button" value="clear"/>

2. When physical sensors are attached to the Dominion PX, they will appear listed below the logical sensors. Temperature sensors will be listed in the Environmental Temperature Sensors table, humidity sensors in the Environmental Humidity Sensors table. If the sensors are not attached properly, the message appears: No sensors were detected.
3. For each physical sensor (shown as a row) in the table, click a radio button under the logical sensor (shown as columns) you want to map it to. Dominion PX will now track this sensor's readings and display it on the home page when configuration is finished.

If you do not want to track the readings of a particular sensor, leave that row blank.

4. To unmap a logical sensor from any physical sensor, click clear at the bottom of the column. That logical sensor will no longer be associated with any of the physical sensors.

Note: It is possible (but not advisable) to map more than one logical sensor to a single physical sensor. You cannot map multiple physical sensors to a single logical one.

Identifying Environmental Sensors for Mapping

Each sensor includes a serial number tag on the sensor cable.



The serial number for each sensor also appears listed with each physical sensor detected by Dominion PX.

Environmental Temperature Sensors

Description	Serial Number	Reading	Temperature 1 (1)	Temperature 2
DS2438 Temperature	AEI7B00019	24.5 degrees C	<input type="radio"/>	<input type="radio"/>
			<input type="button" value="clear"/>	<input type="button" value="clear"/>

Environmental Humidity Sensors

Description	Serial Number	Reading	Humidity 1 (1)	Humidity 2 (2)	Humidity 3 (3)
DS2438 Humidity	AEI7B00019	39 rel. %	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
			<input type="button" value="clear"/>	<input type="button" value="clear"/>	<input type="button" value="clear"/>

Match the serial number from the tag to the ones in the Environmental Sensor table in order to identify and differentiate sensors, then map the physical sensor to the logical sensors and configure the thresholds appropriately.

Configure Environmental Sensors and Thresholds

To make sensors more useful, rename the logical sensors that are in use and configure their threshold settings. Configuring thresholds for these sensors allows Dominion PX to generate an alert whenever environmental factors at those sensors move outside of your idea values.

1. From the Environmental Sensors page, locate the logical sensors that have been mapped to physical sensors as previously described.

Environmental Temperature Sensor 1

Name

Thresholds

	lower critical	non-critical	upper non-critical	critical	
Temperature	-19.0 *	-18.0 *	20.0	107.0 *	degrees C

Environmental Temperature Sensor 2

Name

Thresholds

	lower critical	non-critical	upper non-critical	critical	
Temperature	-19.0 *	-18.0 *	105.5 *	107.0 *	degrees C

2. In the Name field, type a new name for each mapped sensor that will help you identify the sensor and its purpose.
3. Configure the upper and lower thresholds for each sensor in use.
 - The Upper Critical and Lower Critical values are points at which the Dominion PX considers the operating environment is critical and outside the range of the acceptable threshold.
 - Once critical, the temperature or humidity 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.
1. Click Apply. The sensor name and threshold settings are saved.

When the configuration changes have been applied, the sensor readings will be displayed on the Home Page next to the outlet list, and the sensor names will be updated. This updated name will also appear in the physical sensors table at the bottom of the Environmental Sensors page. This can be useful for ensuring that the physical and logical sensors are correctly mapped together.

Environmental Temperature Sensors										
Description	Serial Number	Reading	Outside Cabinet 1 Temp. (1)	Mid-Inside Cabinet 1 Temp. (2)	Temperature 3 (3)	Temperature 4 (4)	Temperature 5 (5)	Temperature 6 (6)	Temperature 7 (7)	Temperature 8 (8)
DS2438 Temperature	FE7AB5000000	24.5 degrees C	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
DS2438 Temperature	6FC894000000	24.0 degrees C	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
			<input type="button" value="clear"/>	<input type="button" value="clear"/>	<input type="button" value="clear"/>	<input type="button" value="clear"/>	<input type="button" value="clear"/>	<input type="button" value="clear"/>	<input type="button" value="clear"/>	<input type="button" value="clear"/>

Environmental Humidity Sensors										
Description	Serial Number	Reading	Cabinet 1 Humidity (top) (1)	Cabinet 1 Humidity (bottom) (2)	Humidity 3 (3)	Humidity 4 (4)	Humidity 5 (5)	Humidity 6 (6)	Humidity 7 (7)	Humidity 8 (8)
DS2438 Humidity	FE7AB5000000	19 rel. %	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
DS2438 Humidity	6FC894000000	16 rel. %	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
			<input type="button" value="clear"/>	<input type="button" value="clear"/>	<input type="button" value="clear"/>	<input type="button" value="clear"/>	<input type="button" value="clear"/>	<input type="button" value="clear"/>	<input type="button" value="clear"/>	<input type="button" value="clear"/>

Note: The recommended maximum ambient operating temperature for the Dominion PX is 40 degrees Celsius.

View Sensor Readings

Mapped sensor readings appear beside the outlet list any time the Home page is open. To view the readings from any other page, click Home in the navigation path at the top of the window.

Name	State	Control	RMS Current	Active Power	Group Member
Outlet 1 (1)	on	<input type="button" value="On"/> <input type="button" value="Off"/> <input type="button" value="Cycle"/>	1.05 Amps	82.09 Watts	yes
Outlet 2 (2)	on	<input type="button" value="On"/> <input type="button" value="Off"/> <input type="button" value="Cycle"/>	0.00 Amps	0.00 Watts	no
Outlet 3 (3)	on	<input type="button" value="On"/> <input type="button" value="Off"/> <input type="button" value="Cycle"/>	0.95 Amps	71.85 Watts	yes
Outlet 4 (4)	on	<input type="button" value="On"/> <input type="button" value="Off"/> <input type="button" value="Cycle"/>	1.00 Amps	78.52 Watts	no
Outlet 5 (5)	on	<input type="button" value="On"/> <input type="button" value="Off"/> <input type="button" value="Cycle"/>	0.59 Amps	62.88 Watts	yes

Environmental Sensors	
Outside Cabinet 1 Temp. (Temperature 1)	24.5 degrees C
Mid-Inside Cabinet 1 Temp. (Temperature 2)	24.5 degrees C
Cabinet 1 Humidity (top) (Humidity 1)	19 rel. %
Cabinet 1 Humidity (bottom) (Humidity 2)	16 rel. %

Configuring and Using Alert Notifications

A benefit of Dominion PX's intelligence is its ability to notify you of (and react to) a change in conditions. This notification is called an Alert.

Components of an Alert

The Alert is a condition statement, that is, if "A" happens, then do "B". This condition statement describes what the Dominion PX will do 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: The Dominion PX's internal temperature exceeds the warning threshold.
- **Policy:** This is the "B" portion of an alert and describes the response to the event. For example: Notify the system administrator and record the event in the log.
- **Threshold:** This is a condition met by the event. For example: a temperature warning level.
- **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 in the Outlet Setup Page. Unit-wide thresholds are assigned in the PDU Setup page. Environmental thresholds are assigned in the Environmental Sensors 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 the Configuring the SMTP Settings section).

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 will 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 in the Alert Destinations page. Choose Alerts > Alert Destinations to open the page.

The screenshot displays the 'Alert Destinations' page. At the top is a blue header with the text 'Alert Destinations'. Below this is a table with a blue header row labeled 'Destination'. The table contains five rows of data:

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

Below the table is a form to add a new destination. It has two labels: 'Destination Type:' and 'Receiver eMail Address:'. Under 'Destination Type' is a dropdown menu with 'eMail' selected and a list of options including 'eMail' and 'SNMP'. Under 'Receiver eMail Address' is a text input field. To the right of the input field is an 'Add' button.

At the bottom of the page, there are navigation links: [Alert Destination](#) - [Alert Policies](#) - [Alert Policy Editor](#).

This table on the page lists the existing destinations configured on 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 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 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 destinations to a policy causes an SNMP trap to be sent to the specified IP address. Multiple SNMP destinations can be created.

► **To add an eMail destination:**

1. Choose Alerts > Alert Destinations. The Alerts Destination window 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 window 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.

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 in the Event Logging page.

For SNMP alert destinations, 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 on these traps can be Details of such 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 will 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 ---

▼

Refresh

New Policy Name

Cycle Outlet + Notify

Destinations

System

Event Log

eMail

sysadmin@companyname.com

weekend@companyname.com

SNMP

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 can create a new policy. The table on this page lists all the configured alert destinations available on the Dominion PX.

► **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 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.
 - 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: In Dominion PX models without outlet switching, the Current Outlet and Switch Outlet destinations have no effect.

These policies will now be available as a response when creating an Alert. When the alert is triggered, outlets will be switched and alert notifications will be sent to the event log, e-mail accounts, and SNMP managers as dictated by the selected policy.

Note: If the Event Log is set as a destination, alert events will be sent to all logging services selected 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. To avoid duplicate notices, Raritan recommends selecting only different SNMP and email destinations when the Event Log destination is selected.

Creating Alerts

The Alert Configuration Page is where you specify how Dominion PX responds to certain events. First describe an event that triggers an alert and then select the policy 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 window opens.
2. Under the Event drop-down list, select the segment of the Dominion PX 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 will have three current lines, single-phase PDUs will only have one.
 - Outlet: refers to a specific, single outlet on the Dominion PX.
 - 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.
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 threshold must be exceeded to trigger the alert.
 - Assert & Deassert: will cause the alert to trigger when the measured value moves past a threshold in either direction.
 - Assert: will cause this alert to trigger only when the measured value moves past the threshold (either above an upper threshold or below a lower threshold). This means when the described event is TRUE.
 - Deassert: will cause this alert to trigger only when the measured value returns towards "normal" from beyond the threshold (either below an upper threshold or above a lower threshold). This means when the described event is FALSE.

For example: If you select "Environmental Temperature above upper critical threshold" and set the event direction to Assert & Deassert, the selected policy will be executed when the temperature of the cabinet exceeds the critical threshold. When the environment cools and the temperature drops below the critical threshold, the policy will be executed 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.
7. Click Add.

Added alerts will now be tracked by Dominion PX. When an alert's event conditions are met, the associated policy will be executed.

Note: If Environmental Temperature or Environmental Humidity is selected as part of the Event, an alert event will be created for each logical 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, and this alert calls a policy that turns the outlet OFF. In this case, the alert will trigger 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 will 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 Dominion PX to notify us when the current draw on a specific outlet (Outlet 6) approaches the critical limit. To do that we would setup 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 will have Event Log, the IP address of an SNMP manager, and the email address of the facilities manager checked. With these settings, Dominion PX will record 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 Dominion PX to shut down most of its outlets if the Dominion PX becomes too hot. However, since mission-critical servers are plugged in to 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 unit 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," will have the Switch Outlet destination selected and Outlet 1 and Outlet 2 set to ON. The remaining outlets will be 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 would power OFF to avoid damage and prevent from adding more heat to the room. The sysadmin and the facilities manager would both receive notification 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 will power 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 will check 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), Dominion PX will power on all of its outlets. Additionally, the system administrator and the facilities manager will receive e-mail notification stating that the room temperature dropped below the warning level.

Setting Up Event Logging

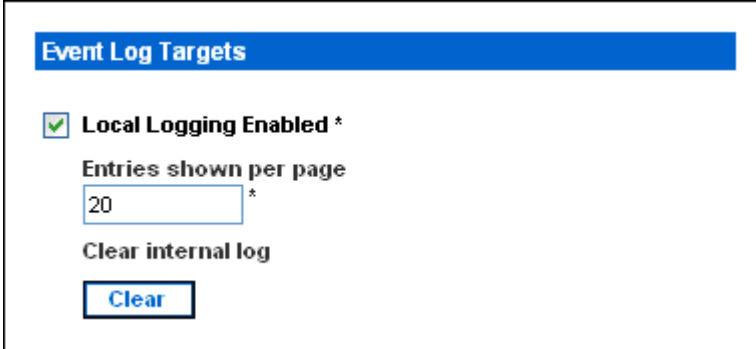
By default, the Dominion PX captures certain system events and saves them in a local (internal) event log. You can expand the scope of the logging to also capture events in the NFS, SMTP, and SNMP logs.

Note: When configuring Dominion PX to use more than one logging method, configure each method individually and apply the changes before configuring the next.

Configure Local Event Log

► **To configure the local event log:**

1. Choose Device Settings > Event Log. The Event Log Settings window opens. The Local Logging panel appears first. This panel controls the local event log.



The screenshot shows a web interface titled "Event Log Targets". It contains a checked checkbox labeled "Local Logging Enabled *". Below this is a text input field labeled "Entries shown per page" with the value "20" and an asterisk. Underneath 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 the Event Types appendix for a more detailed explanation of these event types.

- When you are finished, click Apply. Local logging is configured.

View Internal 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](#)

Entries

For each entry, the event log shows:

- The date and time of the event
- The type of event (board message, security, host control, or authentication)
- A brief 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 internal event log displays 20 events per page. See **Configuring the Local Event Log** (see "Configure Local Event Log" on page 93) for details on changing this number.*

Configure NFS Logging

► **To configure Network File System (NFS) logging:**

1. Choose Device Settings > Event Log. The Event Log Settings window opens. The NFS Logging panel controls NFS logging.

NFS Logging Enabled *

NFS Server
 *

NFS Share
 *

NFS Log File
 *

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.

Configure SMTP Logging

► To configure Simple Mail Transfer Protocol (SMTP) logging:

1. Choose Device Settings > Event Log. The Event Log Settings window 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!

2. Select the SMTP Logging Enabled checkbox.
3. Type the receiver's email address in the Receiver Email Address field.
4. 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"/> *

5. Click Apply. SMTP logging is configured.

Important: If you have not configured the Dominion PX's SMTP settings, you must do so for SMTP logging to work. Click the [here](#) link at the bottom of the panel. See *Configuring the SMTP Settings* (on page 107).

Configure SNMP Logging

Event logging can be performed by sending SNMP traps to a third-party SNMP manager. See the Using SNMP appendix for instructions on enabling SNMP Event Logging on Dominion PX.

Configure Syslog Forwarding

Note: If you enable Syslog forwarding a "--MARK--" message may appear in the Syslog record every 20 minutes. This is a keep-alive method used by Dominion PX.

► **To configure Syslog Forwarding:**

1. Choose Device Settings > Event Log. The Event Log Settings window 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 will be 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.

Managing the Dominion PX

You can display basic device information about the Dominion PX, give the Dominion PX a new device name, and modify any of the network settings that were entered during the initial configuration process. You can also set the unit'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 unit:**

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

Device Information

Product Name:	PX (PX-5532)
Serial Number:	1234567890
Board ID:	06749f010e45afe0
Device IP Address:	192.168.57.67
Device MAC Address:	00:0D:5D:05:0D:33
Firmware Version:	01.02
Firmware Build Number:	7039
Firmware Description:	Standard Edition
Hardware Revision:	0x1A
Relay Board 1 Serial Number:	64
Relay Board 2 Serial Number:	64
Relay Board 3 Serial Number:	64
Relay Board 4 Serial Number:	64
Relay Board 5 Serial Number:	64
Relay Board 6 Serial Number:	64
Relay Firmware Version:	0x46
Relay Hardware Revision:	0x42 : 0x20

[View the datafile for support.](#)

Model Configuration

Input Plug:	CS8365C
Input Voltage:	208 Volts
Line Current Rating:	35.37 Amps
PDU Power Rating:	12.5 kVA
Circuit Breaker Rating:	20 Amps
Outlet Count:	24
Outlet Type:	NEMA 5-15R (12 Amp Rating)
Outlet Voltage:	208 Volts

Outlet Mapping	Circuit Breaker
Outlets 1 - 8	1
Outlets 9 - 16	2
Outlets 17 - 24	3

Connected Users

admin (192.168.32.20) active

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

Displaying Model Configuration Information

To display information about the specific model of the Dominion PX that you are using, choose Maintenance > Device Information. The Device Information window opens. Information about your model is shown in the Model Configuration Panel below the Device Information panel.

This panel shows:

- The unit's and board's maximum RMS current
- The outlet maximum RMS current and current thresholds sum restriction
- The outlets governed by each circuit breaker

Displaying Connected Users

To display a list of users currently connected to the Dominion PX, choose Maintenance > Device Information. The Device Information window opens. A list of connected users is shown in the Connected Users Panel. See **Displaying Basic Device Information** (on page 99).

The panel shows the username and IP address of each user, and indicates whether or not the connection is active.

Naming the Dominion PX

By default, the Dominion PX has a device name of pdu. You may want to give the Dominion PX a more easily recognizable name to help identify it.

► To name the Dominion PX:

1. Choose Device Settings > Network. The Network Settings window opens. The left side of the window 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 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) will be registered with DNS and used on the assigned IPs by DHCP.
4. Click Apply. The Dominion PX is renamed.

Modifying the Network Settings

The Dominion PX was configured for network connectivity during the installation and configuration process (see ***Installation and Configuration*** (on page 12)). If necessary, you can modify any of these settings. To do this:

1. Choose Device Settings > Network. The Network Settings window opens. The left side of the window consists of the Basic Network Settings panel, which shows the current network settings. See ***Naming the Dominion PX*** (on page 102) for details on this panel.
2. Do one of the following:
 - Auto configuration - To auto-configure the Dominion PX, select DHCP or BOOTP from the IP Auto Configuration drop-down list. If you select DHCP, you can also enter a preferred host name.
Optional.
 - Static IP - To enter a static IP address, select none from the drop-down list in the IP Auto Configuration field, and then enter:
IP address
Subnet mask
Gateway address
Primary and (optional) secondary DNS server addresses
3. When you are finished, click Apply. The network settings are modified.

Modifying the Communications, Port and Bandwidth Settings

You can use Telnet or SSH to log into the Dominion PX's CLP interface. However, by default, SSH is enabled and Telnet is not (because it communicates openly and is not secure). You can change this and enable or disable either application.

You can also set a bandwidth limit and change any of the default port settings. Finally, you can enable or disable the Raritan Setup Protocol.

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

Miscellaneous Network Settings

Remote Console & HTTPS Port
 *

HTTP Port
 *

CLP-Telnet Port
 *

CLP-SSH Port
 *

Bandwidth Limit
 kbit/s *

Enable CLP-Telnet Access *

Enable CLP-SSH Access *

Disable Setup Protocol *

2. By default, CLP-Telnet is disabled and CLP-SSH is enabled. To change this, select either checkbox.
3. To set an upper limit on the amount of bandwidth Telnet or SSH will be allowed to use, type the number of kilobits per second in the Bandwidth Limit field.
4. By default, the HTTP, HTTPS, Telnet, and SSH ports are set to the standard ports for these communications protocols. If you prefer to use different ports, you can change the port assignments here.
5. Select the Disable Setup Protocol checkbox to disable it.

Note: No programs are currently available to use the Setup Protocol with Dominion PX. It is safe to leave this disabled.

- 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 **Configuring the Dominion PX for Network Connectivity** (on page 15)).

► **To modify either setting:**

- Choose Device Settings > Network. The Network Settings window 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 interface speed, select the speed you want from the drop-down list in the LAN Interface Speed field. Your choices are:
 - Autodetect (system selects optimum speed)
 - 10 Mbps
 - 100 Mbps
- To change the duplex mode, select the mode you want from the drop-down list in the LAN Interface Duplex Mode field. Your choices are:
 - Autodetect (system selects optimum mode)
 - Half duplex
 - Full duplex
- Half duplex allows data to be transmitted to and from the Dominion PX, but not at the same time. Full duplex allows data to be transmitted in both directions at the same time.
- When you are finished, click Apply. The settings are modified.

Setting the Date and Time

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

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

2. Enter a time zone by selecting the appropriate Coordinated Universal Time (UTC) offset from the UTC Offset drop-down list (for example, US Eastern Standard Time = UTC-5).
3. To set the date and time manually, click the radio button labeled User specified time then enter the date and time in the Date and Time fields. Use the yyyy/mm/dd format for the date and the hh:mm:ss format for the time.
4. To let an NTP server set the date and time, click the radio button labeled Synchronize with NTP server and enter the IP addresses of primary and secondary NTP servers in the corresponding fields. But if PX's IP address is assigned through DHCP, the NTP server addresses will be automatically discovered, then users will not be able to enter any data in the fields of primary and secondary time server.
5. Click Apply. The date and time settings are applied.

Configuring the SMTP Settings

The Dominion PX allows you to configure alerts to send an email message to a specific administrator. To do this, you have to configure the Dominion PX's SMTP settings and enter an IP address for your SMTP server and a sender's email address.

Note: See [Setting Up Alerts](#) for details on configuring alerts to send emails.

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

The screenshot shows two side-by-side panels. 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!', a 'Receiver Address' field with an empty input, 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 applied the SMTP settings, you can test them to ensure they work correctly. 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

The SNMP Settings window allows you to enable and disable SNMP communication between an SNMP manager and the PX device. Enabling SNMP communication will allow the PX to send SNMP trap events to the manager, as well as allow the manager to retrieve and control the power status of each outlet.

► **To configure SNMP communication (necessary for passing SNMP traps as well as individual outlet control):**

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

SNMP Settings

Enable SNMP Agent ^

Enable SNMP v1 / v2c Protocol ^

Read Community *

Write Community *

Enable SNMP 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 will become available.
3. Check SNMP v1 / v2c Protocol to enable communication with an SNMP manager using SNMP v2c protocol. Then type the SNMP read-only community string in the Read Community field and the read/write community string in the Write Community field.
4. Select the Enable SNMP v3 Protocol checkbox to enable communication with an SNMP manager using SNMP v3 protocol.

5. Type the System Location in the System Location field.
6. Type the System Contact in the System Contact field.
7. Click on the link at the bottom of the window 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

This feature allows the retrieval of Dominion PX data (such as unit, outlet, line, and circuit breaker data, etc.) by an SNMP manager. When enabled, Dominion PX will measure all sensor data at regular intervals and store these samples for access over SNMP. Dominion PX will store up to the last 120 measurements taken.

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.

Dominion PX's SNMP agent must be enabled for this feature to work (refer to Enabling SNMP in the Appendix area for more details). Additionally, Raritan recommends using an NTP server for 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) Dominion PX will store 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 will be stored immediately once this feature is enabled and the delay between samples is configured.

Once configured, an external manager or application (such as Power IQ) will be able to access the stored Dominion PX data using SNMP. Download the Dominion PX MIB file to assist you in configuring third-party managers to retrieve data (refer to the Using SNMP appendix).

Retrievable Data

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

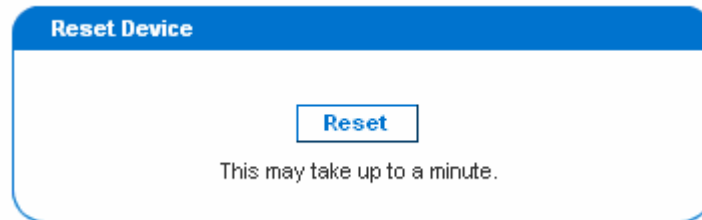
- Time stamp indicating when data sample was collected in UTC format.
- Unit Apparent Power
- Unit Active Power
- For each outlet
 - Outlet Number
 - Outlet Up Time
 - Number of seconds since the outlet was last switched on
 - Outlet RMS current
 - Outlet Voltage
 - Outlet Power Factor
- For each circuit breaker
 - circuit breaker number
 - RMS current drawn
- Line Currents
 - For each Line
 - Line identifier
 - RMS current
- Line Voltages
 - For each Line
 - Line identifier
 - Line Voltage

Resetting the Dominion PX

You can use Unit Reset function to reboot the Dominion PX from the Web interface.

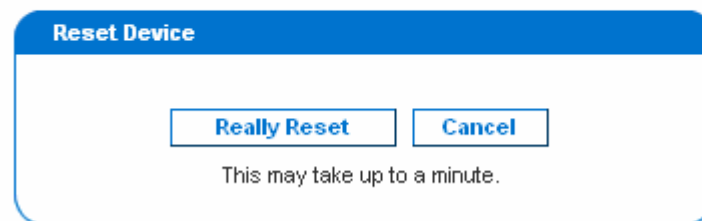
► **To reset the Dominion PX:**

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



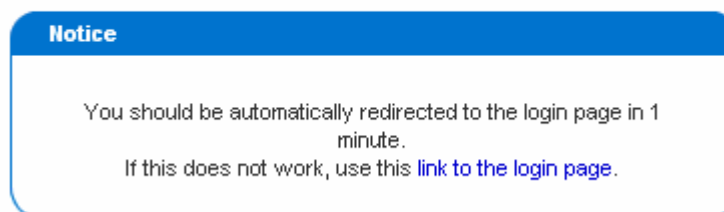
- Click Reset. A Reset Confirmation window opens.

***Are you sure you want to restart the device?
Please confirm by pressing "Really Reset".***



- When you click Really Reset, the Dominion PX will reboot. If you change your mind, click Cancel to terminate the reset operation. If you choose to proceed with the reset, the window shown below opens and the reset takes place. The reset takes about one minute to complete.

The device will be reset in a few seconds.




- When the reset is complete, the Dominion PX unit restarts and the Login window is displayed. Then, you can log back into the Dominion PX.

Updating the Firmware

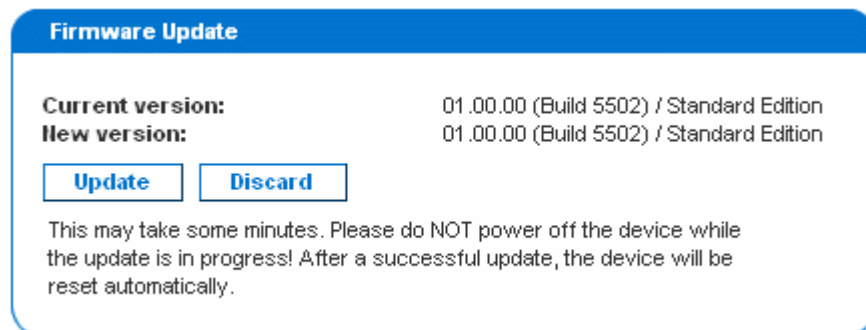
Users must either use the admin account or have both the Firmware Update and Unit Reset privileges in order to successfully update Dominion PX firmware.

To update firmware:

1. Choose Maintenance > Update Firmware. The Firmware Upload window opens.



2. Type the complete path to the firmware file in the Firmware File field, or click Browse and select the file.
OR
In the Firmware URL field, type in an URL link where the firmware file is network-retrievable.
3. Click Upload. The Firmware Update window opens. It shows the current firmware version and the new firmware version, and gives you a last chance to terminate the update.



4. To proceed with the update, click Update. To terminate the update, click Discard. The update may take several minutes. The Status panel on the left tracks the progress of the upgrade.

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

- When the update is complete, a message appears similar to the one shown below indicating the update was successful. The Dominion PX will be reset, and the Login window will re-appear. You can now log in and resume managing the Dominion PX.

Firmware updated successfully.
The device will be reset in a few seconds.

Notice

You should be automatically redirected to the login page in 1 minute. If this does not work, use this [link to the login page](#).

Note: If you are using Dominion PX with an SNMP manager, you should re-download the Dominion PX MIB after updating the unit's firmware. This will ensure your SNMP manager has the correct MIB for the release you are using. See the Using SNMP appendix for details.

Copying Configurations with Bulk Configuration

The Bulk Configuration feature lets you save the settings of a configured Dominion PX unit to your PC. This file can be used to copy that configuration to other PX units of the same model type. Users saving Dominion PX configurations require the Bulk Configuration system permission. Users copying configurations require both the Bulk Configuration and the Unit Reset permissions.

Save Configuration

Copy Configuration to Target

File Name

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** unit is an already configured Dominion PX that is used to create a configuration file. This configuration file contains the settings that can be shared between Dominion PX units, such as user and group configurations, thresholds, alert policies, the access control list, etc. This file does not contain device-specific information, including:

- Device Name
- System Name, System Contact and System Location
- Network settings (IP address, Gateway and Netmask)
- Local Time
- Outlet Names and Outlet Status
- External Sensor Names and Sensor Mappings
- Device Logs
- Outlet Grouping Data
- Default Outlet State (at either the Unit level or Outlet level)

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 Dominion PX units in a different time zone than the source unit.

► **To save a configuration file:**

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

Copying a Dominion PX Configuration

A **target** unit is a Dominion PX that loads another unit's configuration file. Copying a Dominion PX configuration to a target unit will adjust that Dominion PX's settings to match those of the source unit. In order to successfully restore a Dominion PX configuration:

- The user must have the Bulk Configuration and Unit Reset system permission.
- The target Dominion PX must be the same model type as the source Dominion PX.
- The target Dominion PX must be running the same firmware version as the source Dominion PX.

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

1. Login to the target unit's web interface.
2. If the firmware version does not match that of the source Dominion PX, choose Maintenance > Update Firmware to update the firmware of the target Dominion PX.
3. Choose Maintenance > Bulk Configuration. The Bulk Configuration window 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 will record that a configuration copy occurred on the target device, but NFS and Syslog servers will not.

Note: If the source Dominion PX is configured to "Force HTTPS for web access", and the target unit 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 once the copying is complete and the login page will appear.

Outlet Grouping

Using the Outlet Grouping feature, you can combine outlets from separate Dominion PX Units 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 units.

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 units. All units must be accessible over IP and must be running firmware version 1.1 or higher.

Identifying Other Dominion PX Units

To add outlets from other Dominion PX units, you must first identify which Dominion PX units will be sharing their outlets.

► To identify other Dominion PX units:

1. Chose Outlet Groups > Outlet Group Devices. The Outlet Group Devices window 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 unit you want to add in the Name field.
3. Type the IP Address of the Dominion PX unit you want to add in the IP Address field.
4. Type a Username and Password used to authenticate on the Dominion PX unit being added. You can leave these fields blank to use the same username and password as the Dominion PX currently being accessed. **Optional.**

- Click Add/Modify. The new Dominion PX is now available for outlet grouping.

To modify the name or the Username and Password used to access a participating Dominion PX, retype the information for the same Dominion PX unit and click Add/Modify again.

Note: You can re-add the Dominion PX unit 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 units have been added to list of outlet group devices, their individual outlets can be grouped together. Outlets that are grouped together will power on and power off in unison, using a control panel from the Dominion PX where the outlet group was created.

► To group outlets together:

- Choose Outlet Groups > Outlet Group Editor. The Outlet Group Editor window 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.
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 units and their outlets appears under Collection of Real Outlets. Check the box representing the desired physical outlet to make it part of the outlet group. All outlets that are checked will be 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 units. 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 will 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 will appear in this Outlet Groups list. Outlet groups created through another Dominion PX will not appear here, even if they contain outlets from this unit.

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 will be prompted to confirm your choice. Click OK to proceed.
4. The page will refresh 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 will be 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 will take 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 window opens.
2. Select the desired outlet group from the Outlet Groups drop-down list.
3. The details for the outlet group appear. Change the name, 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.

Deleting Outlet Group Devices

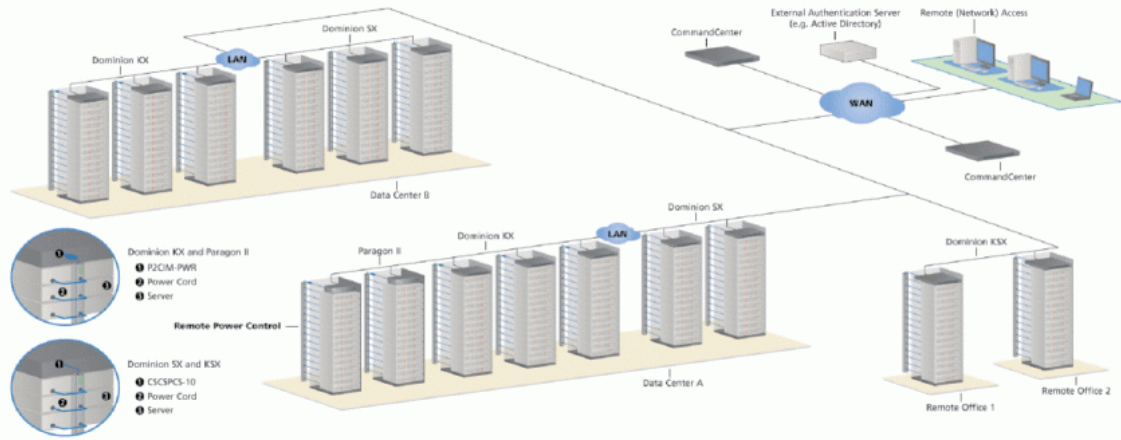
► **To delete a Dominion PX from outlet grouping when it is no longer available or in use:**

1. Choose Outlet Groups > Outlet Group Devices. The Outlet Group Devices window opens, displaying a list of known Dominion PX units.
2. Click Delete for the Dominion PX you want to remove from outlet grouping.

Note: If you delete a Dominion PX that still has outlets in a group, it will remove the associated outlets from that group, but the group will still exist. Remove the group itself using the Outlet Group Editor.

You should not delete the host device (the Dominion PX 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.

Chapter 6 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 later.
Dominion KX-II	KX GUI	RRC/MPC, JAC	CC-GUI	CC GUI	D2CIM-PWR	4; 8 in KX 1.3 or later.

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 serial port of the Dominion PX will switch all the outlets to the ON state, even if they were previously OFF.

In This Chapter

Dominion KX.....	122
Paragon II	125
Dominion SX.....	128
Dominion KSX	130
CommandCenter Secure Gateway	131

Dominion KX

Dominion KX (with the latest firmware) supports up to eight Dominion PX units, and requires P2CIM-PWR and straight CAT5 cable. You can associate up to four outlets to a target; all four outlets can be from separate Dominion PX Units, if needed.

KX Manager Application (Dominion KX-I only)

Use Raritan's KX Manager application to configure associations.

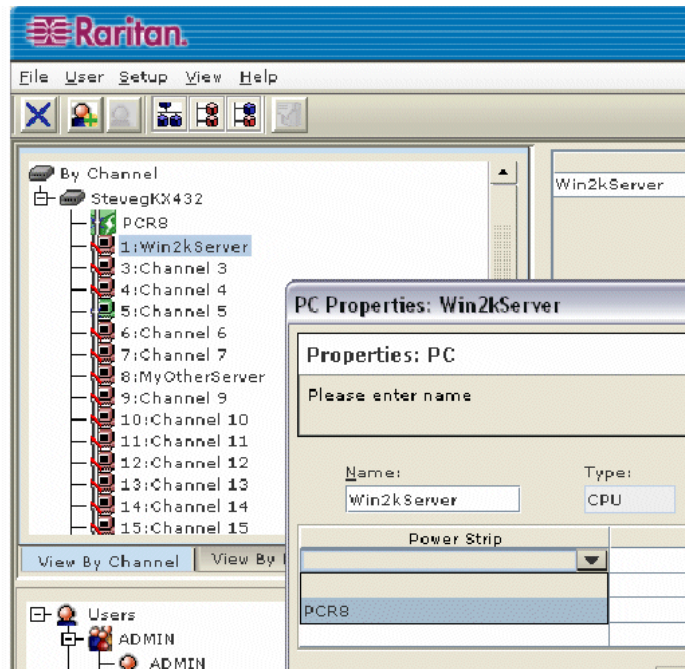
► **To configure associations:**

1. Select the target.
2. Edit the Properties and choose the outlets to associate. The outlets are automatically renamed to the associated target's name.

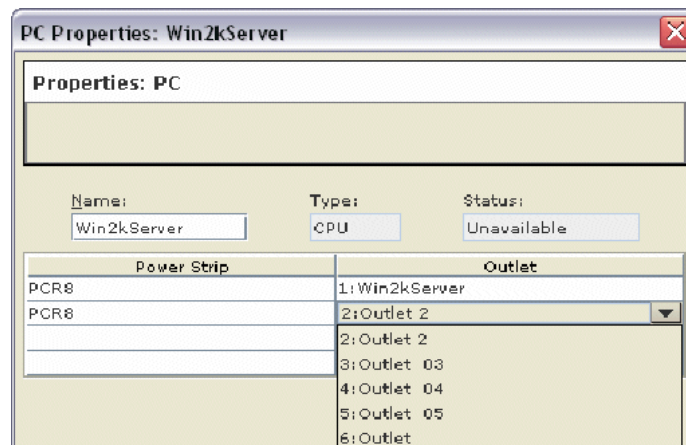
3. RRC for control.
4. Select the target.
5. Select On, Off, or Recycle power from the pop-up menu.
6. See the **KX User Guide** for details.

Associate Outlets with a Target

1. Select target, then select Properties from pop-up menu.
2. Select up to eight Dominion PX units from drop-down list.



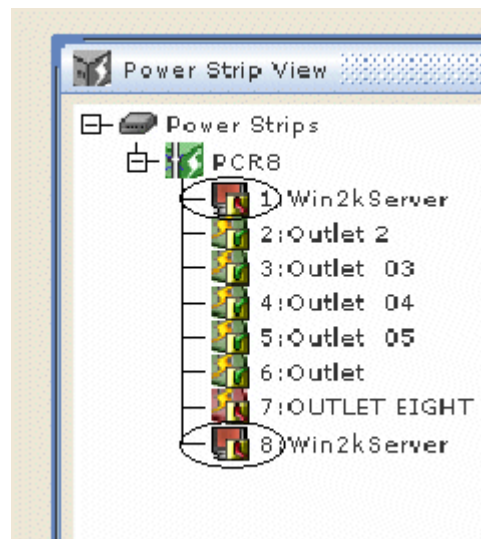
3. Select up to a total of four outlets from the PX units.



4. Notice the target icon change to indicate power.



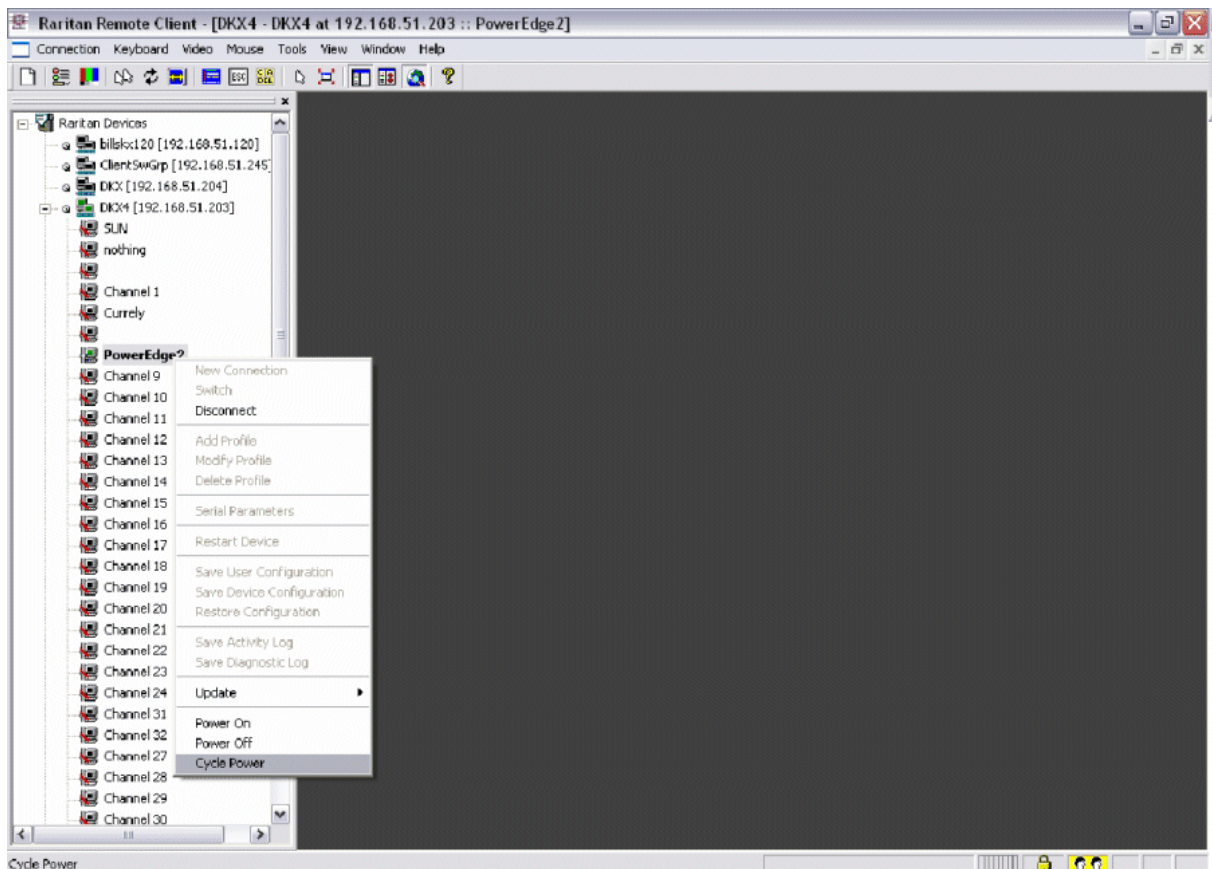
5. Notice the outlet icon change to indicate association.
6. Notice the outlet name automatically changes to the target's name.



Control a Target's Power

1. Select the target associated with outlets.

2. Select from Power On, Power Off, or Cycle Power options.



Dominion KX-II

► **To use the Dominion KX II power control feature:**

1. Connect the Dominion PX to your target server.
2. Name the Dominion PX unit.
3. Associate outlet(s) in the Dominion PX to the target server.
4. Use remote power management of the target server from the Port Access Page.

See the **Dominion KX-II User Guide** for details.

Paragon II

Paragon II use requires P2CIM-PWR and straight CAT5 cable. You can associate up to four outlets to a target; all four outlets can be from separate Dominion PX units, if necessary.

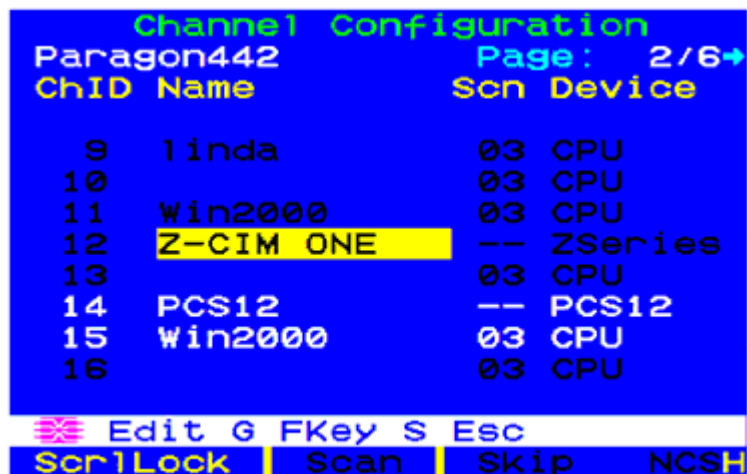
Paragon Manager Application

Use Raritan's Paragon Manager application to configure associations.

1. In Paragon Manager, select the target.
2. Click the target icon and drag-and-drop it on the desired outlets.
3. The outlets will be renamed to the associated target's name.
4. To turn on, turn off, or recycle power to the target, click on the target and press the F3 key; select On, Off, or Recycle power from the drop-down menu.

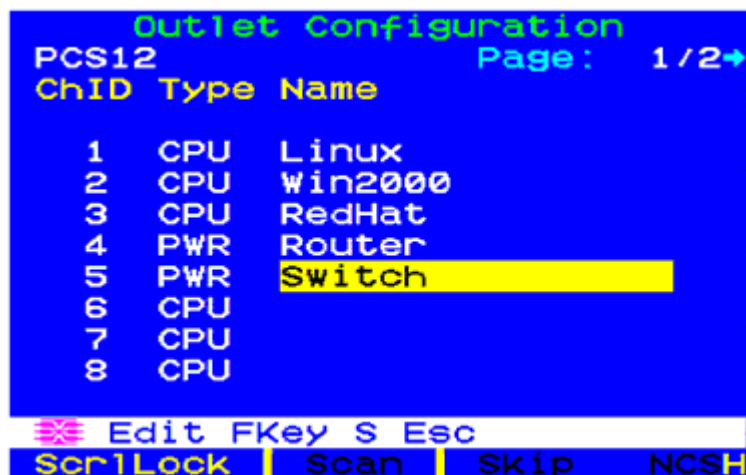
Add a Dominion PX Unit in Paragon II

Add a Dominion PX unit exactly as you would add any second-tier device. Your Paragon II unit auto-detects the Dominion PX and changes the device type to PCR8, PCS12, or PCS20. 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 unit.



Associate Outlets with a Target

On the OSD screen, press the F5 key to enter the Channel Configuration page and select the channel. Press G to enter the special second-tier screen (Outlet Configuration page).



Control a Target's Power

► To control a target's power:

1. From either the Channel Selection by Name OR the Channel Selection menus, press F3 to control power. The message X-Power Off; O-Power On; R-Recycle Power appears on the scrolling help line.
2. If no outlets are associated with the server, the message No power outlets appears.
3. If no permissions to outlets associated with the server exist, the message Permission denied appears.
4. Paragon automatically switches to the channel, so that the server is displayed in the background. If the switch fails, the message Switch fail appears.
5. If the switch is successful, all outlets associated with the server are displayed as shown on the left.
6. Select the outlet and presses X, O, or R:
7. If O, execute on command.
8. If X or R, "Are you sure (yes/no)?" displayed. User must type "yes" (case insensitive) in order for command to execute. Type the full word for command to execute.

Control an Outlet's Power

Use the Channel Selection menus, except for Channel Selection by Name, to navigate to individual Dominion PX ports and control power.

Select an outlet and press X, O, or R:

- If there is no permission to the outlet, the message Permission denied appears.
- If O, executes on command

If X or R, "Are you sure (yes/no)?" displayed. User must type "yes" (case insensitive) in order for command to execute. Typing "Y" or "y" or "ye", etc. is not acceptable. The full word, "yes" must be typed in order for command to execute.

Pressing the Enter key does nothing.

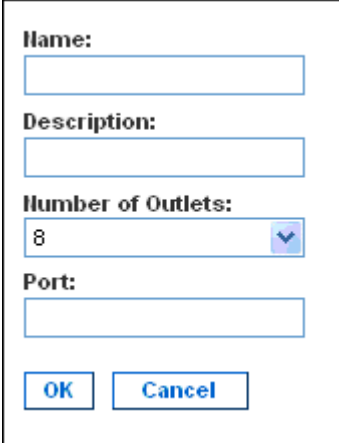
The message X-Power Off; O-Power On; R-Recycle Power should appear on the scrolling help line.

Dominion SX

By connecting to a Dominion SX, you can associate one or more outlets on a Dominion PX unit to specific DSX ports.

Configure a Dominion PX Power Unit on Dominion SX

1. Choose Setup > Power Strip Configuration.
2. Click Add. The Power Strip Configuration screen appears.



The screenshot shows a dialog box titled "Power Strip Configuration". It has four input fields: "Name:" (empty), "Description:" (empty), "Number of Outlets:" (a dropdown menu with "8" selected), and "Port:" (empty). At the bottom, there are two buttons: "OK" and "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.

The screenshot shows the 'Outlet Control' interface. It features a table with 20 rows, each representing an outlet. The table has two columns: 'Outlet' and 'State'. Each row has a checkbox in the 'Outlet' column and a state indicator in the 'State' column. A 'Select All' button is located to the right of the table. At the bottom of the interface, there are three buttons: 'On', 'Off', and 'Recycle'.

Outlet	State
<input type="checkbox"/> Outlet 1	OFF
<input checked="" type="checkbox"/> Outlet 2	OFF
<input type="checkbox"/> Outlet 3	OFF
<input type="checkbox"/> Outlet 4	ON
<input checked="" type="checkbox"/> Outlet 5	OFF
<input type="checkbox"/> Outlet 6	OFF
<input type="checkbox"/> Outlet 7	ON
<input type="checkbox"/> Outlet 8	OFF
<input checked="" type="checkbox"/> Outlet 9	OFF
<input type="checkbox"/> Outlet 10	OFF
<input type="checkbox"/> Outlet 11	OFF
<input type="checkbox"/> Outlet 12	OFF
<input type="checkbox"/> Outlet 13	OFF
<input type="checkbox"/> Outlet 14	OFF
<input type="checkbox"/> Outlet 15	OFF
<input type="checkbox"/> Outlet 16	OFF
<input type="checkbox"/> Outlet 17	OFF
<input type="checkbox"/> Outlet 18	OFF
<input type="checkbox"/> Outlet 19	OFF
<input type="checkbox"/> Outlet 20	ON

Buttons: On, Off, Recycle

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 will appear, indicating successful operation.

Outlet 19: The power operation has been sent.

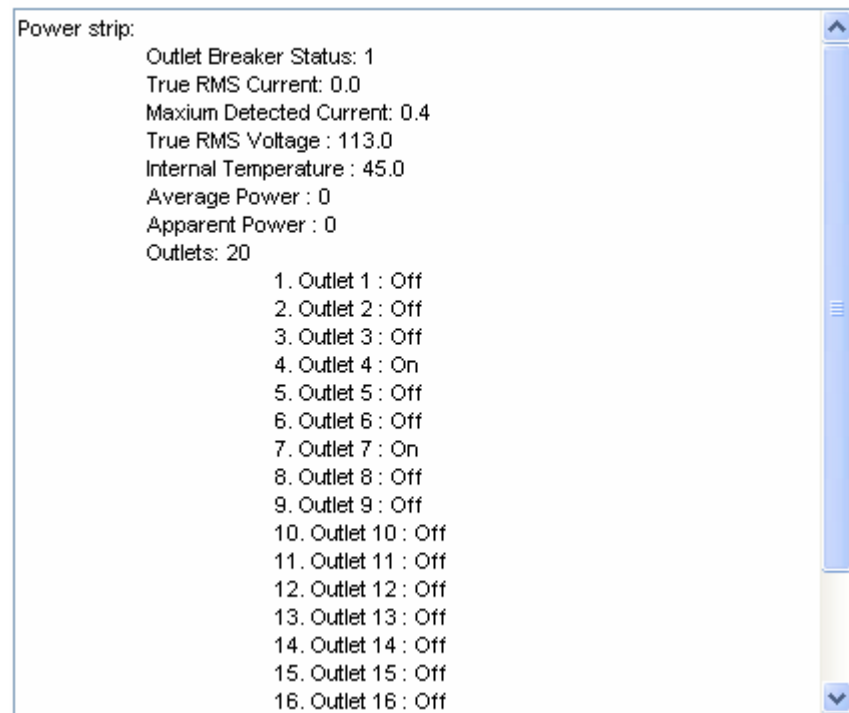
The system shall reflect successful operations shortly.

Figure 1: Outlet Confirmation Screen

Check 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 unit.

Dominion KSX

Support of KSX for Dominion PX is not currently available. However, Dominion PX can be managed as a serial target on one of KSX's serial ports, interacting through CLP interface.

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 while it is integrated with a Raritan product under CC-SG management you should PAUSE MANAGEMENT of the integrated product until the Dominion PX 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 is back online.

Direct Control from CC-SG 4.0

CommandCenter Secure Gateway 4.0 can discover Dominion PX units on the local network and can provide direct control over their outlet states (ON, OFF, and recycle).

Appendix A Equipment Setup Worksheet

Dominion PX Series Unit Model _____

Dominion PX Series Unit Serial Number _____

OUTLET 1	OUTLET 2	OUTLET3
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE
OUTLET 4	OUTLET 5	OUTLET 6
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE
OUTLET 7	OUTLET 8	OUTLET 9
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE
OUTLET 10	OUTLET 11	OUTLET 12
MODEL	MODEL	MODEL

Appendix A: Equipment Setup Worksheet

SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE
OUTLET 13	OUTLET 14	OUTLET 15
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE
OUTLET 16	OUTLET 17	OUTLET 18
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE
OUTLET 19	OUTLET 20	OUTLET 21
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE

OUTLET 22	OUTLET 23	OUTLET 24
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE

Types of adapters

Types of cables

Name of software program

Appendix B Using the CLP Interface

This section explains how to use the Command Line Protocol (CLP) interface to administer a Dominion PX.

In This Chapter

About the CLP Interface	136
Logging into the CLP interface	136
Showing Outlet Information	139
Turning an Outlet On or Off	140
Querying an Outlet Sensor	141

About the CLP Interface

The Dominion PX provides a command line interface that enables data center administrators to perform certain basic management tasks. 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 to the Dominion PX is disabled by default because Telnet transmits in the clear and is insecure. To enable Telnet, choose Device Settings > Network and select the click Enable CLP-Telnet Access checkbox.

Note: About Terminal Emulation Programs - HyperTerminal is available on many Windows OS. But HyperTerminal is not available on Windows Vista. PuTTY is a free program you can download from the internet. see PuTTY's documentation for details on configuration.

The command line interface is based on the Systems Management Architecture for Server Hardware (SMASH) Command Line Protocol (CLP). Using this interface, you can do the following:

- Display the name, power state (on or off), and sensors associated with each Dominion PX outlet
- Turn each outlet on or off
- Display the status of the sensors associated with each outlet

Logging into the CLP interface

Logging in via HyperTerminal and a serial connection is a little different than logging in using SSH or Telnet.

With HyperTerminal

► To log in using HyperTerminal:

1. Connect your PC to the Dominion PX serial port via a serial cable, launch HyperTerminal and open a console window. When the window first opens, it is blank.
2. Press Enter to display a Command 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  
192.168.50.214 command:
```

3. At the Command prompt, type clp and press Enter. You are prompted to enter a login name. The login name is case-sensitive, so make sure you capitalize the correct letters.

```
192.168.50.214 command: clp  
  
Entering character mode  
Escape character is '^]'.  
  
PDU CLP Server (c) 2000-2007  
  
Login: _
```

4. Type a login name and press Enter. You are prompted to enter a password.

```
Login: admin  
Password: _
```

5. Type a password and press Enter. The password is case-sensitive, so make sure you capitalize the correct letters. Once the password is accepted, the clp:/-> system prompt appears.

```
Login: admin
Password:
clp:/->
```

6. You are now logged into the CLP interface and can begin using the interface to administer the Dominion PX.

With SSH or Telnet

► **To log in using SSH or Telnet:**

1. Launch an SSH or Telnet client such as PuTTY and open a console window. A Login prompt appears.

```
login as: █
```

2. Type a login name and press Enter. You are prompted to enter a password.

```
login as: admin
admin@192.168.50.214's password: █
```

3. Type a password and press Enter. The password is case-sensitive, so make sure you capitalize the correct letters. Once the password is accepted, 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:/-> █
```

4. You are now logged into the CLP interface and can begin using the interface to administer the Dominion PX.

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 will be returned as OUTLET1, OUTLET2, and so on. The CLP interface will 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 following shows the output of the show command with no attributes entered.

```
clp:/-> show /system1/outlet7
/system1/outlet7
Properties:
  Name is OUTLET7
  powerState is 1 (on)

Associations:
  CIM_AuthorizedTarget => /system2/authorizedpriv8
  CIM_SystemDevice => /system1
  AssociatedSensor => /system1/ncurrsensor13
  AssociatedSensor => /system1/nsensor33
  AssociatedSensor => /system1/ncurrsensor14
  AssociatedSensor => /system1/nsensor34
  AssociatedSensor => /system1/nsensor35
  AssociatedSensor => /system1/nsensor36
  AssociatedSensor => /system1/nsensor37
```

Example 2 - Name Attribute

The following 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 following 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)
```

Turning an Outlet On or Off

The set command turns an outlet on or off.

Syntax

The following is the syntax for the set command:

```
clp:/-> set /system1/<outlet number> powerState=on|off
```

where the keyword on turns the outlet on and the keyword off turns the outlet off.

Querying an Outlet Sensor

The show command with the Antecedent key word 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.

Appendix C Using SNMP

This Appendix will help you set up 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	142
Configuring SNMP Traps.....	145
SNMP Gets and Sets	146

Enabling SNMP

To communicate with an SNMP manager, you must first enable the SNMP agent on Dominion PX.

1. Choose Device Settings > SNMP Settings. The SNMP Settings window 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 will 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.
4. Select the Enable SNMP v3 Protocol checkbox to enable communication with an SNMP manager using SNMP v3 protocol.
 - Additionally, check Force Encryption to force using encrypted SNMP communication.
1. Type the SNMP MIBII sysLocation value in the System Location field.
2. Type the SNMP MIBII sysContact value in the System Contact field.
3. Click on the link at the bottom of the window to download an SNMP MIB for your Dominion PX to use with your SNMP manager.
4. Click Apply. The SNMP configuration is set.

Configure Users for Encrypted SNMP v3

The SNMP v3 protocol allows for encrypted communication. To take advantage of this, users will need to have a Encryption Phrase, which acts as a shared secret between them and the Dominion PX. This encryption phrase can be set in the User Management page.

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

User Management

Existing Users

Testing1

▼

Refresh

New User Name

Testing1

Full Name

Ron T.

Password

Confirm Password

Use Password as Encryption Phrase ^{*}

SNMP v3 Encryption Phrase

Confirm SNMP v3 Encryption Phrase

Email Address

ront@systemname.com

Mobile Number

User Group

TrialGroup

▼

This user is not blocked and may log in.

Enforce user to change password on next login ^{*}

2. Select the user profile you want to modify from the drop-down list in the Existing Users field.
3. To use the user's password as the Encryption Phrase, select the Use Password as Encryption Phrase checkbox.

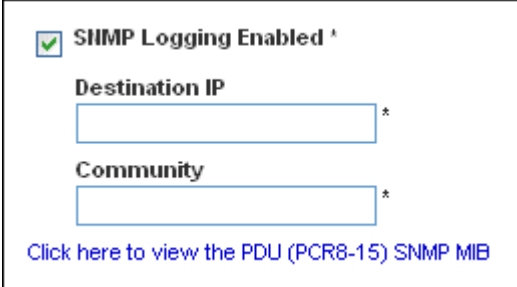
4. To specify a different encryption phrase, deselect this checkbox, type the new phrase in the SNMP v3 Encryption Phrase field, then type it again in the Confirm SNMP v3 Encryption Phrase field.
5. Click Modify. The user is now setup for encrypted SNMP v3 communication.

Configuring SNMP Traps

Dominion PX automatically keeps an internal log of events that occur (see Setting Up Event Logging under the Using the Web interface chapter). These events can also be used to send SNMP traps to a third party manager.

► To configure Dominion PX to send SNMP traps:

1. Choose Device Settings > Event Log. The Event Log Settings window 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 (<device name>) SNMP MIB. It is located under the Community field.

- When SNMP 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	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"/> *

- Click Apply. SNMP logging is configured.
- From the Maintenance tab, select Unit Reset to reset the Dominion PX. You must reset the Dominion PX when enabling SNMP logging or changing the Destination IP address. If you do not, traps will not be 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 will ensure your SNMP manager has the correct MIB for the release you are using.

SNMP Gets and Sets

In addition to sending traps, Dominion PX is able to receive SNMP get and set requests from third-party SNMP managers. Get requests can be used to retrieve information about the Dominion PX (such as the system location, or the current on a specific outlet). Set requests can be used to configure a subset of this information (such as the SNMP system name).

Valid objects for these requests are limited to those found in the SNMP MIBII System Group and the custom Dominion PX MIB.

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 will reveal 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 Dominion PX. outletCurrent, part of the outletsGroup group describes the current passing through a specific outlet.

Note: When performing an SNMP get, all current values are measured in milliamps (ma). HOWEVER: when performing an SNMP set, all are measured in amps (A).

SNMP Sets and Thresholds

Several of these objects can be configured from the SNMP manager using SNMP set commands. Objects that can be written to will have a MAX-ACCESS level of "read-write" in the MIB. These objects include threshold objects, cause Dominion PX to provide a warning (and send an SNMP trap) when certain parameters are exceeded. See **Setting up Outlets and Power Thresholds** (on page 68) for a description of how thresholds work.

Disabling Switching

Using the SNMP SET command, you can disable the switching of outlet states on your Dominion PX (refer to the Dominion PX MIB for more details). This feature is configurable through SNMP only. Upgrading your Dominion PX's firmware will not affect this setting.

Appendix D 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 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	149
Event Commands	150
LAN Commands	151
Sensor Commands	153
OEM Commands	154
IPMI Privilege Levels	161

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 Privileges Levels** for additional information about IPMI privileges.

info [channel number]

Displays information about the selected channel. If no channel is given it will display 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 will likely not produce "accurate" SEL records for a particular system because they will not be correctly tied to a valid sensor number, but 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 will be 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
- *inc* 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.

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

Command Name	Id
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
```

Dominion PX will ignore this command.

Set Power Set Delay Command

The global power on delay defines how much time has to pass between two power on actions.

Request Data	1	delay in 1/10 seconds the delay is the minimum time after which a receptacle will be 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 1/10 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

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
--------------	---	---

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

Request Data	1	# of group [7 - 5] reserved [4 - 0] group #, valid numbers: 0 - 23, 255
	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	1	# of group [7 - 5] reserved [4 - 0] group #, valid numbers: 0 - 23, 255
Data	2	delay in 1/10 seconds This delay overwrites the global delay for all receptacles in that group. The delay will apply 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 1/10 seconds

Set Receptacle ACL

ACLs define who is authorized to change the state of a receptacle. ACLs will be 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 will be 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	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]
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]

Set Sensor Calibration

Sensor calibration is allowed only for threshold-based sensors that return a sensor reading byte with the Get Sensor Reading Command. Note that not all threshold based sensors have capability to be calibrated.

Request Data	1	Sensor number (ffh = reserved)
	2	Actual sensor reading value Assumes, that at the time this command is executed a calibrated measurement is applied to this sensor.

Request Data	1	Sensor number (ffh = reserved)
Response Data	1	Completion Code 00h - If calibration ok CDh - if sensor can't be calibrated

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 Management	No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No
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

Appendix D: Using the IPMI Tool Set

User/Group Management	No	No	No	No	Yes	Yes
User Group Permissions	No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No

Appendix E 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

Appendix F Specifications

In This Chapter

Environmental Specifications	164
Dominion PX Serial RJ-45 Port Pinouts	164
Dominion PX Feature RJ-12 Port Pinouts	164

Environmental Specifications

Environmental Factor	Threshold
Max Ambient Temperature	40 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
6	DCD	Input	Reserved

Dominion PX Feature RJ-12 Port Pinouts

RJ-12 Pin/signal definition			
Pin No.	Signal	Direction	Description
1	+12V	—	Power (500mA, fuse protected)

2	GND	—	Signal Ground
3	RS485 (Data +)	bi- directional	Data Line +
4	RS485 (Data -)	bi- directional	Data Line -
5	GND	—	Signal Ground
6	1-wire		

Index

<

<predefined event number> • 151

1

1U Products • 5

1U Size • 2

2

2U Products • 5

2U Size • 2

A

A Note About Group Commands • 155

About the CLP Interface • 136

Add a Dominion PX Unit in Paragon II • 126

All Outlets Control • 38

Associate Outlets with a Target • 123, 127

Attributes • 139

authcap <channel number> <max priv> • 149

B

Back Panel • 21

Beeper • 24

Before You Begin • 12

Before You Begin Tool-less Mounting: • 10

Blue LED • 21

C

Change Your Password • 29

Channel Commands • 149

Check Power Strip Status • 130

Circuit Breaker • 24

Circuit Breaker Details Page • 40

Circuit Breaker Status • 36

CommandCenter Secure Gateway • 131

Components of an Alert • 81

Configure a Dominion PX Power Unit on
Dominion SX • 128

Configure Environmental Sensors and
Thresholds • 79

Configure Local Event Log • 93, 95

Configure NFS Logging • 96

Configure SMTP Logging • 97

Configure SNMP Logging • 98

Configure Syslog Forwarding • 98

Configure the Firewall • 16, 51

Configure Users for Encrypted SNMP v3 • 144

Configuring and Using Alert Notifications • 80

Configuring SNMP Traps • 145

Configuring the Dominion PX for Network
Connectivity • 15, 105

Configuring the SMTP Settings • 97, 107

Configuring the SNMP Settings • 108

Connect Environmental Sensors • 76

Connecting the Dominion PX to a Computer •
13, 14

Connecting the Dominion PX to Your Network
• 14

Connection Ports • 20

Control a Target's Power • 124, 127

Control an Outlet's Power • 128

Copy a User Group • 49

Copy a User Profile • 43

Copying a Dominion PX Configuration • 115

Copying Configurations with Bulk
Configuration • 113

Create a Certificate Signing Request • 61

Create a User Group • 46

Create a User Profile • 26, 41

Create Group Based Access Control Rules •
54

Creating Alert Destinations • 82

Creating Alert Policies • 85

Creating Alerts • 87

D

Delete a User Group • 50

Delete a User Profile • 44

Deleting Outlet Group Devices • 119

Direct Control from CC-SG 4.0 • 131

Disabling Switching • 148

Displaying Basic Device Information • 99, 101

Displaying Connected Users • 101

Displaying Model Configuration Information •
101

Dominion KSX • 130

Dominion KX • 122

Dominion KX-II • 125

Dominion PX Feature RJ-12 Port Pinouts •
164

Dominion PX Serial RJ-45 Port Pinouts • 164

Dominion SX • 128

E

Editing or Deleting Outlet Groups • 119
 Enabling Data Retrieval • 109
 Enabling SNMP • 142
 Environmental Sensors • 75
 Environmental Specifications • 164
 Equipment Setup Worksheet • 12, 132
 Event Commands • 150
 Event Types • 163
 Examples • 140

F

file <filename> • 151
 Fill Out the Equipment Setup Worksheet • 12
 For Zero U Models Using L-Bracket • 9
 For Zero U Models Using Tool-less Button
 Mounting • 10
 Force HTTPS Encryption • 50, 60
 Front Panel • 20

G

Gather Information for LDAP Configuration. •
 64
 get <id> ... [<id>] • 153
 Get Group Membership Command • 157
 Get Group Power On Delay Command • 158
 Get Power Cycle Delay Command • 160
 Get Power On Delay Command • 155
 Get Receptacle ACL • 159
 Get Receptacle State Command • 156
 getaccess <channel number> [userid] • 150
 getciphers <all | supported> <ipmi | sol>
 [channel] • 150
 Grouping Outlets Together • 117

H

How to Configure an Alert • 81

I

Identifying Environmental Sensors for
 Mapping • 77
 Identifying Other Dominion PX Units • 116
 info [channel number] • 150
 Install a Certificate • 63
 Installation and Configuration • 12, 51, 103
 Integration • 121
 Introduction • 1
 IPMI Privilege Levels • 161

K

KX Manager Application (Dominion KX-I only)
 • 122

L

LAN Commands • 151
 LED Display • 22
 Line Details Page • 39
 Line Loads Display • 36
 list • 153
 Log In • 26
 Logging into the CLP interface • 136
 Logging into the Web Interface • 26

M

Managing the Dominion PX • 99
 Map Environmental Sensors • 76
 Measurement Accuracy • 25
 Menus • 30
 Modify a User Group • 49
 Modify a User Profile • 44
 Modifying the Communications, Port and
 Bandwidth Settings • 104
 Modifying the LAN Interface Settings • 105
 Modifying the Network Settings • 103
 Monitoring Line and Circuit Breaker Status •
 39

N

Name Outlets • 72, 75
 Naming the Dominion PX • 102, 103
 Navigation Path • 31

O

OEM Commands • 154
 Outlet Grouping • 116
 Outlets • 21
 Outlets List • 37

P

Package Contents • 4
 Paragon II • 125
 Paragon Manager Application • 126
 Power Control • 129
 Power Cord • 21
 Power Cycle an Outlet • 70, 73, 75
 Prepare the Installation Site • 12
 print <channel> • 151
 Product Features • 3

Product Models • 1
Product Photos • 1

Q

Querying an Outlet Sensor • 141

R

Rack Mount Safety Guidelines • 6
Rack-Mounting the Dominion PX • 6
Refresh • 35
Reset to Defaults • 35
Resetting the Dominion PX • 110
Resetting to Factory Defaults • 18, 23
Retrievable Data • 110

S

Safety Guidelines • 2
Sample Alerts • 89
Sample Environmental Alert 1 • 91
Sample Environmental Alert 2 • 92
Sample Outlet-Level Alert • 89
Sample Unit Level Alert • 90
Saving a Dominion PX Configuration • 114
Sensor Commands • 153
set <channel> <parameter> • 152
Set Default Outlet State • 69
Set Dominion PX Thresholds • 70, 75
Set Group Membership Command • 157
Set Group Power On Delay Command • 158
Set Group State Command • 156
Set Outlet Permissions • 45, 48
Set Outlet Power-Up Sequence • 71
Set Outlet Thresholds • 70, 73, 75
Set Power Cycle Delay Command • 160
Set Power Set Delay Command • 155
Set Receptacle ACL • 159
Set Receptacle State Command • 155
Set Sensor Calibration • 159
Set System Permissions • 44, 46
Set Up User Login Controls • 57
Set User Permissions Individually • 43, 44
setaccess <channel number>
 <userid>[callin=on|off] [ipmi=on|off]
 [link=on|off] [privilege=level] • 150
Setting the Date and Time • 106
Setting Up a Digital Certificate • 60
Setting Up Access Controls • 50
Setting Up Event Logging • 92
Setting Up External User Authentication • 63

Setting Up Outlets and Power Thresholds •
 68, 148
Setting Up RADIUS Authentication • 67
Setting Up User Groups • 45
Setting Up User Profiles • 41
Setup LDAP Authentication • 65
Showing Outlet Information • 139
SNMP Gets and Sets • 146
Specifications • 164
Standard Rack Mounting • 6
Status Messages • 34
Status Panel • 32
Syntax • 139, 141

T

Test Actors • 160
Test Sensors • 160
The Dominion PX MIB • 147
thresh <id> <threshold> <setting> • 154
To Mount • 10
Turn Outlet On or Off • 75
Turning an Outlet On or Off • 140

U

Unavailable Options • 34
Unpack the Dominion PX and Components •
 12
Updating the Firmware • 112
Using SNMP • 142
Using the CLP Interface • 136
Using the Dominion PX • 20
Using the Home Window • 35
Using the IPMI Tool Set • 149
Using the Web Interface • 26, 30

V

View Internal Event Log • 95
View Outlet Details • 74
View Sensor Readings • 80
Viewing and Controlling Outlet Groups • 118

W

With HyperTerminal • 137
With SSH or Telnet • 138

Z

Zero U Products • 4
Zero U Size • 1

▶ **U.S./Canada/Latin America**

Monday - Friday
8 a.m. - 8 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: +81-3-3523-5994
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 p.m. GMT+1 CET
Phone: +49-20-17-47-98-0

▶ **Korea**

Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +82-2-5578730

▶ **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: tech.rap@raritan.com