



# Dominion® PX

## User Guide Release 1.1.0

Copyright © 2008 Raritan, Inc.  
DPX-0G-E  
March 2008  
255-80-6080-00

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.



# Safety Guidelines

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

SYSTEMS SHOULD ONLY BE CONFIGURED BY A COMPETENT 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.

## Product Models

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	iii
-------------------	-----

---

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

---

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

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

---

Rack Mount Safety Guidelines .....	6
Tool-less Mounting Instructions.....	8
Before Beginning: .....	8
To Mount: .....	9

Chapter 3 Installation and Configuration	10
--	----

---

Before You Begin .....	10
Unpack the Dominion PX and Components .....	10
Prepare the Installation Site .....	10
Fill Out the Equipment Setup Worksheet.....	11
Connect the Dominion PX to a Computer .....	11
Connect the Dominion PX to Your Network.....	12
Configure the Dominion PX for Network Connectivity .....	12
Resetting to Factory Defaults.....	16

Chapter 4 Using the Dominion PX	19
---------------------------------	----

---

Front Panel .....	19
Connection Ports .....	19
Blue LED.....	20

## Contents

Back Panel.....	20
Power Cord .....	20
Outlets.....	21
LED Display .....	22
Circuit Breaker .....	24
Beeper.....	25
Measurement Accuracy .....	25

## Chapter 5 Using the Web Interface 26

---

Logging into the Web Interface .....	26
Logging In .....	26
Changing Your Password .....	30
Using the Web Interface .....	30
Menus .....	31
Navigation Path.....	32
Status Panel.....	32
Status Messages.....	34
Unavailable Options .....	35
Reset to Defaults.....	35
Refresh .....	35
Using the Home Window.....	36
Global Status Panel .....	36
Outlets List .....	37
All Outlets Control.....	38
Setting Up User Profiles .....	39
Creating a User Profile .....	39
Copying a User Profile .....	41
Modifying a User Profile.....	42
Deleting a User Profile.....	42
Setting User Permissions Individually .....	42
Setting Up User Groups.....	43
Creating a User Group .....	44
Setting the System Permissions.....	44
Setting the Outlet Permissions .....	47
Copying a User Group .....	48
Modifying a User Group.....	48
Deleting a User Group.....	49
Setting Up Access Controls.....	49
Forcing HTTPS Encryption.....	49
Configuring the Firewall.....	50
Creating Group Based Access Control Rules .....	53
Setting Up User Login Controls .....	56
Setting Up a Digital Certificate.....	59
Creating a Certificate Signing Request.....	60
Installing a Certificate.....	61

Setting Up External User Authentication.....	62
Settings Up LDAP Authentication.....	63
Setting Up Outlets and Power Thresholds.....	65
Setting the Default Outlet State.....	66
Setting the Dominion PX Thresholds .....	66
Setting the Outlet Power-Up Sequence.....	67
Naming the Outlets.....	69
Setting the Outlet Thresholds.....	70
Viewing Outlet Details .....	71
Power Cycling an Outlet.....	72
Turning an Outlet On or Off.....	72
Environmental Sensors.....	72
Connecting the Environmental Sensors.....	72
Mapping the Environmental Sensors.....	73
Configuring Environmental Sensors and Thresholds.....	74
Viewing Sensor Readings.....	75
Setting Up Alerts .....	76
Configuring Alert Events.....	76
Creating Alert Policies.....	78
Specifying the Alert Destination .....	81
Setting Up Event Logging.....	82
Configuring the Local Event Log.....	83
Viewing the Internal Event Log.....	85
Configuring NFS Logging.....	86
Configuring SMTP Logging.....	87
Configuring SNMP Logging.....	88
Configuring Syslog Forwarding .....	88
Managing the Dominion PX .....	89
Displaying Basic Device Information.....	89
Displaying Model Configuration Information.....	91
Displaying Connected Users .....	91
Naming the Dominion PX.....	92
Modifying the Network Settings.....	93
Modifying the Communications, Port and Bandwidth Settings .....	94
Modifying the LAN Interface Settings .....	95
Setting the Date and Time.....	96
Configuring the SMTP Settings.....	97
Configuring the SNMP Settings.....	98
Resetting the Dominion PX.....	99
Updating the Firmware.....	100
Outlet Grouping .....	102
Identifying Other Dominion PX Units .....	102
Grouping Outlets Together.....	103
Controlling Outlet Groups.....	105
Editing or Deleting Outlet Groups .....	106

## Contents

Deleting Outlet Group Devices .....	106
<b>Chapter 6 Integration</b> .....	<b>107</b>
Dominion KX .....	108
KX Manager Application (Dominion KX-I only) .....	108
Associate Outlets with a Target .....	108
Control a Target's Power .....	110
Dominion KX-II .....	111
Paragon II .....	111
Paragon Manager Application .....	112
Add a Dominion PX Unit in Paragon II .....	112
Associate Outlets with a Target .....	113
Control a Target's Power .....	113
Control an Outlet's Power .....	114
Dominion SX .....	114
Configure a Dominion PX Power Unit on Dominion SX .....	114
Power Control .....	115
Check Power Strip Status .....	116
Dominion KSX .....	116
CommandCenter .....	117
<b>Appendix A Dominion PX Models</b> .....	<b>118</b>
Hardware Specification .....	119
Environmental Specifications .....	120
<b>Appendix B Equipment Setup Worksheet</b> .....	<b>121</b>
<b>Appendix C Using the CLP Interface</b> .....	<b>125</b>
About the CLP Interface .....	125
Logging into the CLP interface .....	126
Using HyperTerminal .....	126
Using SSH or Telnet .....	127
Showing Outlet Information .....	127
Syntax .....	128
Attributes .....	128
Examples .....	129
Turning an Outlet On or Off .....	130
Syntax .....	130



Querying an Outlet Sensor.....	130
<b>Appendix D Using SNMP</b>	<b>131</b>
Enabling SNMP .....	132
Configuring Users for Encrypted SNMP v3.....	134
Configuring SNMP Traps.....	135
SNMP Gets and Sets.....	136
The Dominion PX MIB .....	137
<b>Appendix E Using the IPMI Tool Set</b>	<b>139</b>
Channel Commands.....	139
authcap <channel number> <max priv> .....	139
info [channel number] .....	140
getaccess <channel number> [userid].....	140
setaccess <channel number> <userid>[callin=on   off] [ipmi=on   off] [link=on   off]	
[privilege=level].....	140
getciphers <all   supported> <ipmi   sol> [channel] .....	141
Event Commands .....	141
<predefined event number>.....	141
file <filename>.....	142
LAN Commands.....	142
print <channel> .....	142
set <channel> <parameter>.....	143
Sensor Commands.....	144
list .....	144
get <id> ... [<id>] .....	144
thresh <id> <threshold> <setting> .....	145
OEM Commands .....	145
Set Power Set Delay Command.....	146
Get Power On Delay Command .....	146
Set Receptacle State Command .....	146
Get Receptacle State Command .....	147
Set Group State Command .....	147
Set Group Membership Command.....	148
Get Group Membership Command.....	148
Set Group Power On Delay Command.....	149
Get Group Power On Delay Command .....	149
Set Receptacle ACL .....	150
Get Receptacle ACL .....	150
Set Sensor Calibration.....	151
Test Actors.....	151
Test Sensors.....	151
Set Power Cycle Delay Command.....	151

**Contents**

Get Power Cycle Delay Command .....	152
IPMI Privilege Levels .....	152
Appendix F Event Types	153
<hr/>	
Appendix G Specifications	155
<hr/>	
Index	157
<hr/>	

# 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 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.

Refer to *Appendix A* (see "Dominion PX Models" on page 118) for a list of Dominion PX models.

---

## Product Photos

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

Product Photos

---

Zero U Size



---

1U Size



---

## 2U Size



---

## Product Features

All models and sizes of the Dominion PX provide the following features:

- 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

RMS Voltage

Active Power

Apparent Power

## Package Contents

- 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 configure and set values through SNMP, including unit and outlet threshold levels.
- 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, CommandCenter Secure Gateway (CC-SG), and Dominion solutions

---

## Package Contents

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

---

### Zero U Products

- Dominion PX unit including power cord 1.80m (6 feet)
- 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 1.80m (6 feet)
- 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 1.80m (6 feet)
- 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
Tool-less Mounting Instructions.....	8

---

## Rack Mount Safety Guidelines

In Raritan products which require Rack Mounting, please follow these precautions:

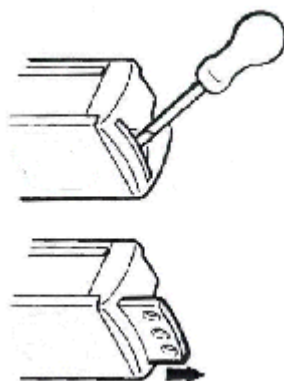
Operation temperature in a closed rack environment may be greater than room temperature. Do not exceed the rated maximum ambient temperature of the appliances (see Appendix A: Specifications).

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.



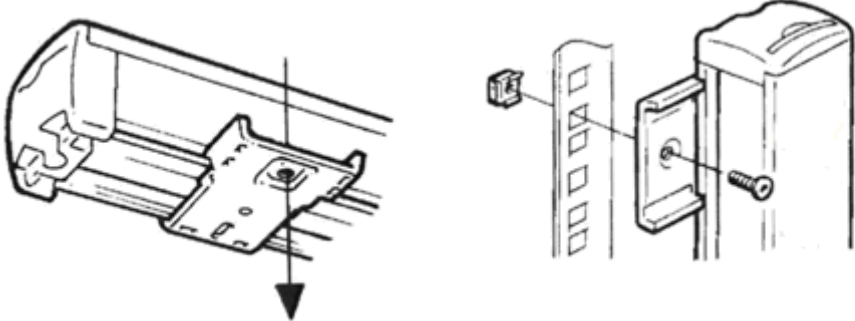
The Zero U units are provided with high grade engineering polycarbonate isolation hardware to allow fixing in a variety of positions within the rack.

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

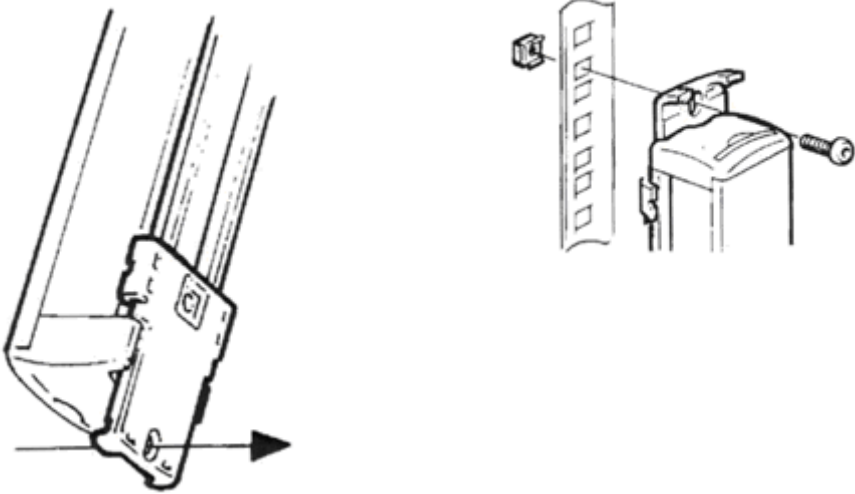
See other options shown below.



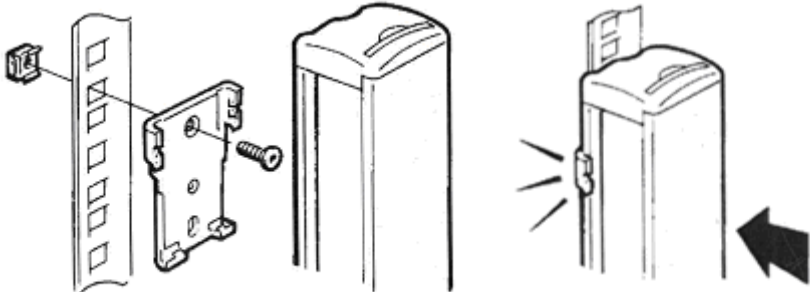
Side Fixing



End Fixing



Blind Fixing



## Tool-less Mounting Instructions

The Zero U units also ship with a tool-less mounting kit consisting of a claw feet with a silver 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 Beginning:

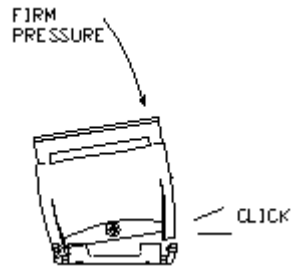
- Ensure that you have sufficient space in the cabinet to mount the Dominion PX. Approximately one inch of clearance is required at each end (top and bottom) of the unit.
- It may help to mark the back of the Dominion PX through the mounting holes you intend to use. You can then use this mark to assist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

---

To Mount:

- Snap fit the claw feet mounts onto the back of the Dominion PX unit. Leave at least 24 inches between the buttons for stability. Once the claw feet are mounted on the Dominion PX rail, they will not readily move—a flat-head screwdriver can be used to remove the feet if they need to be repositioned.
- Align the silver buttons with the mounting holes in the cabinet, and ensure that both buttons can engage their mounting holes simultaneously.
- Press the Dominion PX forward, pushing the silver buttons through the mounting holes, then letting the Dominion PX drop about 5/8ths of an inch. This will secure the Dominion PX in place and complete the installation.

The picture shows how firm pressure is applied to snap fit the claw feet to the Dominion PX Zero-U unit. Hook one side of the product body into one side of a claw foot first, and then apply pressure to snap in the second side.



# 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.....	10
Connect the Dominion PX to a Computer.....	11
Connect the Dominion PX to Your Network .....	12
Configure the Dominion PX for Network Connectivity .....	12
Resetting to Factory Defaults .....	16

---

## Before You Begin

Before beginning the installation, perform the activities listed below:

---

### Unpack the Dominion PX and Components

1. Remove the Dominion PX unit and other equipment from the box in which they were shipped. Refer to "Package Contents" section 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 121). 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.

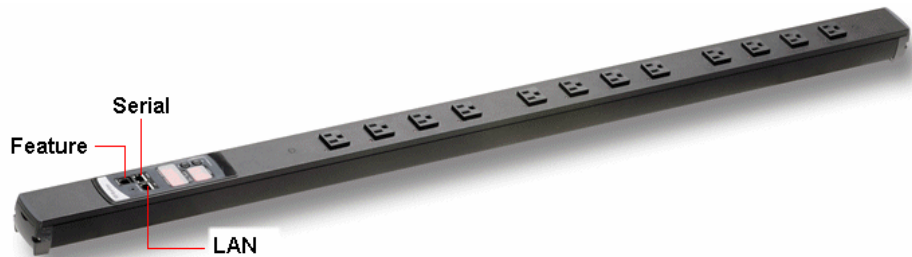
---

### Connect the Dominion PX to a Computer

You must connect the Dominion PX to a computer to configure it. This is done by means of 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 also 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. (Refer to the following pictures for the location of this port on your Dominion PX.)



## Connect the Dominion PX to Your Network



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

---

## Connect 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. (Refer to the pictures shown in *Connect the Dominion PX to a Computer* (on page 11) for the location of this port on your size Dominion PX.)
2. Connect the other end of the cable to your LAN.

---

## Configure 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” for the communications program to 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 **Enter** to display the opening configuration prompt.

```

Welcome!
At the prompt type one of the following commands:
- "clp"      : Enter Command Line Protocol
- "config"   : Perform initial IP configuration
- "unblock"  : Unblock currently blocked users
192.168.0.192 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.

## Configure the Dominion PX for Network Connectivity

---

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, please 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 now. Later on, you can enable the firewall from the Web interface and create firewall rules (refer to "*Configuring the Firewall*" (on page 50)" section for details).

---

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. For now, 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 as shown in the screenshot of Step 3.

## Resetting to Factory Defaults

- 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 as shown in the screenshot of Step 3.
11. If you entered **y** to confirm the configuration, a message is displayed telling you when the configuration is complete. You are then returned to the opening prompt as shown in the screenshot of Step 3. 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, etc.**

---

For security reasons, the Dominion PX may only be reset 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.
  2. Execute the defaults command to reset the DPX to its factory defaults.

## Resetting to Factory Defaults

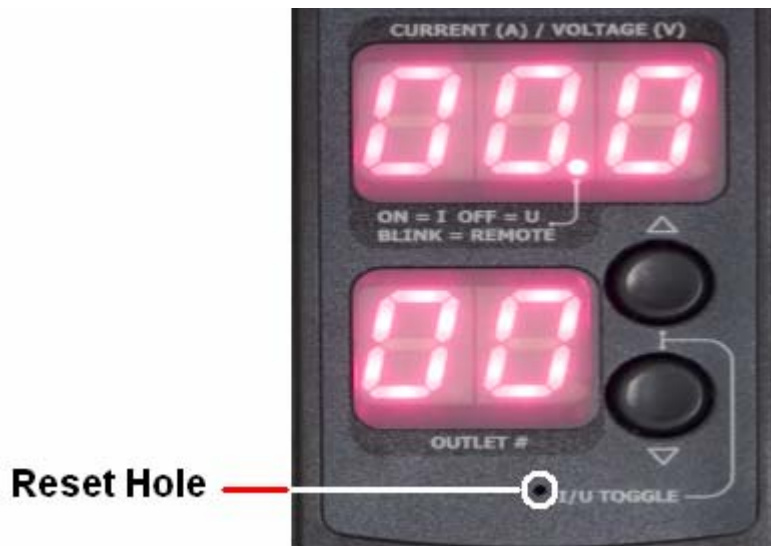
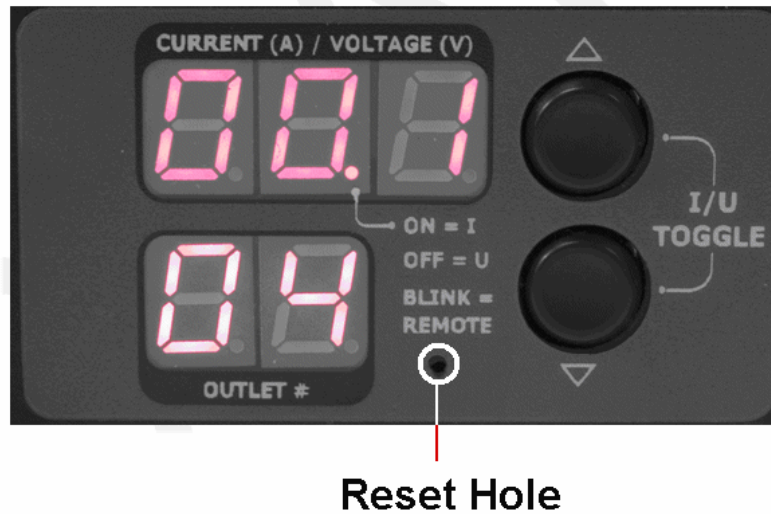
---

Note: Enter "help" to show a list of available command 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. Please refer to PuTTY's documentation for details on configuration.

---

The picture below shows 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 goes off.

## In This Chapter

Front Panel.....	19
Back Panel.....	20
Circuit Breaker .....	24
Beeper.....	25
Measurement Accuracy .....	25

---

## Front Panel

The front panel of the 1U and 2U Dominion PX units consists of a blue LED to the right and three connection ports to the left, while that of the Zero U model consists of 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...
<b>Serial</b>	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.
<b>Feature</b>	For use with Raritan provided environmental sensors.

## Back Panel

<b>LAN</b>	<p>Connecting the Dominion PX to your company's network</p> <p>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.</p> <p>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.</p>
------------	---

---

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

---

### Blue LED

Only 1U and 2U models consist of 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, while the Zero U models consist of no 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. All devices can not 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.
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 will cycle through red, green and yellow. When the software has completed loading, the outlet LEDs will display a steady color and the meter will illuminate.

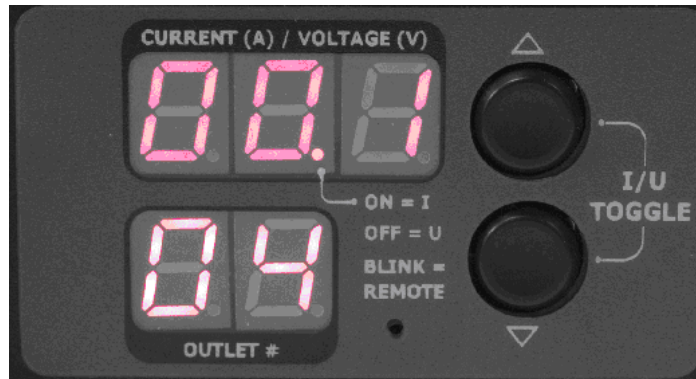
---

## Back Panel

---

### 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 these components:

- A lower row displaying two digits
- An upper row displaying three 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 through this hole when connected to the serial port. Refer to *Resetting to Factory Defaults* (on page 16) section for additional details. Simply pressing on 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.

How to Operate the LED Display

1. Use the **Up** and **Down** buttons to select an outlet. Pressing the **Up** button once moves up one outlet number. Pressing the **Down** button once moves down one outlet number.
2. When an outlet is selected, the outlet number is displayed 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 5 seconds, after which the current will return.
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 is displayed in the format: **X.XX** in volt-amps (**VA**).

## Circuit Breaker

---

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 the current and voltage for the entire Dominion PX unit by using the **Up** and **Down** buttons to select the outlet number **00**. The LEDs do not show the active power for the unit and display --- instead.

---

## 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.....	36
Setting Up User Profiles.....	39
Setting Up User Groups.....	43
Setting Up Access Controls .....	49
Setting Up a Digital Certificate .....	59
Setting Up External User Authentication.....	62
Setting Up Outlets and Power Thresholds.....	65
Environmental Sensors .....	72
Setting Up Alerts.....	76
Setting Up Event Logging .....	82
Managing the Dominion PX.....	89
Outlet Grouping.....	102

---

## 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. (Refer to *“Creating a User Profile* (on page 39)” section for instructions on creating a user profile.)

---

### Logging 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.

## Logging into the Web Interface

3. Click **Login**. The Home window appears.

Overview | Home - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://192.168.43.234/home.asp

Getting Started Latest Headlines http://blog.raleigh.ra... Various latest posts f... Latest topics from "IDS" Latest topics from "E..."

**Raritan.** Power Outlets Alerts User Management Device Settings Maintenance Outlet Groups

Home > Overview Logout

Last Update: 2008-03-10 07:15

**Global Status**

Unit Voltage	RMS Current	Active Power	CPU Temperature
123 Volts	0.00 Amps	0.00 Watts	40 degrees C

Name	State	Control	RMS Current	Active Power	Group Member
Server1 (1)	on	On Off Cycle	0.00 Amps	0.00 Watts	no
Outlet 2 (2)	off	On Off Cycle	0.00 Amps	0.00 Watts	no
Outlet 3 (3)	on	On Off Cycle	0.00 Amps	0.00 Watts	no
Outlet 4 (4)	off	On Off Cycle	0.00 Amps	0.00 Watts	no
Outlet 5 (5)	off	On Off Cycle	0.00 Amps	0.00 Watts	no
Outlet 6 (6)	off	On Off Cycle	0.00 Amps	0.00 Watts	no
Outlet 7 (7)	off	On Off Cycle	0.00 Amps	0.00 Watts	no
Outlet 8 (8)	off	On Off Cycle	0.00 Amps	0.00 Watts	no

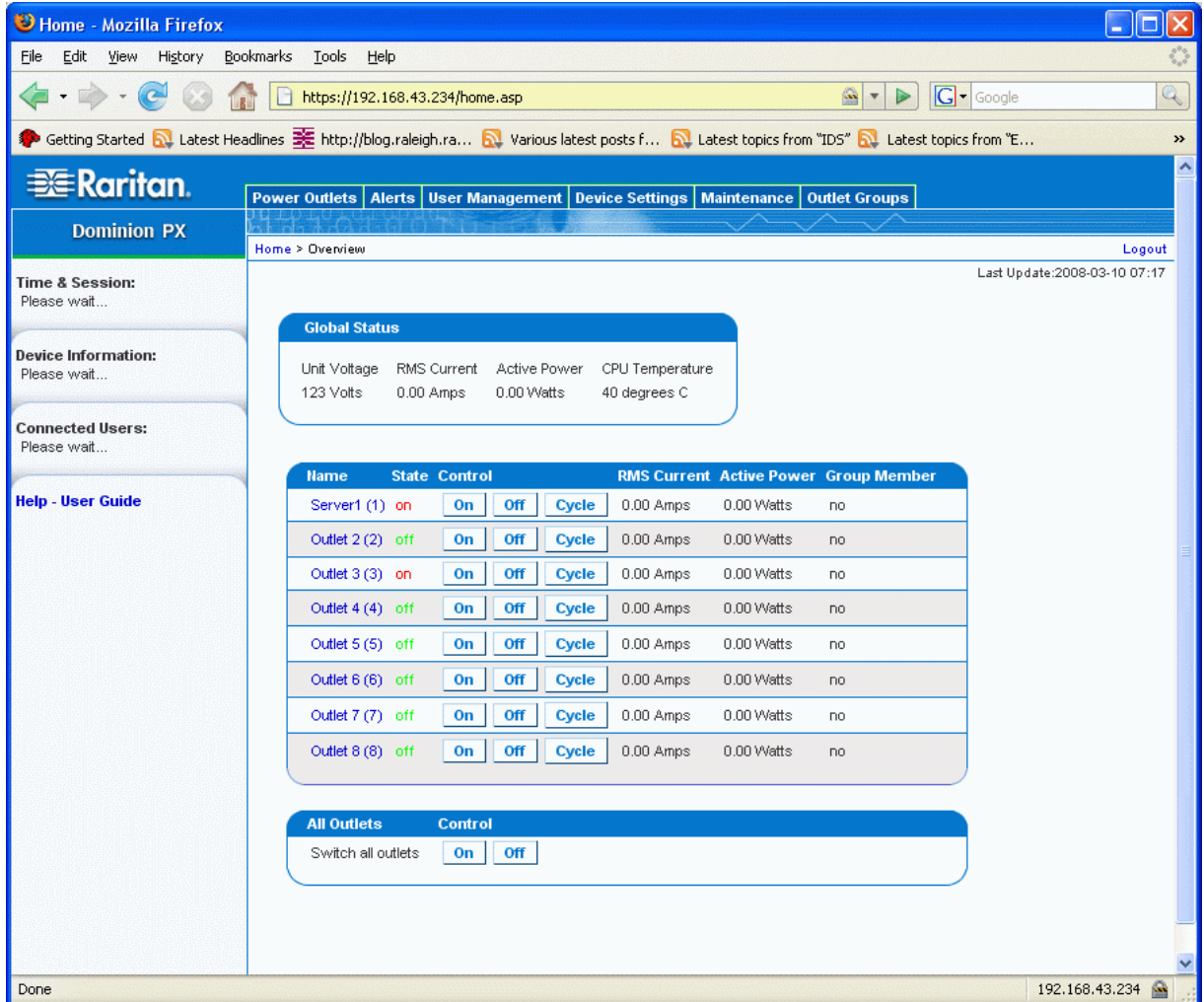
**All Outlets Control**

Switch all outlets

Done 192.168.43.234

Note: The Home window shown above shows 8 outlets. If your Dominion PX has 20 outlets, the Home window will show all 20.

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.

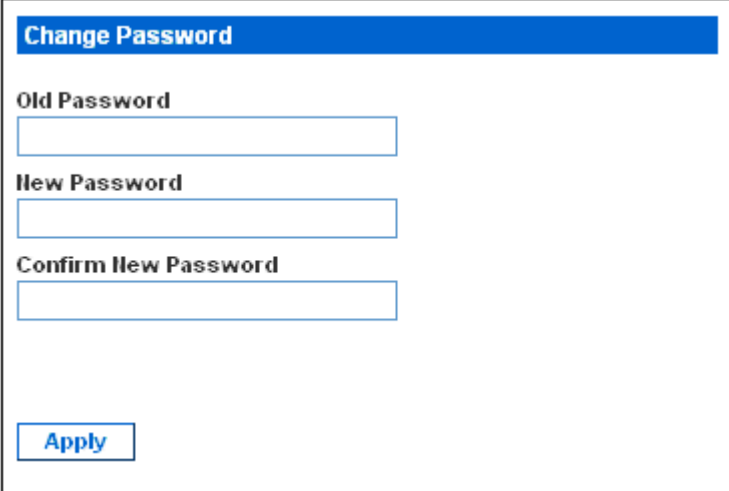


---

### Changing Your Password

To change your password:

1. Choose **User Management --> Change Password**. The Change Password window appears.



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

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, so be sure to capitalize the same letters each time.
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.



---

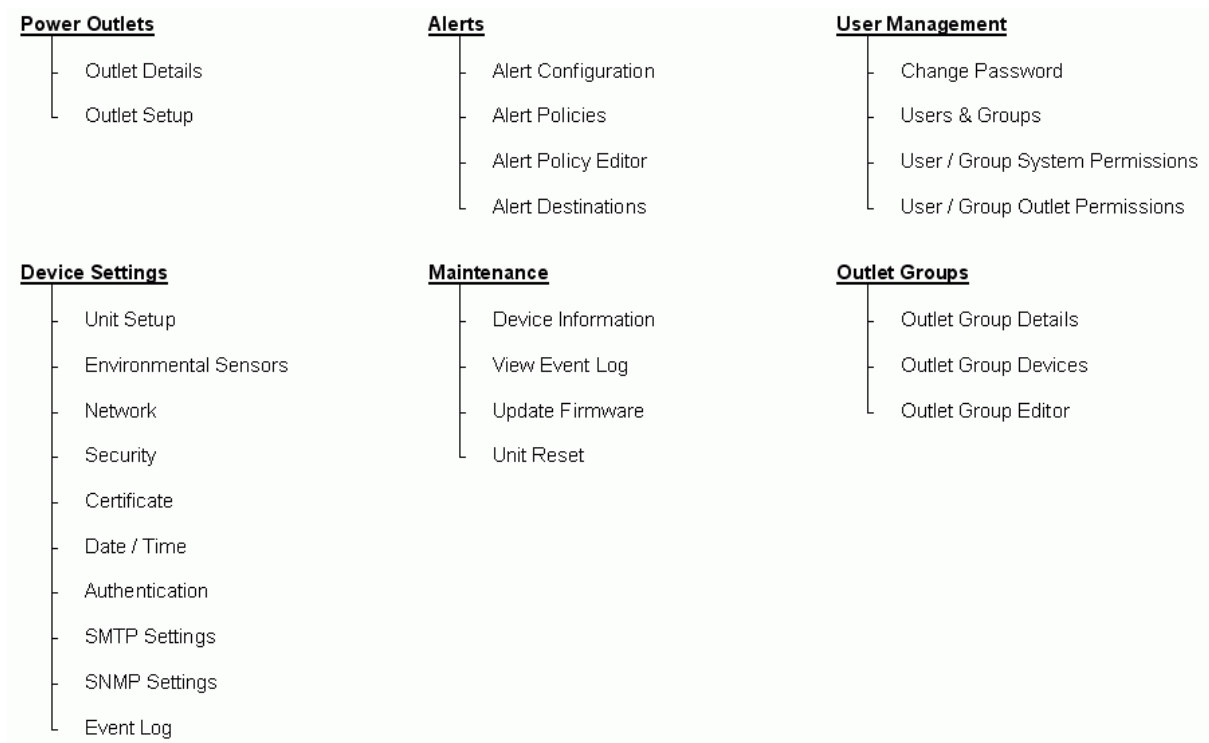
## Menus

There are several menus in the Web interface:

- Power Outlets
- Alerts
- User Management
- Device Settings
- Maintenance
- Outlet Groups

## Options

The following figure shows a complete list of the options available from each menu.



## Using the Web Interface

### How 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 it.
- 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 one shown below.

**Click to return to previous windows**



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.

---

### Status Panel

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

- Current date and time
- Information about the user, including:
  - User name
  - User's current state (active, idle, etc.)
  - 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 current state. Your current session is included in this list.
- A link to the User Guide on the Raritan Website.

The screenshot displays the 'Dominion PX' web interface. It features a blue header with the text 'Dominion PX'. Below the header, there are three main sections: 'Time & Session', 'Device Information', and 'Connected Users'. At the bottom, there is a blue link labeled 'Help - User Guide'.

**Dominion PX**

**Time & Session:**  
2008-03-10 02:24

User : admin  
State : active  
Your IP : 192.168.43.181  
Last Login : 2000-03-29 18:41

**Device Information:**  
Name: my\_device  
Model: PX (PCR8-15)  
IP Address: 192.168.43.234  
Firmware: 01.01.00

**Connected Users:**  
admin (192.168.43.181)  
active

[Help - User Guide](#)

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

If you exceed the idle time limit, you will be logged out, and re-directed to the main login window automatically.

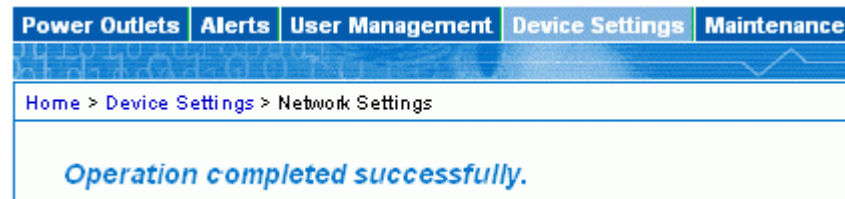
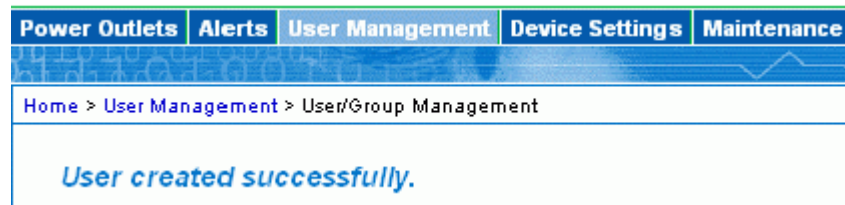
---

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

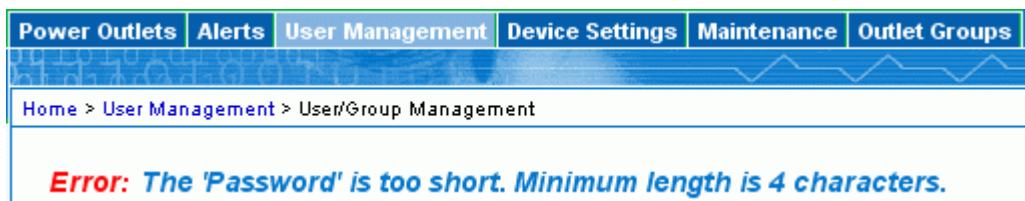
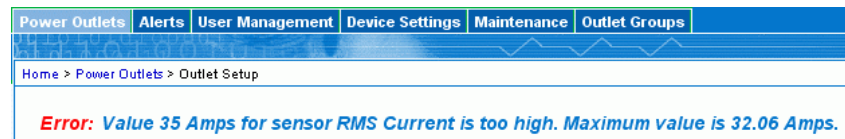
### Successful messages

The following are examples of status messages after an operation has completed successfully:



### Unsuccessful messages

The following are examples of status messages after an operation has completed unsuccessfully:



---

### Unavailable Options

At times, 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 and simply 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. This saves the defaults. If you neglect to do this, 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 **Global Status**, an **Outlets** list, and an **All Outlets Control** panel. The home window also contains an environmental sensors panel, and a time stamp in the top right corner, noting when the data on the screen was last refreshed.

You can return to the Home window from any other window in the Web interface by clicking:

- The **Home** link in the navigation path
- The **Raritan logo** in the upper left of the window
- Device Model Name under the logo

---

### Global Status Panel

The **Global Status** panel provides an overview of the Dominion PX's power consumption and temperature. It shows:

- Unit Voltage
- RMS Current (in Amps)
- Active Power (in Watts)
- CPU Temperature (in degrees Celsius)

Global Status			
Unit Voltage	RMS Current	Active Power	CPU Temperature
123 Volts	0.00 Amps	0.00 Watts	40 degrees C

---

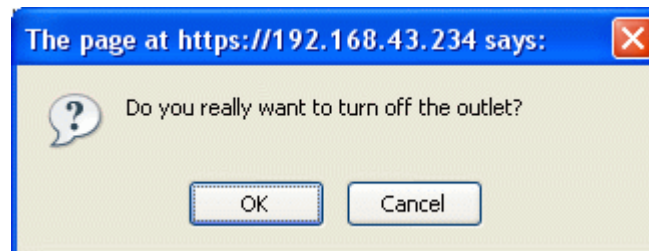
## Outlets List

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
Server1 (1)	on	On	Off	Cycle	0.00 Amps	0.00 Watts	no
Outlet 2 (2)	on	On	Off	Cycle	0.00 Amps	0.00 Watts	yes
Outlet 3 (3)	on	On	Off	Cycle	0.00 Amps	0.00 Watts	no
Outlet 4 (4)	off	On	Off	Cycle	0.00 Amps	0.00 Watts	no
Outlet 5 (5)	off	On	Off	Cycle	0.00 Amps	0.00 Watts	no
Outlet 6 (6)	off	On	Off	Cycle	0.00 Amps	0.00 Watts	no
Outlet 7 (7)	off	On	Off	Cycle	0.00 Amps	0.00 Watts	no
Outlet 8 (8)	off	On	Off	Cycle	0.00 Amps	0.00 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 (refer to Figure 49 for a picture of the window).



### Display Additional Details

To display additional details about an outlet, click the outlet name. This displays the Outlet Details window (refer to Figure 49 for a picture of the window). This window gives the name and status of the outlet, as well as:

- RMS Current
- Power Factor
- Maximum RMS Current
- RMS 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 or voltage 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.

---



---

## Setting Up User Profiles

The Dominion PX is shipped with one user profile built in. This is the Admin profile, which was 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 checking the checkbox labeled **Enable Single Login Limitation**.

---

---

### Creating a User Profile

To create a user profile:

1. Choose **User Management --> Users & Groups**. The User/Group Management window appears. It is divided into a **User Management** panel and a **Group Management** panel.

## Setting Up User Profiles

User Management

**Existing Users**  
 --- select ---

**New User Name**

**Full Name**

**Password**

**Confirm Password**

Use Password as Encryption Phrase <sup>\*</sup>

**SNMP v3 Encryption Phrase**

**Confirm SNMP v3 Encryption Phrase**

**Email Address**

**Mobile Number**

**User Group**  
 --- select ---

Enforce user to change password on next login <sup>\*</sup>

---

Note: Before entering any information in the user profile, please 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...
<b>New user name</b>	The name the user will enter to log into the Web interface
<b>Full Name</b>	The user's first and last names
<b>Password</b> <b>Confirm Password</b>	The password the user will enter to log in. Type it first in the <b>Password</b> field and then again in the <b>Confirm Password</b> field.  The password must be at least four characters long, and spaces are not permitted. The password is case sensitive, so be sure to capitalize the same letters each time.
<b>Email address</b>	An email address where the user can be reached
<b>Mobile Number</b>	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 effectively blocked from accessing any system functions and outlets. (For instructions on setting permissions individually, refer to "*Setting User Permissions Individually*" (on page 42)" section for details.)
5. If you would like this user to set his or her own password, click the checkbox labeled **Enforce user to change password on next login**. 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. Refer to the **Using SNMP** appendix for more details.

---

### Copying a User Profile

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

---

### Modifying a User Profile

Every user with user management permissions can modify a user profile. (Refer to “*Setting the System Permissions* (on page 44)” section for information about setting user permissions.)

To modify a user profile:

1. Choose **User Management --> Users & Groups**. The User/Group Management window appears.
2. Select the user profile you want to modify from the drop-down list in the **Existing Users** field. All the 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.

---

### Deleting a User Profile

To delete a user profile:

1. Choose **User Management --> Users & Groups**. The User/Group Management window appears.
2. Select the user profile you want to delete from the drop-down list in the **Existing Users** field.
3. Click **Delete**. The user profile is deleted.

---


### Setting User Permissions Individually

If you selected None for User Group when creating a user profile, you must set the user's permissions individually. Until you do this, the user is effectively 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 appears (refer to the figure shown in *Setting the System Permissions* (on page 44) section).

2. Select the user from the drop-down list in the **User (not in group)** field. The drop-down list shows all user profiles that have NOT been assigned to a User Group.
3. Set the permissions as necessary. Click this icon  in a field and choose either **Yes** or **No**.
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 appears (refer to the figure shown in *Setting the Outlet Permissions* (on page 47) section).
2. Select the user from the drop-down list in the **User** field.
3. Set the permissions as necessary. Click this icon  in a field and choose either **Yes** or **No**.
4. When you are finished, click **Apply**. The permissions are applied to the user.

---

Note: At least IPMI privilege level "user" is required to switch outlets over IPMI, which causes no effect on web front-end use. However, privilege level has nothing to do with outlet permissions.

---

---

## Setting Up User Groups

The Dominion PX is shipped with one User Group built in. This is 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 enjoy 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.

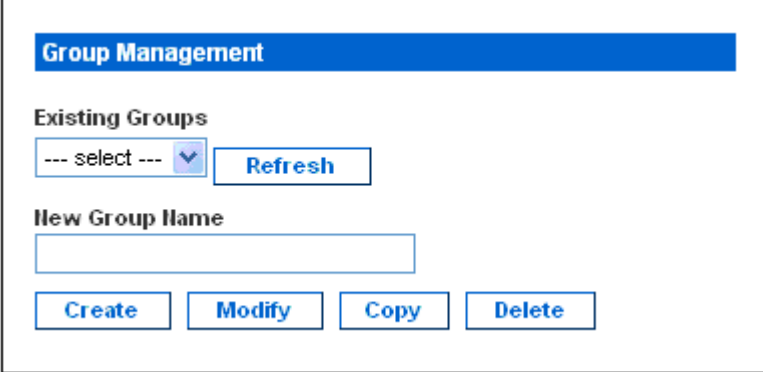
## Setting Up User Groups

---

### Creating a User Group

To create a User Group:

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



The screenshot shows a window titled "Group Management" with a blue header. Below the header, there is a section labeled "Existing Groups" containing a dropdown menu with the text "--- select ---" and a "Refresh" button. Below this 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.

---

### Setting the System Permissions

System permissions include all the 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 appears.

**User/Group System Permissions**

**Show permissions for:**

**User (not in a group)**

**Group**

---

[Setup Outlet Access Permissions](#)

---

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

2. Select the User Group from the drop-down list in the **Group** field. The permissions that apply to this group are displayed. 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 this icon in a field and select either **Yes** or **No**.

## Setting Up User Groups

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.

---



## Setting the Outlet Permissions

Setting outlet permissions allows you to specify which outlets 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 appears.

	Permission
Outlet 1:	No
Outlet 2:	No
Outlet 3:	No
Outlet 4:	No
Outlet 5:	No
Outlet 6:	No
Outlet 7:	No
Outlet 8:	No
Outlet 9:	No
Outlet 10:	No
Outlet 11:	No
Outlet 12:	No
Outlet 13:	No
Outlet 14:	No
Outlet 15:	No
Outlet 16:	No
Outlet 17:	No
Outlet 18:	No
Outlet 19:	No
Outlet 20:	No

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

## Setting Up User Groups

3. Set the permissions as necessary. Click this icon  in a field and select either **Yes** or **No**.
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.

---

---

### Copying a User Group

You can create a new User Group with the exact same permissions as an existing User Group by 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 appears.
2. Select the existing **User Group** from the drop-down list in the **Existing Groups** field.
3. Type the name of the new User Group in the **New Group Name** field.
4. Click **Copy**. A new User Group is created with the same permissions as the existing group. The new User Group can be seen by clicking the drop-down list in the **Existing Groups** field.

---

### Modifying a User Group

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

1. Choose **User Management --> Users & Groups**. The User/Group Management window appears.
2. Select the User Group you want to modify from the drop-down list in the **Existing groups** field. 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.

---

---

### Deleting a User Group

To delete a User Group:

1. Choose **User Management --> Users & Groups**. The User/Group Management window appears.
2. Select the User Group you want to delete from the drop-down list in the **Existing groups** field.
3. Click **Delete**. The User Group is deleted.

---

## Setting Up Access Controls

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

---

### Forcing 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 appears. The panel at the upper left is labeled **HTTP Encryption**.



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

---

Note: Attempts using HTTP will be redirected back to HTTPS automatically, only if the option "Force HTTPS for web access" is checked.

---

---

### Configuring 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 have to enable the firewall, and then you have to set the default policy and create rules specifying which addresses to accept and which addresses to drop. Changes made to firewall rules will 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. Refer to *Installation and Configuration* (on page 10) chapter for details.

---

#### Enable the Firewall

To enable the Dominion PX firewall:

1. Choose **Device Settings --> Security**. The Security Settings window appears. The panel at the upper right is labeled IP Access Control. This controls the firewall.

**IP Access Control**

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

**Enable IP Access Control** \*

**Default policy**

ACCEPT ▾ \*

Rule #	IP/Mask	Policy
<input type="text"/>	<input type="text"/>	ACCEPT ▾

**Append** **Insert** **Replace** **Delete**

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

### Change the Default Policy

Once enabled, the firewall has a default policy built in that accepts traffic from all IP addresses. This means 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 appears. The panel at the upper right is labeled **IP Access Control**. This controls the firewall.
2. Make sure the checkbox labeled **Enable IP Access Control** is checked.
3. The default policy is shown in the **Default Policy** field (refer to the figure shown above ). 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 appears. The panel at the upper right is labeled **IP Access Control**. This controls the firewall.

## Setting Up Access Controls

2. Make sure the checkbox labeled **Enable IP Access Control** is checked.

Action	Do this...
<b>Add a rule to the end of the rules list</b>	<ul style="list-style-type: none"> <li>Type an IP address and subnet mask in the <b>IP/Mask</b> field.</li> <li>Select <b>ACCEPT</b> or <b>DROP</b> in the <b>Policy</b> field.</li> <li>Click <b>Append</b>.</li> </ul> <p>Do NOT enter a rule number. The system automatically numbers the rule.</p>
<b>Insert a rule between two existing rules</b>	<ul style="list-style-type: none"> <li>Type a rule number where you want to insert a new rule above in the <b>Rule #</b> field. For example, to insert a rule between rules #5 and #6, type 6.</li> <li>Type an IP address and subnet mask in the <b>IP/Mask</b> field.</li> <li>Select <b>ACCEPT</b> or <b>DROP</b> from the drop-down list in the <b>Policy</b> field.</li> <li>Click <b>Insert</b>.</li> </ul> <p>The system inserts the rule and automatically rennumbers the rules.</p>
<b>Replace an existing rule</b>	<ul style="list-style-type: none"> <li>Type the number of the rule to be replaced in the <b>Rule #</b> field.</li> <li>Type an IP address and subnet mask in the <b>IP/Mask</b> field.</li> <li>Select <b>ACCEPT</b> or <b>DROP</b> from the drop-down list in the <b>Policy</b> field.</li> <li>Click <b>Replace</b>.</li> </ul> <p>This system replaces the existing rule with the one you just created.</p>

1. When you are finished, the rules are displayed in the IP Access Control panel, as shown below.

**IP Access Control**

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

**Enable IP Access Control** \*

**Default policy**

ACCEPT  \*

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

2. Click **Apply**. The rules are applied.

#### Delete Firewall Rules

To delete a firewall rule:

1. Choose **Device Settings --> Security**. The Security Settings window appears.
2. Make sure the checkbox labeled **Enable IP Access Control** is checked.
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.

#### Creating 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. In effect, 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, you first have to enable the feature. Then, you have to set the default action, specify an IP address range, and associate the rule with a specific User group. Finally, you have to indicate whether the rule will accept or drop traffic. However, 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 appears. The panel labeled **Group based System Access Control** controls this feature.

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

## Setting Up Access Controls

2. Click the checkbox labeled **Enable Group based System Access Control**. 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 appears. The panel labeled **Group based System Access Control** controls this feature.
2. Make sure the checkbox labeled **Enable Group based System Access Control** is checked.
3. Select the action you want from the drop-down list in the **Default Action** field (refer to the figure above).
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 appears. The panel labeled **Group based System Access Control** controls this feature.
2. Make sure the checkbox labeled **Enable Group based System Access Control** is checked.
3. Create or delete specific rules. The following explains how:



Action	Do this...
<b>Add a rule to the end of the rules list</b>	<ul style="list-style-type: none"> <li>Type a starting IP address in the <b>Starting IP</b> field.</li> <li>Type an ending IP address in the <b>Ending IP</b> field.</li> <li>Select a User Group from the drop-down list in the <b>Group</b> field. This rule applies to members of this group only.</li> <li>Select <b>ACCEPT</b> or <b>DROP</b> from the drop-down list in the <b>Policy</b> field.</li> <li>Click <b>Append</b>.</li> </ul> <p>Do NOT enter a rule number. This system automatically numbers the rule.</p>
<b>Insert a rule between two existing rules</b>	<ul style="list-style-type: none"> <li>Type the higher of the two rule numbers in the <b>Rule #</b> field. For example, to insert a rule between rules #5 and #6, type 6.</li> <li>Type a starting IP address in the <b>Starting IP</b> field.</li> <li>Type an ending IP address in the <b>Ending IP</b> field.</li> <li>Select <b>ACCEPT</b> or <b>DROP</b> from the drop-down list in the <b>Action</b> field.</li> <li>Click <b>Insert</b>.</li> </ul> <p>The system inserts the rule and automatically renumbers the rules.</p>
<b>Replace an existing rule</b>	<ul style="list-style-type: none"> <li>Type the number of the rule to be replaced in the <b>Rule #</b> field.</li> <li>Type an IP address and subnet mask in the <b>IP/Mask</b> field.</li> <li>Select <b>ACCEPT</b> or <b>DROP</b> from the drop-down list in the <b>Action</b> field.</li> <li>Click <b>Replace</b>.</li> </ul> <p>This system replaces the existing rule with the one you just created.</p>

- When you are finished, click **Apply**. The rules are applied.

#### Delete Group Based Access Control Rules

To delete a firewall rule:

- Choose **Device Settings --> Security**. The Security Settings window appears.

## Setting Up Access Controls

2. Make sure the checkbox labeled **Enable Group based System Access Control** is checked.
3. Type the number of the rule to be deleted in the **Rule #** field.
4. Click **Delete**. The rule is removed from the **Group based System Access Control** panel.
5. Click **Apply**. The rule is deleted.

---

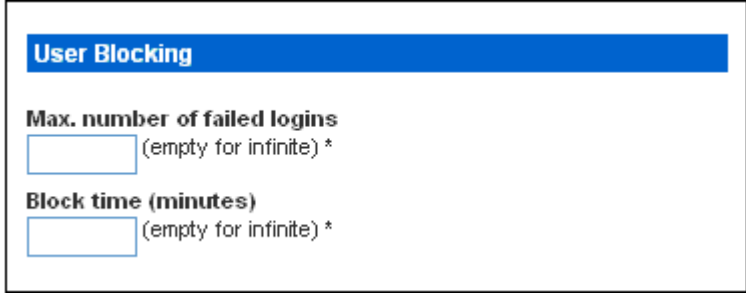
## Setting Up User Login Controls

You can set up login controls to make it more difficult for hackers to access the Dominion PX and the devices connected to it. You can arrange to lock persons out after a specified number of failed logins, limit the number of persons who 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 set it up:

1. Choose **Device Settings --> Security**. The Security Settings window appears. The User Blocking panel controls this feature.



**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 appears. The Login Limitations panel controls this feature.

**Login Limitations**

**Enable Single Login Limitation** ^

**Enable Password Aging** ^

**Password Aging Interval (days)**

\*

2. To prevent more than one person from using the same login at the same time, click the checkbox labeled **Enable Single Login Limitation**.
3. To force users to change their passwords regularly, click the checkbox labeled **Enable Password Aging**, 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. Click **Apply**. The controls are applied.

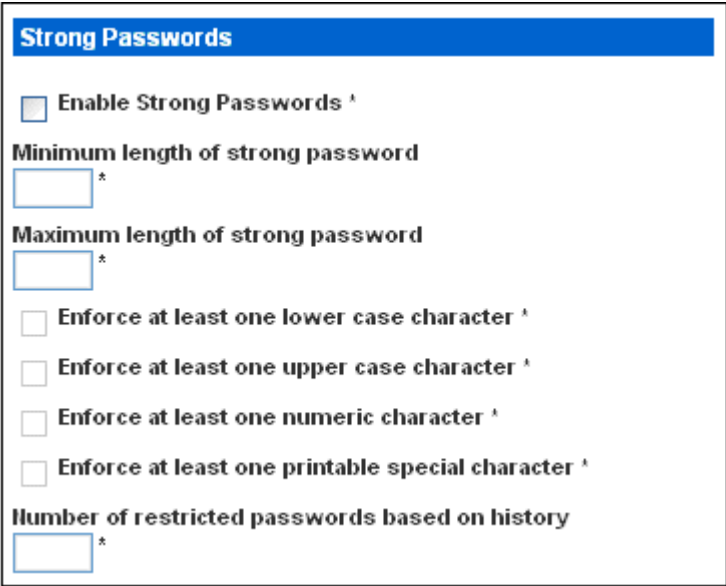
## Setting Up Access Controls

### 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 appears. The Strong Passwords panel appears at the bottom of the window.



**Strong Passwords**

**Enable Strong Passwords** \*

**Minimum length of strong password**  
 \*

**Maximum length of strong password**  
 \*

**Enforce at least one lower case character** \*

**Enforce at least one upper case character** \*

**Enforce at least one numeric character** \*

**Enforce at least one printable special character** \*

**Number of restricted passwords based on history**  
 \*

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

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

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

The purpose of an X.509 digital certificate is to ensure that both parties in an SSL connection are who they say they are. To obtain a certificate for the Dominion PX, you must 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: Refer to *“Forcing HTTPS Encryption (on page 49)”* for instructions on forcing users to employ SSL when connecting to the Dominion PX.

---

---

### Creating 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**

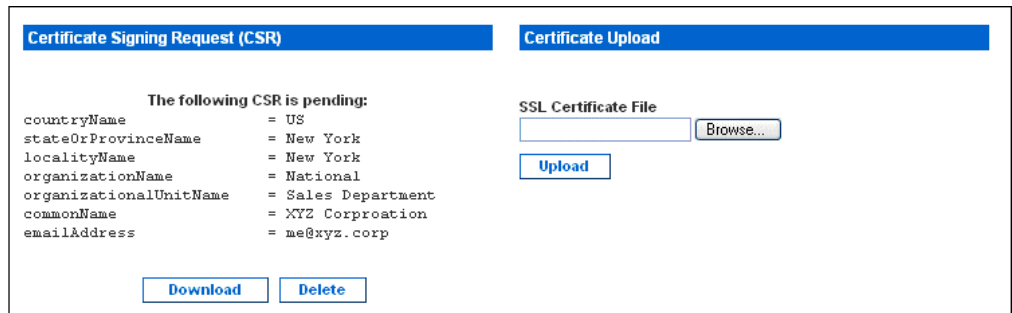
**Key Length (bits)**  
1024  \*

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

Field	Type this...
<b>Common name</b>	The name of your company
<b>Organization unit</b>	The name of your department
<b>Organization</b>	The name of your organization within the department
<b>Locality/City</b>	The city where your company is located

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

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 appears. This window shows the information you entered when creating the CSR.



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

---

### Installing a Certificate

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

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 appears.

## Setting Up External User Authentication

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 have to provide the system with information about the server.

Keep in mind that you still need to create user profiles for users who are authenticated externally. This is 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.



---

## Settings Up LDAP Authentication

To set up LDAP authentication:

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

2. Click the radio button labeled **LDAP**.
3. Type the IP address of the LDAP server in the **User LDAP Server** field.
4. To encrypt traffic to and from the LDAP server, click the checkbox labeled **SSL Enabled**.
5. By default, the Dominion PX uses the standard ports 389 for LDAP and 636 for secure LDAP (SSL). If you prefer to use non-standard ports, change the ports.

---

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

---

## Setting Up External User Authentication

6. 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.
7. Select the type of LDAP server from the drop-down list in the Type of external LDAP server field. Your choices are:
  - Generic LDAP Server
  - Novell Directory Service
  - Microsoft Active Directory
8. Type the following information in the corresponding fields. LDAP needs this information to verify user names and passwords.
  - Login name attribute (also called as “AuthorizationString”)
  - User entry object class
  - User search subfilter (also called as “BaseSearch”)
9. If you selected **Microsoft Active Directory** in Step 6, enter the domain name in the **Active Directory Domain** field.
10. Click **Apply**. LDAP authentication is now in place.

## Setting Up RADIUS Authentication

To set up RADIUS authentication:

1. Choose **Device Settings --> Authentication**. The Authentication Settings window appears. 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:

2. Click the radio button labeled **RADIUS**.
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 the **More Entries** button. 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, keep in mind that you can set up alerts that are triggered whenever any of these thresholds are crossed. Refer to “*Setting Up Alerts* (on page 76)” section for details.

## Setting Up Outlets and Power Thresholds

---

### Setting the Default Outlet State

Sets 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** (refer to **Naming the Outlets**) will override this default state for that outlet. To set this default:

1. Select **Device Settings**, and then select **Unit Setup**. The Unit Setup window appears.

**Unit Setup**

**Default outlet state on device startup**  
Last Known State \*

**Power off period during outlet power cycling**  
10 \* s

**Sequence Delay**  
200 \* ms

**Thresholds**

	lower critical	non-critical	upper non-critical	critical	
RMS Voltage	79 *	81 *	250 *	250 *	Volts
Unit RMS Current			15.0 *	15.0 *	Amps
Board 1 RMS Current			20.0 *	20.0 *	Amps
Temperature	2 *	4 *	85 *	87 *	degrees C

see also: [Model Configuration](#)

Restrict sum of outlet current thresholds to specified hardware limits  
Enabling this feature may cause reshaping of thresholds, you already configured!

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

---

### Setting the Dominion PX Thresholds

To set the Dominion PX thresholds:

Choose **Device Settings** then **Unit Setup**. The Unit Setup window appears.

1. 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 cycling delay 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, if you wish. refer to “*Setting the Outlet Thresholds* (on page 70)” section for more information. You can power cycle an outlet from the Outlet Details window. Refer to “*Power Cycling an Outlet* (on page 72)” section for instructions.

---

2. Type a number of seconds in the field labeled **Sequence Delay** in ms. The default is 200 milliseconds.
  3. Set the RMS voltage, current and temperature thresholds for the unit in the **Thresholds** panel. Enter critical or non-critical threshold for each setting.
  4. When you are finished, click **Apply**. The delays and thresholds are applied.
- 

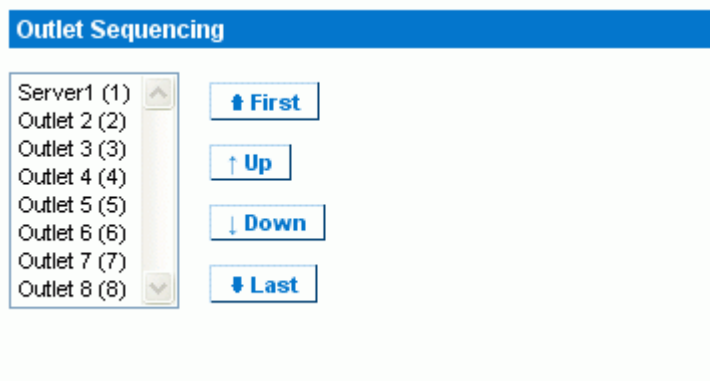
Note: When a large number of outlets are present, especially when dealing with outlets grouped from other Dominion PX Units, you may want to set both the Power off period and the Sequence Delays to lower numbers in order to avoid a long wait before all the outlets are available again.

---

### Setting the 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 do this:

1. Select **Device Settings**, and then select **Unit Setup**. The Unit Setup window appears.



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 options:

## Setting Up Outlets and Power Thresholds

- **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.

---

## Naming the Outlets

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

1. Choose **Power Outlets --> Outlet Setup**. The Outlet Setup window appears.

**Outlet 1 Setup**

**Show setup of outlet**

Server1 (1)

**Outlet Name**

**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	upper	
	critical	non-critical	non-critical critical
RMS Current		1.80	1.80 (max 3.88) Amps

**RMS Current Threshold Summary**

	specified	currently set
Unit	14.68 Amps	12.60 Amps
Board 1	19.68 Amps	12.60 Amps

see also: [Model Configuration](#)

### [\[Outlet 1 Details\]](#)

2. Select the outlet from the drop-down list in the **Show setup of outlet** field.
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 **Unit Setup** page.

## Setting Up Outlets and Power Thresholds

5. Click **Apply**. The new name is applied.

---

### Setting the Outlet Thresholds

To set the current thresholds of an outlet:

1. Choose **Power Outlets --> Outlet Setup**. The Outlet Setup window appears.
2. Select an outlet from the drop-down list in the **Show setup of outlet** field.
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 **Unit Setup** page as a default.

---

Note: You can power cycle an outlet from the Outlet Details window. Refer to "*Power Cycling an Outlet* (on page 72)" section for instructions.

---

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.



---

## Viewing Outlet Details

To display details about a particular outlet:

1. Choose **Power Outlets --> Outlet Details**. The Outlet Details window appears.

**Outlet 1 Details**

Show details of outlet

Server1 (1)

**Outlet Name:** Server1

**Outlet Status:** on

	Value	Status
RMS Current	0.00 Amps	ok
Power Factor	0.035	ok
Maximum RMS Current	0.00 Amps	ok
RMS Voltage	124 Volts	ok
Active Power	0.00 Watts	
Apparent Power	0.00 VA	

[\[Setup\]](#)

2. Select an outlet from the drop-down list in the **Show details of outlet** field. The window shows these details about the outlet:
  - Outlet name
  - Outlet status
  - RMS current, voltage and power readings, including:
    - RMS current
    - Power Factor
    - Maximum RMS Current
    - RMS Voltage
    - Active Power
    - Apparent Power

## Environmental Sensors

---

Note: To display the Outlet Setup window, click the *[Setup]* link. Refer to *Naming the Outlets* (on page 69) section for a picture of the Outlet Setup Window.

---

---

### Power Cycling an Outlet

To turn an outlet off and on:

1. Choose **Power Outlets --> Outlet Details**. The Outlet Details window appears.
2. Select an outlet from the drop-down list in the Show details of outlet field. The outlet must be **ON**.
3. Click **Cycle**. The outlet turns OFF and then back ON.

---

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. Refer to "*Setting the Dominion PX Thresholds* (on page 66)" and "*Setting the Outlet Thresholds* (on page 70)" sections for details.

---

---

### Turning an Outlet On or Off

To turn an outlet on or off:

1. Choose **Power Outlets --> Outlet Details**. The Outlet Details window appears.
2. Select an outlet from the drop-down list in the **Show details of outlet** field.
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.

---

### Connecting the Environmental Sensors

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

### Mapping the 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 do this:

1. Select **Device Settings**, and then select **Environmental Sensors**. The Environmental Sensors window appears. The page will list the logical Temperature and Humidity sensors first.

**Environmental Humidity Sensor 8**

**Name**  
 \*

**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 page will state that "No sensors were detected".
3. For each physical sensor (shown as a row) in the table, click a radio select under the logical sensor (shown as columns) you want to map it to. Dominion PX will now track this sensors readings and will display them 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.

## Environmental Sensors

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.

---

### Configuring Environmental Sensors and Thresholds

To make sensors more useful, you should 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 described above.

#### 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 outlets list and the sensor names will be updated. This updated name will also display 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.

### Viewing Sensor Readings

Mapped sensor readings appear beside the outlets list any time the Home page is displayed. 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. %

---

## Setting Up Alerts

The Dominion PX can be configured to issue an alert whenever a threshold is crossed, either for the Dominion PX unit as a whole or for a specific outlet. The alert can be programmed to send an administrator an email message, or it can be programmed to send a Simple Network Management Protocol (SNMP) trap to a specific IP address.

---

Note: Refer to “*Setting Up Outlets and Power Thresholds* (on page 65)” section for instructions on setting power thresholds.

---

### Configuring Alert Events

Alert events consist of an outlet, an associated threshold, and an associated policy. To configure an alert event:

1. Choose **Alerts --> Alert Configuration**. The Alert Configuration window appears. It shows all existing policies.

**Alert Configuration**

You may want to [adjust outlet sensor thresholds](#) according to your needs.

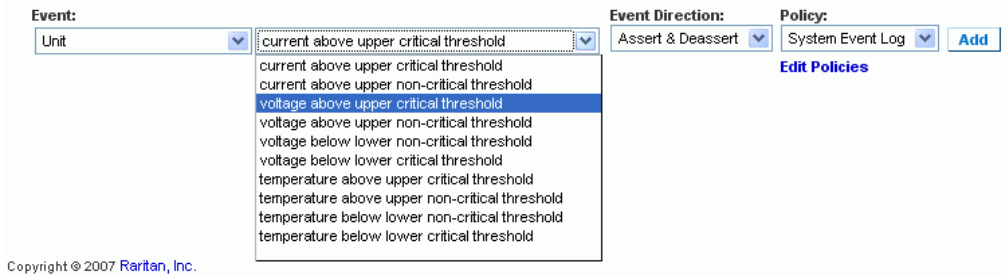
Event	Event Direction	Policy	Destinations	
Outlet 4: current above upper critical threshold	Assert & Deassert	System Event Log	Event Log	<a href="#">Delete</a>
Outlet 6: current above upper critical threshold	Assert & Deassert	System Event Log	Event Log	<a href="#">Delete</a>
Outlet 7: current above upper critical threshold	Assert & Deassert	System Event Log	Event Log	<a href="#">Delete</a>

**Event:**   **Event Direction:**  **Policy:**  [Add](#)

[Edit Policies](#)

2. Go to the **Event** field and select the outlet from the first (left) drop-down list. You can select the Dominion PX unit as a whole or you can select a specific outlet. You can also select an individual relay board, the Environmental Temperature Sensors or the Environmental Humidity Sensors.

3. Select the threshold from the second drop-down list in the **Event** field as shown below. The list of thresholds will vary depending on what was selected in the first drop-down list.



4. Select an **Event Direction** from the third drop-down list.
  - If set to **Assert**, this alert will only trigger when a measured value moves past a critical threshold (either above an upper critical threshold, or below a lower critical one).
  - If set to **Deassert**, this alert will only trigger when a measured value returns to normal from a critical state (either below an upper non-critical threshold, or above a lower non-critical one).
  - If set to **Assert & Deassert**, this alert will trigger when a measured value crosses any threshold state.
1. Select a policy from the drop-down list in the **Policy** field.
2. Click **Add**. The alert is added to the system.

---

Note: No policies appear in this drop-down list until you create them. Refer to “*Creating Alert Policies* (on page 78)” section for instructions.

If an Environmental Temperature or Humidity sensor is selected, an 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.

---

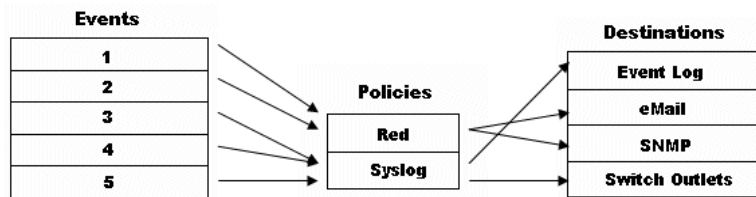
### Creating Alert Policies

Alert policies allow you to associate events with destinations. Policies determine whether specific events trigger an entry in the event log, an email message to an administrator, an SNMP trap, a selected outlet to be switched on/off/cycled, or any combination of the four.

#### About Policies

The diagram below illustrates the way policies associate events with destinations. In this example, five events and two policies are defined.

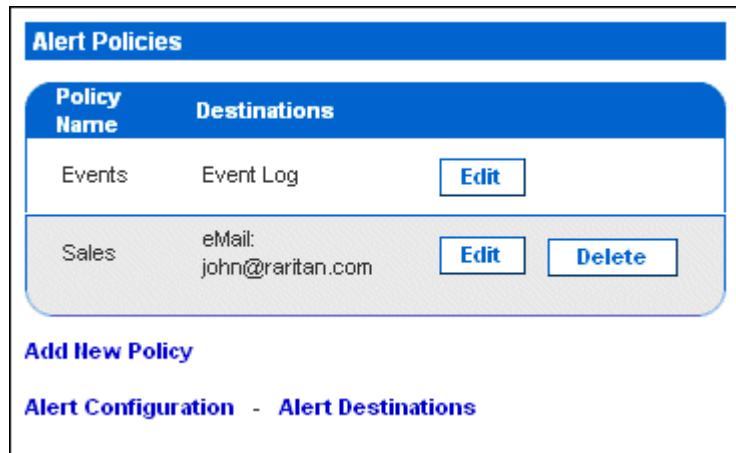
- Events **1** and **2** are associated with the **Red** policy. This means they trigger an email message to an administrator and an SNMP trap.
- Events **3**, **4**, and **5** are associated with the **Syslog** policy. They trigger entries in the event log and selected outlets to be switched, but do not send email messages or traps.



#### Display Existing Policies

To display a list of existing policies:

1. Choose **Alerts --> Alert Policies**. The Alert Policies window appears. It lists each policy and shows their destinations.





2. You can modify or delete a policy by clicking the corresponding button next to the policy. You can add a new policy and configure alerts and destinations by clicking the appropriate link.

Create a Policy

To create a policy:

1. Choose **Alerts --> Alert Policy Editor**. The Alert Policy Editor appears.

**Alert Policy Editor**

Existing Policies  
 --- select --- Refresh

New Policy Name  
 Sales

**Destinations**

System  
 Event Log

eMail  
 john@raritan.com

SHMP  
 192.168.1.1

Switch Outlet Off On Cycle

<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"/>
<input type="checkbox"/>	Outlet 4	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<input type="checkbox"/>	Outlet 5	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<input type="checkbox"/>	Outlet 6	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<input type="checkbox"/>	Outlet 7	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<input type="checkbox"/>	Outlet 8	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<input type="checkbox"/>	Outlet 9	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<input type="checkbox"/>	Outlet 10	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<input type="checkbox"/>	Outlet 11	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<input type="checkbox"/>	Outlet 12	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<input type="checkbox"/>	Outlet 13	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<input type="checkbox"/>	Outlet 14	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<input type="checkbox"/>	Outlet 15	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<input type="checkbox"/>	Outlet 16	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<input type="checkbox"/>	Outlet 17	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<input type="checkbox"/>	Outlet 18	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<input type="checkbox"/>	Outlet 19	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<input type="checkbox"/>	Outlet 20	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Configure System Event Log - Edit Destinations

Create Modify Delete

Alert Configuration - Alert Policies

2. Type a name for the policy in the **New policy Name** field.

## Setting Up Alerts

3. Select the destinations associated with the policy in the Destinations panel. Your choices are **System** (event log), **Switch Outlet**, **eMail**, and **SNMP**.
4. Click **Create**. The policy is created.

### Modify a Policy

To modify a policy:

1. Choose **Alerts --> Alert Policy Editor**. The Alert Policy Editor appears.
2. Select the policy to be modified from the drop-down list in the **Existing Policies** field.
3. Make any necessary changes to the policy's name or destinations.
4. Click **Modify**. The policy is modified.

### Delete a Policy

To delete a policy:

1. Choose **Alerts --> Alert Policy Editor**. The Alert Policy Editor appears.
2. Select the policy to be deleted from the drop-down list in the **Existing Policies** field.
3. Click **Delete**. The policy is deleted.

---

Note: The default alert policy - System Event Log cannot be deleted.

---

---

## Specifying the Alert Destination

The alert destination can be an email address or an SNMP trap. To specify the destination:

1. Choose **Alerts --> Alert Destinations**. The Alert Destinations window appears.

Alert Destinations		
Destination		
Event Log		(read only)
Switch Outlets	Outlets 1 - 20 (Off, On, Cycle)	(read only)
eMail	john@raritan.com	<a href="#">Delete</a>
SNMP	192.168.1.1	<a href="#">Delete</a>

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

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

Note: If you have not configured the Dominion PX's SMTP, a note will appear on this page prompting you to do so now. You cannot enter an email address until you have configured the SMTP server. Either click the SMTP server here link that appears this page, or select **Devices Settings --> SMTP Settings**. Refer to *Configuring the SMTP Settings* (on page 97) section for details.

2. Select the destination from the drop-down list in the **Destination type** field. Your choices are **Event Log**, **Switch Outlets**, **eMail** and **SNMP**.
3. Do one of the following:
  - **Event Log** This is one of the default options for Alert Destination. If you selected this option, event entries are recorded in the event log. This destination is built in by default, and can be neither added nor deleted.
  - **Switch Outlets** This is one of the default options for Alert Destinations. If you selected this option, configured outlet is switched on, off, or cycled. This destination is built in by default, and can be neither added nor deleted.

## Setting Up Event Logging

- **Email** If you selected email, type the receiver's email address.
  - **SNMP** If you selected SNMP, enter the IP address of the trap and the community string.
4. Click **Add**. The destination is added.

---

Note: To delete an alert destination, click the appropriate *Delete* button.

---

---

Note: The Dominion PX is capable of sending out two types of SNMP traps, including: (1) PX-specific traps, which are sent if configured in Event Log setting, while the PDU-MIBs should be self-explanatory. (2) IPMI PET (Platform Event Traps) traps, which are generated in alert configuration and sent out in IPMI-specific formats, containing raw data. 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)

([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

<http://download.intel.com/design/servers/ipmi/PET100.pdf>

(<http://download.intel.com/design/servers/ipmi/pet100.pdf>).

---

## Setting Up Event Logging

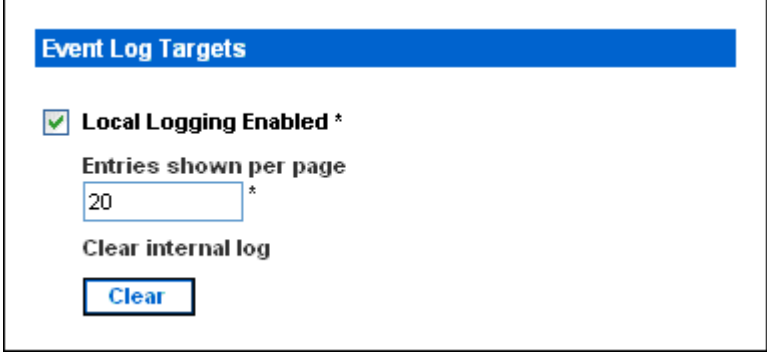
By default, the Dominion PX captures certain system events and saves them in a local (internal) event log. You can expand the scope of the logging to also capture events in the NFS, SMTP, and SNMP logs.

---

## Configuring the Local Event Log

To configure the local event log:

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



The screenshot shows a web interface panel titled "Event Log Targets" with a blue header. Below the header, there is a checked checkbox labeled "Local Logging Enabled \*". Underneath, the text "Entries shown per page" is followed by a text input field containing the number "20" and an asterisk. Below the input field 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, uncheck the checkbox labeled **Local Logging Enabled**.
3. By default, 20 log entries appear on each page of the local event log when it is displayed on your screen. 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 the **Clear** button. The button changes to **Really Clear** and you are prompted to click it only if you really want to clear the log.
  - b. Click **Really Clear** to complete the clear operation, or click **Cancel** to terminate it.

## Setting Up Event Logging

- 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, clear the appropriate check boxes.

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: Refer to the **Event Types** appendix for a more detailed explanation of these event types.

---

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

---

## Viewing the Internal Event Log

To display the internal event log, select Maintenance and then select 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. Refer to “*Configuring the Local Event Log* (on page 83)” section for instructions on changing this number.

---

### Configuring NFS Logging

To configure Network File System (NFS) logging:

1. Choose **Device Settings --> Event Log**. The Event Log Settings window appears. The NFS Logging panel controls NFS logging.

**NFS Logging Enabled** \*

**NFS Server**  
 \*

**NFS Share**  
 \*

**NFS Log File**  
 \*

2. Click the checkbox labeled **NFS Logging Enabled**.
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, check the corresponding checkboxes.

Event Log Assignments		
Event	List	NFS
Outlet Control	<input checked="" type="checkbox"/> *	<input checked="" type="checkbox"/> *
User/Group Administration	<input checked="" type="checkbox"/> *	<input checked="" type="checkbox"/> *
Security Relevant	<input checked="" type="checkbox"/> *	<input checked="" type="checkbox"/> *
User Activity	<input checked="" type="checkbox"/> *	<input type="checkbox"/> *
Device Operation	<input checked="" type="checkbox"/> *	<input checked="" type="checkbox"/> *
Outlet/Unit/Environmental Sensors	<input checked="" type="checkbox"/> *	<input checked="" type="checkbox"/> *
Device Management	<input checked="" type="checkbox"/> *	<input type="checkbox"/> *
Virtual Device Management	<input checked="" type="checkbox"/> *	<input checked="" type="checkbox"/> *

7. Click **Apply**. NFS logging is configured.



---

## Configuring SMTP Logging

To configure Simple Mail Transfer Protocol (SMTP) logging:

1. Choose **Device Settings --> Event Log**. The Event Log Settings window appears. 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. Click the checkbox labeled **SMTP Logging Enabled**.
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, check 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. Refer to "Configuring the SMTP settings (on page 97)" section for instructions.**

---

---

### Configuring SNMP Logging

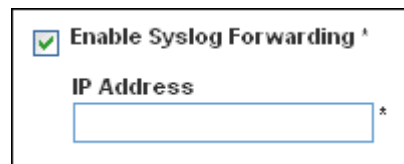
Event logging can be performed by sending SNMP traps to a third-party SNMP manager. Refer to the **Using SNMP** appendix for instructions on enabling SNMP Event Logging on Dominion PX.

---

### Configuring Syslog Forwarding

To configure Syslog Forwarding:

1. Choose **Device Settings --> Event Log**. The Event Log Settings window appears. The Syslog Forwarding panel controls forwarding of system logs.



**Enable Syslog Forwarding** \*

**IP Address** \*

2. Click the checkbox labeled **Enable Syslog Forwarding**.
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, check 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.

---

## 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

1. To display basic information about a Dominion PX unit, choose **Maintenance --> Device Information**. The Device Information window appears.

**Device Information**

<b>Product Name:</b>	PX (PCS20-20L)
<b>Serial Number:</b>	0a72b801bf44cd4e
<b>Control Board Serial Number:</b>	ADB6B00023
<b>Device IP Address:</b>	192.168.80.36
<b>Device MAC Address:</b>	00:0D:5D:01:84:59
<b>Firmware Version:</b>	01.00.00
<b>Firmware Build Number:</b>	5502
<b>Firmware Description:</b>	Standard Edition
<b>Hardware Revision:</b>	0x1A
<b>Relay Board 1 Serial Number:</b>	64
<b>Relay Board 2 Serial Number:</b>	64
<b>Relay Board 3 Serial Number:</b>	64
<b>Relay Board 4 Serial Number:</b>	64
<b>Relay Board 5 Serial Number:</b>	64
<b>Relay Firmware Version:</b>	0x20
<b>Relay Hardware Revision:</b>	0x42 : 0x20

---

[View the datafile for support.](#)

**Model Configuration**

<b>Unit Maximum RMS Current:</b>	20.0 Amps
<b>Board Maximum RMS Current:</b>	16.0 Amps
<b>Outlet Maximum RMS Current:</b>	10.0 Amps
<b>Outlet Current Thresholds Sum Restriction:</b>	disabled

<b>Outlet Mapping</b>	<b>Board</b>
Outlets 1 - 4	1
Outlets 5 - 8	2
Outlets 9 - 12	3
Outlets 13 - 16	4
Outlets 17 - 20	5

**Connected Users**

admin (192.168.80.94) active

2. This 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 link entitled **View the datafile for support**.

---

### 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 appears. Information about your model is shown in the Model Configuration Panel below the Device Information panel. See Figure 64 for details.

This panel shows:

- The unit's and board's maximum RMS current
- The outlet maximum RMS current and current thresholds sum restriction
- The number of outlets mapped to the board

---

### Displaying Connected Users

To display a list of users currently connected to the Dominion PX, choose **Maintenance --> Device Information**. The **Device Information** window appears. A list of connected users is shown in the Connected Users Panel. See the figure shown in *Displaying Basic Device Information* (on page 89) section for details.

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 do this:

1. Choose **Device Settings --> Network**. The Network Settings window appears. 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 (refer to *Installation and Configuration* (on page 10) chapter for details). If necessary, you can modify any of these settings. To do this:

1. Choose **Device Settings --> Network**. The Network Settings window appears. The left side of the window consists of the Basic Network Settings panel, which shows the current network settings. Refer to the figure shown in *Naming the Dominion PX* (on page 92) section for details about this panel.
2. Do one of the following:
  - **Auto configuration** To auto configure the Dominion PX, select DHCP or BOOTP from the drop-down list in the IP Auto Configuration field. If you select DHCP, you can also enter a preferred host name (this is 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.

---

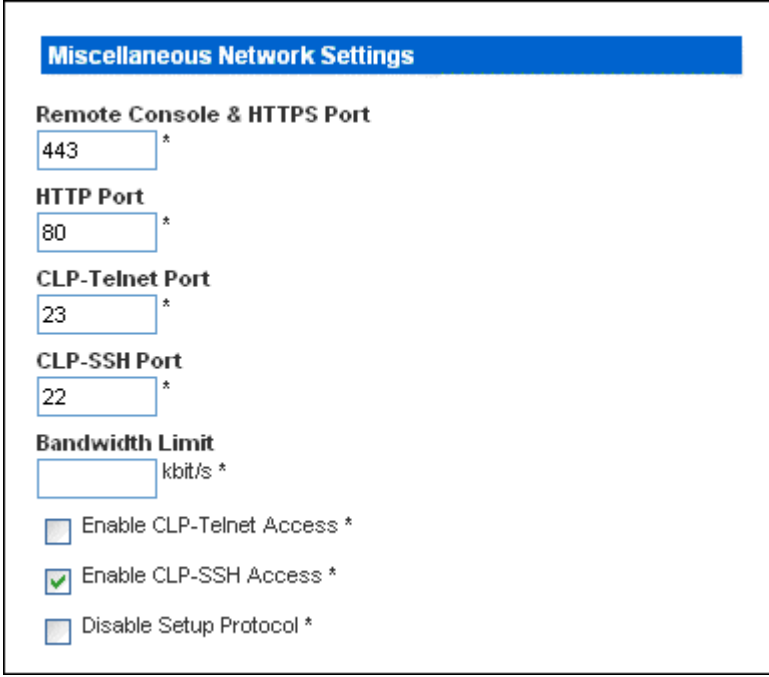
## Modifying the Communications, Port and Bandwidth Settings

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 in the clear and is therefore 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.

To do all this:

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



**Miscellaneous Network Settings**

**Remote Console & HTTPS Port**  
443 \*

**HTTP Port**  
80 \*

**CLP-Telnet Port**  
23 \*

**CLP-SSH Port**  
22 \*

**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, click either check box.
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. Click the check box labeled **Disable Setup Protocol** 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 (refer to for details). To modify either setting:

- Choose **Device Settings --> Network**. The Network Settings window appears. 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 appears.

**Date/Time Settings**

UTC Offset  \*

User specified time \*

**Date**  
 -  -  (yyyy-mm-dd)

**Time**  
 :  :  (hh:mm:ss)

Synchronize with NTP server

**Primary Time Server**  
 \*

**Secondary Time Server**  
 \*

2. Enter a time zone by selecting the appropriate Coordinated Universal Time (UTC) offset from the drop-down list in the **UTC Offset** field (e.g. 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: Refer to “*Setting Up Alerts* (on page 76)” section for instructions on configuring alerts to send emails.

---

1. Choose **Device Settings --> SMTP Settings**. The SMTP Settings window appears.

The screenshot shows two adjacent web interface panels. The left panel, titled "SMTP Settings", contains several input fields: "SMTP Server" with the value "plum.raritan.com", "Sender Email Address" with "stanley.ratner@raritan.com", a checkbox for "SMTP server requires password authentication" which is unchecked, "User Account" (empty), and "Password" (empty). The right panel, titled "Test SMTP Settings", contains a warning message: "Please ensure you have applied all changes before testing SMTP settings or changes will be lost!". Below the message is a "Receiver Address" input field 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.**

---

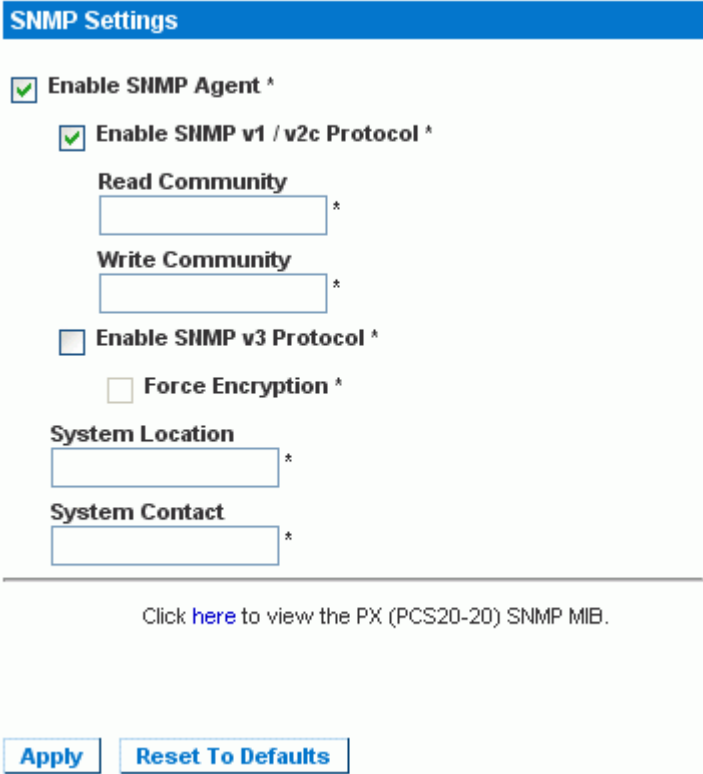
---

## Configuring the SNMP Settings

The SNMP Settings window allows you to enable and disable SNMP communication between an SNMP manager and the PX unit. 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. Select **Device Settings**, and then select **SNMP Settings**. The SNMP Settings window appears.



**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.

2. Check the box for **Enable SNMP Agent** to enable the Dominion PX to communicate with external SNMP managers. A number of options will then become available.
3. Check **Enable 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.

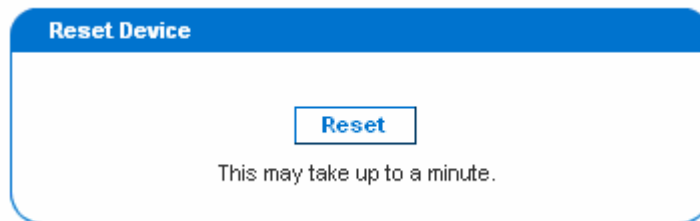
4. Check **Enable SNMP v3 Protocol** to enable communication with an SNMP manager using SNMP v3 protocol.
5. Type the System Location in the **System Location** field.
6. Type the System Contact in the **System Contact** field.
7. Click on the link at the bottom of the window to download an SNMP MIB for your Dominion PX to use with your SNMP manager.
8. Click **Apply**. The SNMP configuration is set.

---

### Resetting the Dominion PX

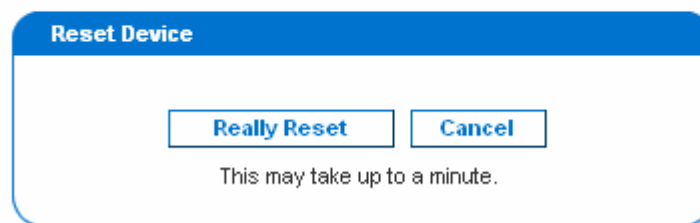
You can use Unit Reset function to reboot the Dominion PX from the Web interface. To do this:

1. Choose **Maintenance --> Unit Reset**. The Reset Operations window appears.



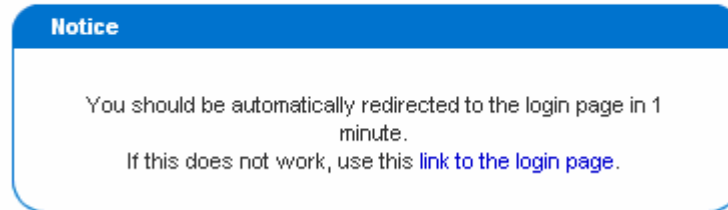
2. Click Reset. A Reset Confirmation window appears.

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



3. By clicking **Really Reset** button, the Dominion PX unit 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 appears and the reset takes place. The reset takes about one minute to complete.

*The device will be reset in a few seconds.*



4. 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.

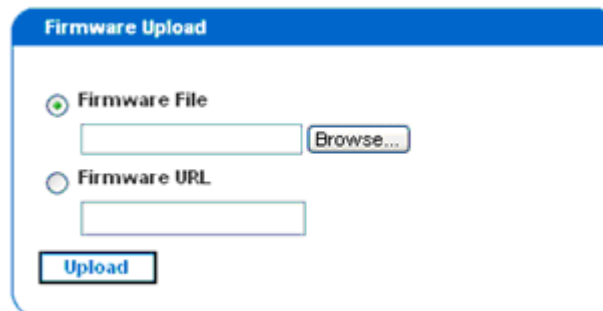
---

### Updating the Firmware

Raritan will notify customers when new firmware is available to update the Dominion PX. Customers will be given instructions where to go to download the new firmware. Once the firmware is downloaded onto a PC, you can install it on the Dominion PX from the Web interface.

To perform a firmware update:

1. Choose **Maintenance --> Update Firmware**. The Firmware Upload window appears.



2. Type the complete path to the firmware file in the Firmware File field, or click **Browse** and select the file.
3. Or in the Firmware URL field, type in an URL link where the firmware file is network-retrievable.

- Click **Upload**. The Firmware Update window appears. It shows the current firmware version and the new firmware version, and gives you a last chance to terminate the update.

**Firmware Update**

<b>Current version:</b>	01.00.00 (Build 5502) / Standard Edition
<b>New version:</b>	01.00.00 (Build 5502) / Standard Edition

Update
Discard

This may take some minutes. Please do NOT power off the device while the update is in progress! After a successful update, the device will be reset automatically.

- 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. Refer to the **Using SNMP** appendix for more information.

---

## Outlet Grouping

Using the Outlet Grouping feature, users 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.

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 do this:

1. Select **Outlet Groups**, and then select **Outlet Group Devices**. The Outlet Group Devices window appears.

Outlet Group Devices

Name	IP Address	Outlets	Model	Status	Access User	
Local Device	127.0.0.1	8	PCR8-15	alive	n/a	<a href="#" style="color: white; text-decoration: none;">Delete</a>
Weaver's PX	192.168.42.98	n/a	n/a	unknown	admin	<a href="#" style="color: white; text-decoration: none;">Delete</a>

**Name:**  **IP Address:**  [Add / Modify](#)

**Username:**  **Password:**  (leave empty for 'Outlet Groups' to use user credentials)

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. Optionally, 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.



5. 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, simply 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 together, in unison, using a control panel from the Dominion PX where the outlet group was created.

To group outlets together:

1. Select **Outlet Groups**, and then select **Outlet Group Editor**. The **Outlet Group Editor** window appears.

**Outlet Group Editor**

**Outlet Groups:**

**Name:**

**Comment:**

**Capabilities:**  
 On  Off  Cycle

**Collection Of Real Outlets:**

Device	Outlets
<b>Local Device</b> 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
<b>Weaver's PX</b> 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

## Outlet Grouping

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.

### 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. Select **Outlet Groups**, then **Outlet Group Details**. The Outlet Groups List appears.

Outlet Groups		
Name	Control	Outlets
<b>Test Box 1</b> (Testing group's server in the first server rack)	<input type="button" value="On"/> <input type="button" value="Off"/> <input type="button" value="Cycle"/>	<input type="button" value="off"/> <input type="button" value="off"/>
<b>Marketing File Server</b> (Purple box in the server rack. Marketing Materials)	<input type="button" value="On"/> <input type="button" value="Off"/> <input type="button" value="Cycle"/>	<input type="button" value="off"/> <input type="button" value="off"/> <input type="button" value="off"/>
<b>Weaver's Test Server</b> (Weaver's new server. temp install. Plugged into both outlet 8s)	<input type="button" value="On"/> <input type="button" value="Off"/> <input type="button" value="Cycle"/>	<input type="button" value="on"/> <input type="button" value="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. Select **Outlet Groups**, and then select **Outlet Group Editor**. The **Outlet Group Editor** window appears.
2. Select the desired outlet group from the drop-down list in the **Outlet Groups** field.
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. Select **Outlet Groups**, and then select **Outlet Group Devices**. The Outlet Group Devices window appears with a list of known Dominion PX units.
2. Click **Delete** for the Dominion PX you want to remove from outlet grouping.

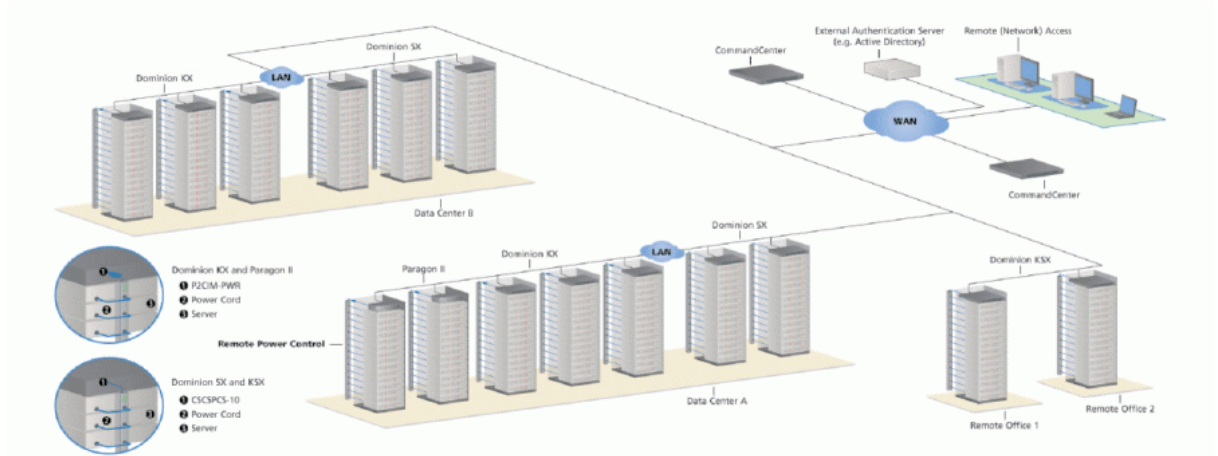
---

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 thru CC Interfaces		Connectivity	Max # of PX units supported	
	Association	Control	Association	Control			
<b>Dominion SX</b>	>= 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	
<b>Dominion KX</b>	KX-I KX Manager KX-II KX GUI	RRC/MPC JAC for KX-II Only	CC GUI	CC GUI	P2CIM-PWR D2CIM-PWR	4 (Increased to 8 in KX1.3)	
<b>Paragon II</b>	<b>UST</b>	<ul style="list-style-type: none"> <li>Paragon Manager</li> <li>OSD</li> </ul>	OSD	IPR + OSD	IPR + OSD	P2CIM-PWR	Max = number of channel ports
	<b>USTIP</b>	<ul style="list-style-type: none"> <li>Paragon Manager</li> <li>OSD</li> </ul>	<ul style="list-style-type: none"> <li>RRC</li> <li>OSD</li> </ul>	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.....	108
Paragon II.....	111
Dominion SX .....	114
Dominion KSX.....	116
CommandCenter .....	117

---

## 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 do this:

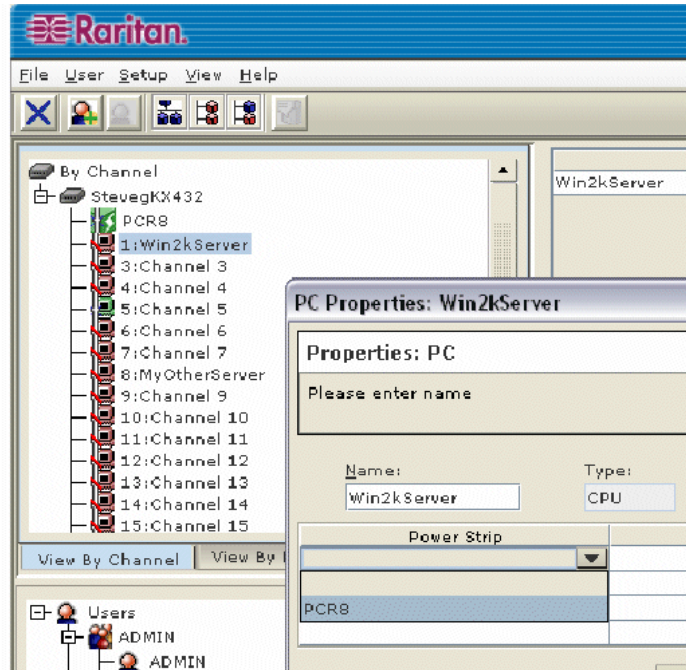
1. Select the target.
2. Edit the **Properties** and choose the outlets to associate. The outlets are automatically renamed to the associated target's name.
3. RRC for control.
4. Select the target.
5. Select On, Off, or Recycle power from pop-up menu.
6. Refer to KX user guide for details.

---

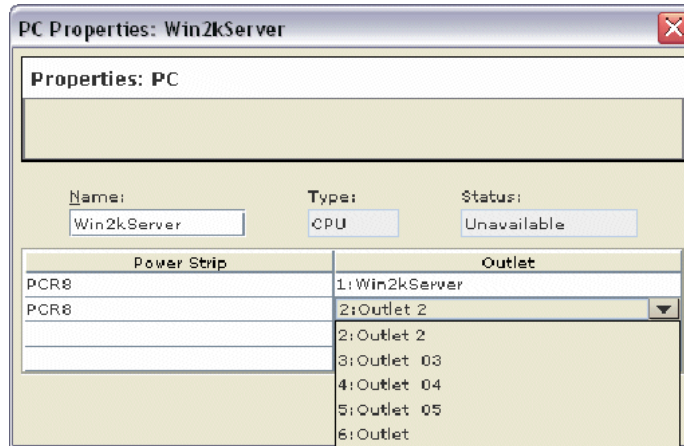
### Associate Outlets with a Target

1. Select target; select Properties from pop-up menu.

2. Select up to eight Dominion PX units from drop-down list.



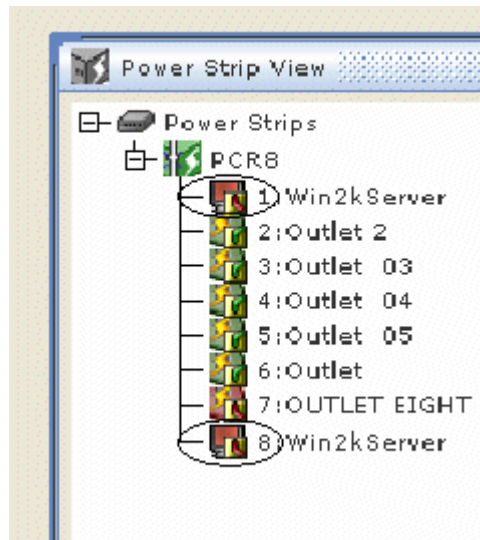
3. Select up to a total of four outlets from the PX units.



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.



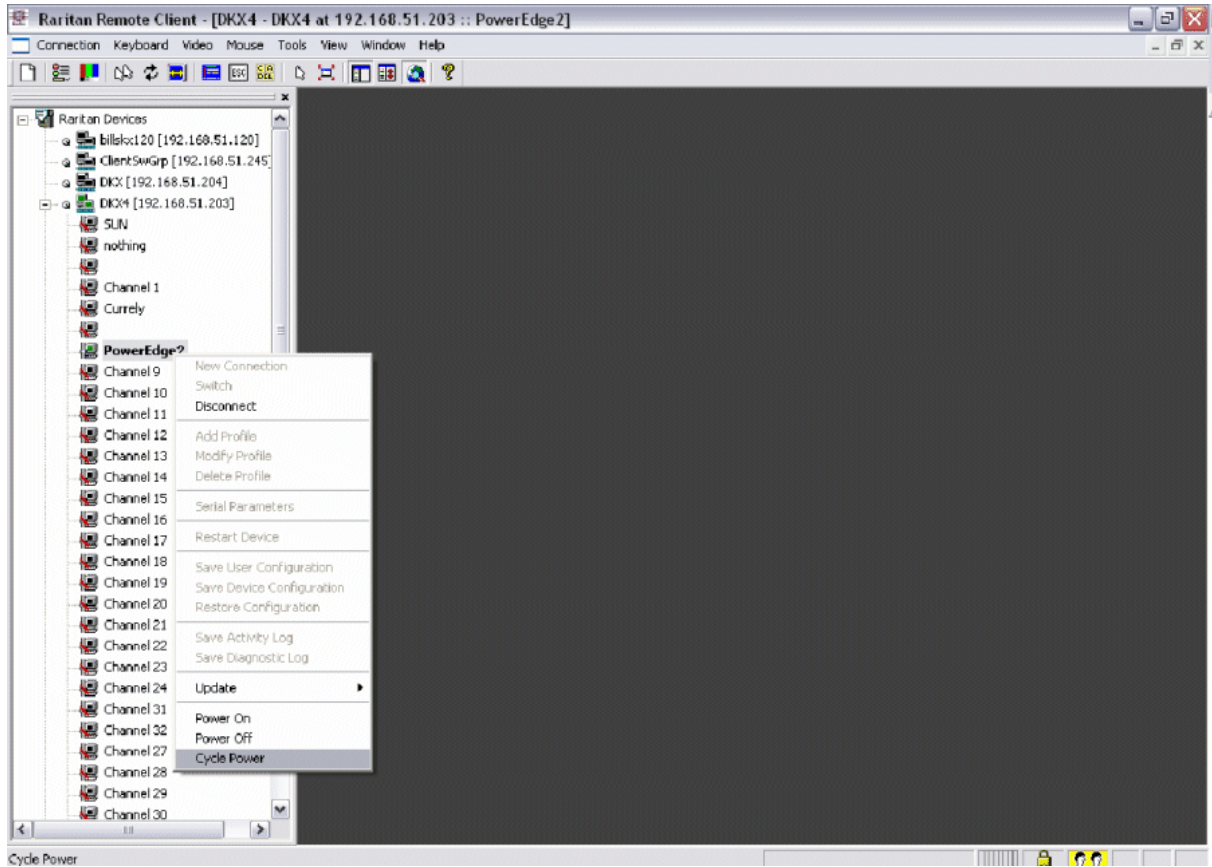
---

### Control a Target's Power

1. Select 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. Utilize remote power management of the target server from the Port Access Page.

Refer to Dominion KX-II user guide for more 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

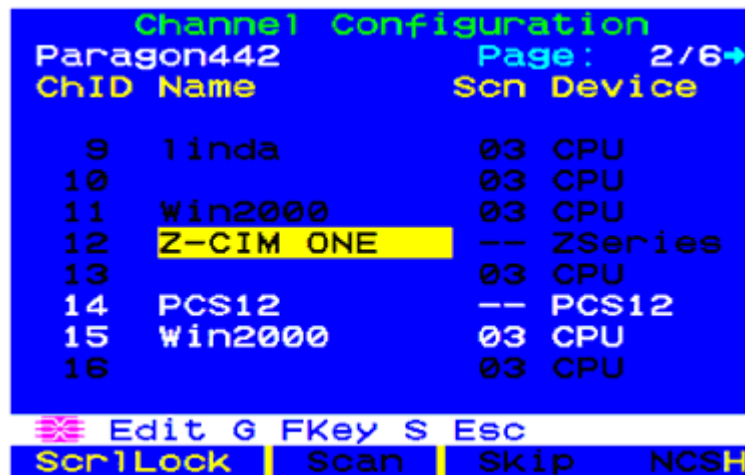
Use Raritan's Paragon Manager application to configure associations:

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 automatically.
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

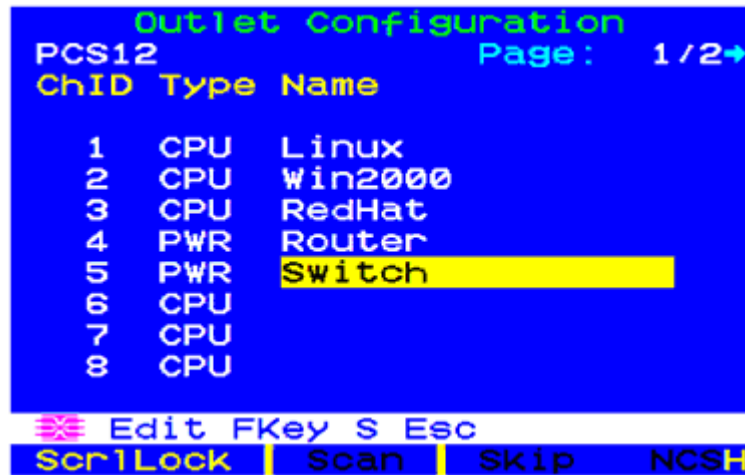
Add a Dominion PX unit exactly as you would add any second-tier device. Your Paragon II unit auto-detects the Dominion PX and changes the device type to PCR8, PCS12, or PCS20. On the OSD screen, press F5 to enter the Channel Configuration page. Select the channel and change the channel name from the default name to an identifying name for the Dominion PX unit.



---

### Associate Outlets with a Target

On the OSD screen, press **F5** 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 "Channel Selection by Name" OR "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 associated with the server, "No power outlets" displayed
3. If no permission to outlets associated with the server, "Permission denied." displayed
4. Else, Paragon automatically switches to the channel, so that the server is displayed in the background. If switch fails, "Switch fail." displays
5. If switch successful, all outlets associated with the server are displayed as shown on the left.
6. User selects 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

When in "Channel Selection" Menu (NOT in "Channel Selection by Name"), users

can navigate to individual Dominion PX ports and control power.

User Selects Outlet and Presses X, O, or R:

- If no permission to the outlet, "Permission denied." displayed
- 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 <ENTER> 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're allowed to 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 drop-down menu in the **Number of Outlets** field.
5. Type the port number in the Port field.
6. Click **OK**.

---

### Power Control

1. Choose **Power Control --> Power Strip Power Control**.
2. The Outlet Control screen appears.

The screenshot shows the 'Outlet Control' window with a table of 20 outlets. Each row contains a checkbox, the outlet name, and its current state. A 'Select All' button is located to the right of the table. At the bottom of the window 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

3. Check the box of outlet number you wish to control, and click On/Off buttons to power on/off the selected outlet(s).

4. A confirmation message will appear to indicate the successful operation.

**Outlet 19: The power operation has been sent.**

**The system shall reflect successful operations shortly.**

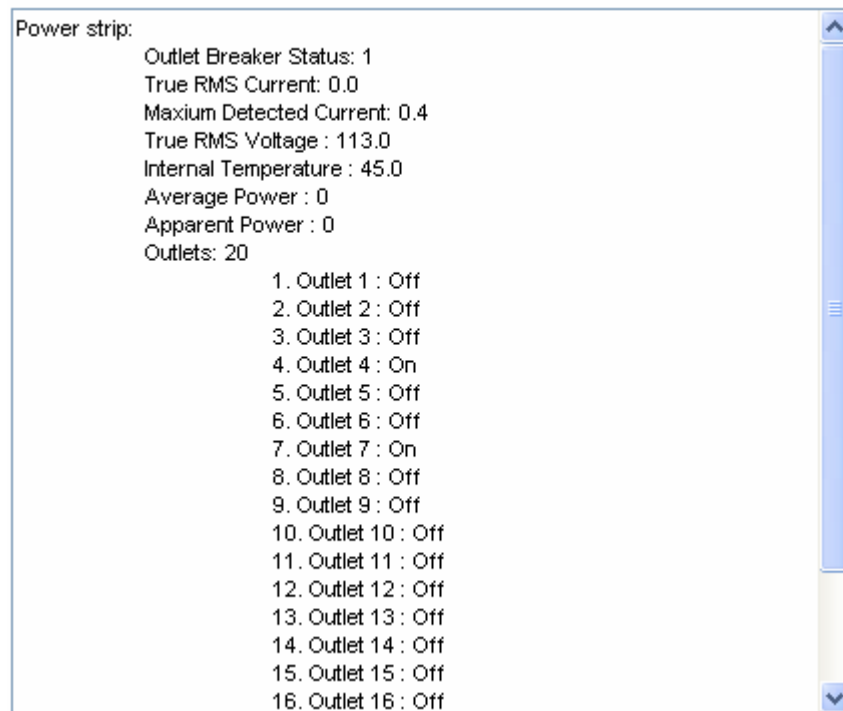
Figure 1: Outlet Confirmation Screen

---

### Check Power Strip Status

1. Choose **Power Control --> Power Strip Status.**

#### DPX Status:



2. A status box appears to display details of the controlled Dominion PX, including power state of each outlet on the unit.

---

## Dominion KSX

Support of KSX G1 for Dominion PX is currently not available at this stage. However, Dominion PX can be managed as a serial target on one of KSX's serial ports, interacting through CLP interface.

---

## CommandCenter

You can manage a Dominion PX from a CommandCenter if it is connected through any of the following Raritan products:

- Dominion SX
- Dominion KX
- Paragon II
- Refer to CC-SG user 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.

---

## Appendix A Dominion PX Models

Model	Rack	V	Current	Outlet Type	# of Outlets	Plug Type	# of Circuit	# of Circuit Breaker
DPCR8-15	1U	120	15	Nema 5-15R	8	Nema 5-15P	1	None
DPCR8A-16	1U	230	16	IEC320 C13	8	IEC60309 16A	1	None
DPCR8A-20L6	1U	208	20	IEC320 C13	8	Nema L6-20P	1	None
DPCS12-20	0U	120	20	Nema 5-15R	12	Nema 5-20P	1	None
DPCS12A-16	0U	230	16	IEC320 C13	12	IEC60309 16A	1	None
DPCS20-20	0U	120	20	Nema 5-15R	20	Nema 5-20P	1	None
DPCS20-20L	0U	120	20	Nema 5-15R	20	Nema L5-20P	1	None
DPCS20-30L	0U	120	30	Nema 5-15R	20	Nema L5-30P	1	2 (dual)
DPCS20A-16	0U	230	16	IEC320 C13	20	IEC60309 16A	1	None
DPCS20A-32	0U	230	32	IEC320 C13	20	IEC60309 32A	1	2
DPCS20A-20L6	0U	208	20	IEC320 C13	20	Nema L6-20P	1	None
DPCS20A-30L6	0U	208	30	IEC320 C13	20	Nema L6-30P	1	2 (dual)
DPCR20-20	2U	120	20	Nema 5-15R	20	Nema 5-20P	1	None
DPCR20-30L	2U	120	20	Nema 5-15R	20	Nema L5-30P	1	2 (dual)
DPCR20A-32	2U	230	32	IEC320 C13	20	IEC60309 32A	1	2
DPCR20A-30L6	2U	208	30	IEC320 C13	20	Nema L6-30P	1	2



Note: Per NEC rules, North American units should be de-rated by 20%. For example, a Dominion PX rated at 30A can provide 24A of current in North America.

Regardless of Dominion PX model, the maximum current load is 10A per outlet.

In This Chapter

Hardware Specification.....119  
 Environmental Specifications.....120

Hardware Specification

Model	weights (lb / kg)	dimensions
DPCR8-15	8.02 / 3.64	17.32" x 6.57" x 1.69"; 440 x 167 x 43mm
DPCR8A-16	8.02 / 3.64	17.32" x 6.57" x 1.69"; 440 x 167 x 43mm
DPCR8A-20L6	8.02 / 3.64	17.32" x 6.57" x 1.69"; 440 x 167 x 43mm
DPCS12-20	7.67 / 3.48	2.24" x 1.95" x 49.33"; 57 x 49.5 x 1,253mm
DPCS12A-16	7.67 / 3.48	2.24" x 1.95" x 49.33"; 57 x 49.5 x 1,253mm
DPCS20-20	11.20 / 5.08	2.24" x 1.95" x 70.71"; 57 x 43 x 1,796mm
DPCS20-20L	11.20 / 5.08	2.24" x 1.95" x 70.71"; 57 x 43 x 1,796mm
DPCS20-30L	11.81 / 5.36	2.24" x 1.95" x 70.71"; 57 x 43 x 1,796mm
DPCS20A-16	11.20 / 5.08	2.24" x 1.95" x 70.79"; 57 x 43 x 1,798mm
PCS20A-32	11.81 / 5.36	2.24" x 1.95" x 70.79"; 57 x 43 x 1,798mm
DPCS20A-20L6	11.20 / 5.08	2.24" x 1.95" x 70.79"; 57 x 43 x 1,798mm
DPCS20A-30L6	11.81 / 5.36	2.24" x 1.95" x 70.79"; 57 x 43 x 1,798mm
DPCR20-20	12.78 / 5.80	17.32" x 3.46" x 10.79"; 440 x 88 x 274mm
DPCR20-30L	13.40 / 6.08	17.32" x 3.46" x 10.79"; 440 x 88 x 274mm
DPCR20A-32	13.40 / 6.08	17.32" x 3.46" x 10.79"; 440 x 88 x 274mm
DPCR20A-30L6	13.40 / 6.08	17.32" x 3.46" x 10.79"; 440 x 88 x 274mm

## Environmental Specifications

---

### Environmental Specifications

Environmental Factor	Threshold
Max Ambient Temperature	40 degrees Celsius

# Appendix B Equipment Setup Worksheet

Dominion PX Series Unit Model \_\_\_\_\_

Dominion PX Series Unit Serial Number \_\_\_\_\_

Environmental Specifications

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

Appendix B: Equipment Setup Worksheet

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

## Environmental Specifications

SERIAL NUMBER	SERIAL NUMBER	
USE	USE	

Types of adapters

---

Types of cables

---

Name of software program

---

# Appendix C 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 .....	125
Logging into the CLP interface .....	126
Showing Outlet Information .....	127
Turning an Outlet On or Off .....	130
Querying an Outlet Sensor .....	130

---

## 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, select **Device Settings --> Network** and click the check box labeled **Enable CLP-Telnet Access**.

---

---

**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. Please refer to 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.

---

### Using 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 appears, 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.

---

### Using 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.

## Showing Outlet Information

---

### 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.

```

Name
Power State
Associations

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

---

### 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>=>AssociatedSensor
```

where <outlet number> is the number of the outlet.

# Appendix D 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 .....	132
Configuring SNMP Traps.....	135
SNMP Gets and Sets.....	136

---

## Enabling SNMP

To communicate with an SNMP manager, you must first enable the SNMP agent on Dominion PX. This can be done from the SNMP Settings window:

1. Select **Device Settings**, and then select **SNMP Settings**. The SNMP Settings window appears.

**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. Check the box for **Enable SNMP Agent** to enable the Dominion PX to communicate with external SNMP managers. A number of options will then become available.
3. Check **Enable SNMP v1 / v2c Protocol** to enable communication with an SNMP manager using SNMP v1 or 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. Check **Enable SNMP v3 Protocol** 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.

### Configuring 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**, then **Users & Groups**. The User/Group Management window appears.

User Management

**Existing Users**

Testing1
▼
Refresh

**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**

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. If you want to use the user's password as their Encryption Phrase leave the box marked **Use Password as Encryption Phrase** checked (or check the box if it is unchecked).



4. If you want to specify a different encryption phrase, uncheck this box, 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.

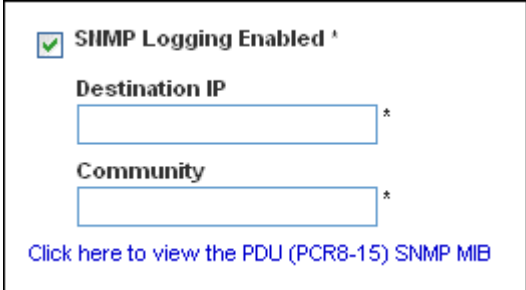
---

## Configuring SNMP Traps

Dominion PX automatically keeps an internal log of events that occur (refer to **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 appears. 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. Click the checkbox labeled **SNMP Logging Enabled**.
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.

## SNMP Gets and Sets

- 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, check 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.

---

Note: 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.

---

---

## 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.

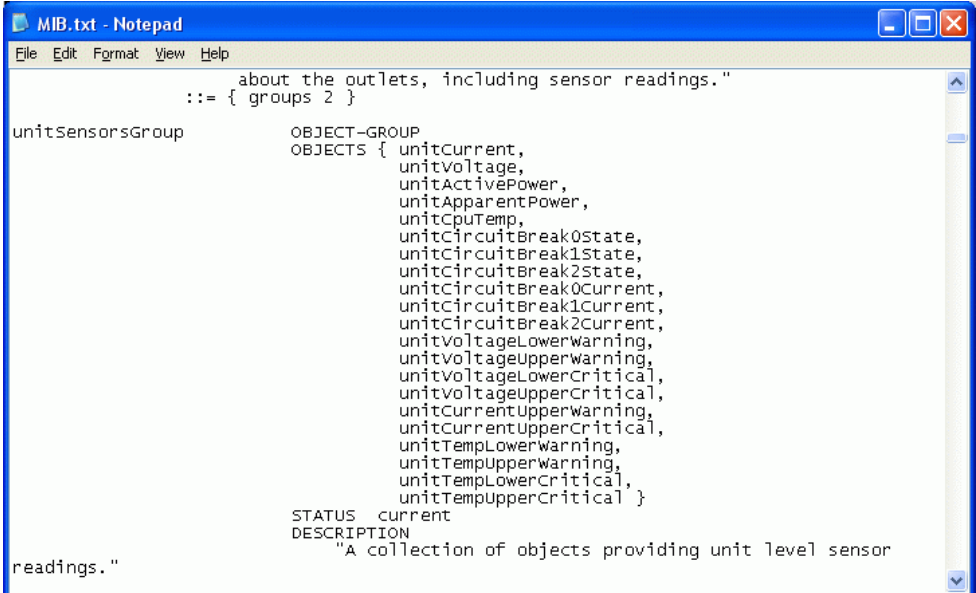
---

## 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."

```

## SNMP Gets and Sets

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. Refer to the **Setting up Outlets and Power Thresholds** section in the **Using the Web Interface** chapter for a description of how thresholds work.

# Appendix E Using the IPMI Tool Set

The IPMI tool set is command-line that allows users to display channel information, print sensor data, and set LAN configuration parameters. The following explains the available IPMI commands.

---

Note: The open source IPMI tool can be downloaded from sourceforge, and compiled on Linux system .Then users can interact with 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.....	139
Event Commands .....	141
LAN Commands.....	142
Sensor Commands.....	144
OEM Commands .....	145
IPMI Privilege Levels .....	152

---

## 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

## Channel Commands

### Example

```
$ ipmitool -I lan -H 192.168.51.58 -U admin -a channel  
authcap 14 5
```

Refer to the **IPMI Privileges Levels** section 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
```

## LAN Commands

---

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* <privolist> 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.

## Sensor Commands

The format of `privlist` is as follows. Each character represents a privilege level and the character position identifies the cipher suite number. For example, the first character represents cipher suite 1 (cipher suite 0 is reserved), the second represents cipher suite 2, and so on. `privlist` must be 15 characters in length.

Characters used in `privlist` and their associated privilege levels are:

- X Cipher Suite Unused
- c CALLBACK
- u USER
- O OPERATOR
- a ADMIN
- O OEM

---

## Sensor Commands

The Sensor commands allow you to display detailed sensor information.

---

### `list`

Lists sensors and thresholds in a wide table format.

Example

```
$ ipmitool -I lan -H allen-dpxpcr20-20 -U admin -a  
sensor list
```

---

### `get <id> ... [<id>]`

Prints information for sensors specified by name.

Example

```
$ ipmitool -I lan -H allen-dpxpcr20-20 -U admin -P  
raritan1 sensor get "R.14 Current"
```

thresh <id> <threshold> <setting>

This allows you to set a particular sensor threshold value. The sensor is specified by name. Valid thresholds are:

- *unr* Upper Non-Recoverable
- *ucr* Upper Critical
- *unc* Upper Non-Critical
- *lnc* Lower Non-Critical
- *lcr* Lower Critical
- *lnr* Lower Non-Recoverable

Example

```
$ ipmitool -I lan -H allen-dpxpcr20-20 -U admin -P raritan1 sensor thresh "R.14 Current" unr 10.5
```

## OEM Commands

You can use the OEM commands to manage and control the operation of the Dominion PX.

OEM Net-Fn is as defined below:

```
#define IPMI_NETFN_OEM_PP 0x3C
```

The table below 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

## OEM Commands

Command Name	Id
Set Receptacle ACL	0x19
Get Receptacle ACL	0x1A
Set Sensor Calibration	0x1B
Test Actors	0x1C
Test Sensors	0x1D
Set Power Cycle Delay Command	0x1E
Get Power Cycle Delay Command	0x1F

---

### 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 individual receptacles.

Request Data	1	# of receptacle [7 - 5] reserved [4 - 0] # of receptacle, 0 based, highest valid # depends on device model
--------------	---	--

Request Data	1	# of receptacle [7 - 5] reserved [4 - 0] # of receptacle, 0 based, highest valid # depends on device model
	2	new state [7 - 1] reserved [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.

OEM Commands

Request Data	1	# of group [7 - 5] reserved [4 - 0] group #, valid numbers: 0 - 23
	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
	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
Response Data	1	Completion Code

Request Data	1	# of group [7 - 5] reserved [4 - 0] group #, valid numbers: 0 - 23
	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
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

OEM Commands

Request Data	1	# of group [7 - 5] reserved [4 - 0] group #, valid numbers: 0 - 23
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 +N	ACL entry [7] 0b = deny, 1b = allow [6] 0b = user id, 1b = privilege level [5 - 0] user id or privilege level depending on [6]
Response Data	1	Completion Code

---

Get Receptacle ACL

Request Data	1	# of receptacle
Response Data	1	Completion Code
	2	number of ACL entries to follow
	3 +N	ACL entry [7] 0b = deny, 1b = allow [6] 0b = user id, 1b = privilege level [5 - 0] user id or privilege level depending on [6]



---

Set Sensor Calibration

Sensor calibration is only allowed for threshold based sensors that return a sensor reading byte with the Get Sensor Reading Command. Also 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.
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)
--------------	---	--

## IPMI Privilege Levels

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. In order to set the Power Cycle Delay to longer than 255 seconds, you must use the web interface.

---



---

## IPMI Privilege Levels

The IPMI privilege level that you select determines:

	IPMI PRIVILEGE LEVELS					
	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 Settings	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
User/Group Management	No	No	No	No	Yes	Yes
User Group Permissions	No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No

Figure 2: IPMI Privilege Level

## Appendix F Event Types

Event Type	Examples
<b>Outlet Control</b>	Outlet(#) switched on by user Outlet(#) switched off by user Outlet(#) cycled by user
<b>Outlet/Unit/Environmental Sensors</b>	Assertion: Environmental Temperature (#) above upper non-critical threshold Deassertion: Environmental Temperature (#) above upper critical threshold
<b>User/Group Administration</b>	User added successfully User successfully changed User successfully deleted User password successfully changed Group added successfully Group successfully changed Group successfully deleted
<b>Security Relevant</b>	User login failed
<b>User Activity</b>	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.
<b>Device Operation</b>	Device successfully started
<b>Device Management</b>	The Device update has started
<b>Virtual Device Management</b>	Master PDU lost connectivity with SlaveIPAddress :

## IPMI Privilege Levels

# Appendix G Specifications

This appendix contains information describing:

- DPX Serial RJ-45 pinouts

RJ-45 Pin/signal definition			
Pin No.	Signal	Direction	Description
1	DTR	Output	Reserved
2	GND	—	Signal Ground
3	+5V	—	Power for CIM (200mA, fuse protected)
4	TxD	Output	Transmit Data (Data out)
5	RxD	Input	Receive Data (Data in)
6	N/C	N/C	No Connection
7	GND	—	Signal Ground
8	DCD	Input	Reserved

- DPX Feature RJ-11 pinouts

RJ-11 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> • 141

## 1

1U Products • 4

1U Size • 2

## 2

2U Products • 5

2U Size • 3

## A

About the CLP Interface • 125

Add a Dominion PX Unit in Paragon II • 112

All Outlets Control • 38

Associate Outlets with a Target • 108, 113

Attributes • 128

authcap <channel number> <max priv> • 139

## B

Back Panel • 20

Beeper • 25

Before Beginning: • 8

Before You Begin • 10

Blue LED • 20

## C

Changing Your Password • 30

Channel Commands • 139

Check Power Strip Status • 116

Circuit Breaker • 24

CommandCenter • 117

Configure a Dominion PX Power Unit on  
Dominion SX • 114

Configure the Dominion PX for Network  
Connectivity • 12

Configuring Alert Events • 76

Configuring Environmental Sensors and  
Thresholds • 74

Configuring NFS Logging • 86

Configuring SMTP Logging • 87

Configuring SNMP Logging • 88

Configuring SNMP Traps • 135

Configuring Syslog Forwarding • 88

Configuring the Firewall • 14, 50

Configuring the Local Event Log • 83, 85

Configuring the SMTP Settings • 81, 87, 97

Configuring the SNMP Settings • 98

Configuring Users for Encrypted SNMP v3 •  
134

Connect the Dominion PX to a Computer • 11,  
12

Connect the Dominion PX to Your Network •  
12

Connecting the Environmental Sensors • 72

Connection Ports • 19

Control a Target's Power • 110, 113

Control an Outlet's Power • 114

Controlling Outlet Groups • 105

Copying a User Group • 48

Copying a User Profile • 41

Creating a Certificate Signing Request • 60

Creating a User Group • 44

Creating a User Profile • 26, 39

Creating Alert Policies • 77, 78

Creating Group Based Access Control Rules •  
53

## D

Deleting a User Group • 49

Deleting a User Profile • 42

Deleting Outlet Group Devices • 106

Displaying Basic Device Information • 89, 91

Displaying Connected Users • 91

Displaying Model Configuration Information  
• 91

Dominion KSX • 116

Dominion KX • 108

Dominion KX-II • 111

Dominion PX Models • 1, 118

Dominion SX • 114

## E

Editing or Deleting Outlet Groups • 106

## Index

Enabling SNMP • 132  
Environmental Sensors • 72  
Environmental Specifications • 120  
Equipment Setup Worksheet • 11, 121  
Event Commands • 141  
Event Types • 153  
Examples • 129

## F

file <filename> • 142  
Fill Out the Equipment Setup Worksheet • 11  
Forcing HTTPS Encryption • 49, 59  
Front Panel • 19

## G

get <id> ... [<id>] • 144  
Get Group Membership Command • 148  
Get Group Power On Delay Command • 149  
Get Power Cycle Delay Command • 152  
Get Power On Delay Command • 146  
Get Receptacle ACL • 150  
Get Receptacle State Command • 147  
getaccess <channel number> [userid] • 140  
getciphers <all | supported> <ipmi | sol>  
[channel] • 141  
Global Status Panel • 36  
Grouping Outlets Together • 103

## H

Hardware Specification • 119

## I

Identifying Other Dominion PX Units • 102  
info [channel number] • 140  
Installation and Configuration • 10, 50, 93  
Installing a Certificate • 61  
Integration • 107  
Introduction • 1  
IPMI Privilege Levels • 152

## K

KX Manager Application (Dominion KX-I  
only) • 108

## L

LAN Commands • 142  
LED Display • 22  
list • 144  
Logging In • 26  
Logging into the CLP interface • 126  
Logging into the Web Interface • 26

## M

Managing the Dominion PX • 89  
Mapping the Environmental Sensors • 73  
Measurement Accuracy • 25  
Menus • 31  
Modifying a User Group • 48  
Modifying a User Profile • 42  
Modifying the Communications, Port and  
Bandwidth Settings • 94  
Modifying the LAN Interface Settings • 95  
Modifying the Network Settings • 93

## N

Naming the Dominion PX • 92, 93  
Naming the Outlets • 69, 72  
Navigation Path • 32

## O

OEM Commands • 145  
Outlet Grouping • 102  
Outlets • 21  
Outlets List • 37

## P

Package Contents • 4  
Paragon II • 111  
Paragon Manager Application • 112  
Power Control • 115  
Power Cord • 20  
Power Cycling an Outlet • 67, 70, 72  
Prepare the Installation Site • 10  
print <channel> • 142  
Product Features • 3  
Product Models • 1  
Product Photos • 1



## Q

Querying an Outlet Sensor • 130

## R

Rack Mount Safety Guidelines • 6  
 Rack-Mounting the Dominion PX • 6  
 Refresh • 35  
 Reset to Defaults • 35  
 Resetting the Dominion PX • 99  
 Resetting to Factory Defaults • 16, 23

## S

Safety Guidelines • iii  
 Sensor Commands • 144  
 set <channel> <parameter> • 143  
 Set Group Membership Command • 148  
 Set Group Power On Delay Command • 149  
 Set Group State Command • 147  
 Set Power Cycle Delay Command • 151  
 Set Power Set Delay Command • 146  
 Set Receptacle ACL • 150  
 Set Receptacle State Command • 146  
 Set Sensor Calibration • 151  
 setaccess <channel number>  
   <userid>[callin=on|off] [ipmi=on|off]  
   [link=on|off] [privilege=level] • 140  
 Setting the Date and Time • 96  
 Setting the Default Outlet State • 66  
 Setting the Dominion PX Thresholds • 66, 72  
 Setting the Outlet Permissions • 43, 47  
 Setting the Outlet Power-Up Sequence • 67  
 Setting the Outlet Thresholds • 67, 70, 72  
 Setting the System Permissions • 42, 44  
 Setting Up a Digital Certificate • 59  
 Setting Up Access Controls • 49  
 Setting Up Alerts • 65, 76, 97  
 Setting Up Event Logging • 82  
 Setting Up External User Authentication • 62  
 Setting Up Outlets and Power Thresholds •  
   65, 76  
 Setting Up RADIUS Authentication • 64  
 Setting Up User Groups • 43  
 Setting Up User Login Controls • 56  
 Setting Up User Profiles • 39

Setting User Permissions Individually • 41, 42  
 Settings Up LDAP Authentication • 63  
 Showing Outlet Information • 127  
 SNMP Gets and Sets • 136  
 Specifications • 155  
 Specifying the Alert Destination • 81  
 Status Messages • 34  
 Status Panel • 32  
 Syntax • 128, 130

## T

Test Actors • 151  
 Test Sensors • 151  
 The Dominion PX MIB • 137  
 thresh <id> <threshold> <setting> • 145  
 To Mount: • 9  
 Tool-less Mounting Instructions • 8  
 Turning an Outlet On or Off • 72, 130

## U

Unavailable Options • 35  
 Unpack the Dominion PX and Components •  
   10  
 Updating the Firmware • 100  
 Using HyperTerminal • 126  
 Using SNMP • 131  
 Using SSH or Telnet • 127  
 Using the CLP Interface • 125  
 Using the Dominion PX • 19  
 Using the Home Window • 36  
 Using the IPMI Tool Set • 139  
 Using the Web Interface • 26, 30

## V

Viewing Outlet Details • 71  
 Viewing Sensor Readings • 75  
 Viewing the Internal Event Log • 85

## Z

Zero U Products • 4  
 Zero U Size • 2





➤ *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+1 CET  
Phone +44-20-7614-77-00  
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

## Free Manuals Download Website

<http://myh66.com>

<http://usermanuals.us>

<http://www.somanuals.com>

<http://www.4manuals.cc>

<http://www.manual-lib.com>

<http://www.404manual.com>

<http://www.luxmanual.com>

<http://aubethermostatmanual.com>

Golf course search by state

<http://golfingnear.com>

Email search by domain

<http://emailbydomain.com>

Auto manuals search

<http://auto.somanuals.com>

TV manuals search

<http://tv.somanuals.com>