PANDUIT® infrastructure for a connected world

smartzone™ G5

# G5 PDU User Manual

# Table of Contents

Section 1 – System Overview ..... 7
Intelligent Network Controller ..... 7
Connecting the PDU to a LAN Ethernet Port ..... 7
Connecting the PDU to a Computer Serial Port ..... 8
Setup Serial Communication ..... 9
Section 2 – Web Graphical User Interface (GUI) Configuration ..... 12
Internet Protocol (IP) Address ..... 12
Web Configuration ..... 12
Supported Web Browsers ..... 12
Logging in to the Web Interface ..... 12
Introduction to the Web GUI ..... 13
Screen Resize Due to Multiple PDU Configuration ..... 15
Menu Dropdowns ..... 16
Introduction to the Dashboard ..... 17
Section 3 – Simple Network Management Protocol (SNMP) ..... 19
SNMP Management Configuration ..... 19
Configuring Users for SNMP v3 Communications ..... 23
Configuring SNMP Traps ..... 26
Section 4 – Connecting to CLI Connection ..... 29
Supported Commands ..... 29
Connecting to the CLI through the serial interface ..... 30
Section 5 – Local Display ..... 32
Onboard Display and Intelligent Network Controller (iNC) ..... 32
Control Buttons ..... 33
iNC Menu Structure ..... 33
Main Menu Selections ..... 34

Setup Menu ..... 35
Sensors Menu ..... 48
Section 6 – User Access ..... 49
Access Types ..... 51
Setting Up the System for Radius Authentication ..... 52
Configuring the system with LDAP Server Settings ..... 54
Section 7 – Daisy Chain Configuration ..... 58
Daisy-Chain Overview ..... 58
Daisy-Chain Setup ..... 58
RNA (Redundant Network Access) Functionality ..... 58
RNA Setup ..... 59
Section 8– Web GUI configuration ..... 61
**System Management Information** ..... 61
Setting Time and Date on the PDU ..... 64
G5 iPDU Outlet Power Sequence Setup ..... 67
Outlet Power Management ..... 70
Setting Metering Thresholds ..... 71
Email Setup ..... 83
Data Log ..... 86
Section 9 – Connecting and Configuring Optional Hardware ..... 88
Accessory Hardware Overview ..... 88
Configuring Environmental Sensors ..... 91
Section 10 – Rack Access Control ..... 92
Configuring Rack Access Control ..... 93
Configuring User for Local Rack Access ..... 96
Handle and Compatible Cards Types ..... 98
Warranty and Regulatory Information ..... 99
Warranty Information ..... 99
Regulatory Information ..... 99

Support and Other Resources ..... 100
Accessing Panduit Support ..... 100
Acronyms and Abbreviations ..... 101
Documentation Feedback ..... 104
Appendix A: CLI Commands ..... 105
Appendix B: Sensor Configuration ..... 114
Appendix C: Firmware Update Procedure ..... 118
USB Method ..... 118
Web Interface Method ..... 118
FTPs Method ..... 120
Bootloader Mode ..... 121
Firmware Recovery with Bootloader Mode ..... 121
Appendix D: System or Password Recovery ..... 122
Upgrade Configuration with Bootloader Mode ..... 122
Appendix E: PDU Alarms ..... 123
Trap Codes assigned to Alarms List ..... 125
Appendix F: Horizontal Intelligent Network Controller Replacement ..... 130
Appendix G: Vertical Intelligent Network Controller Replace or Rotate 180° ..... 133
Appendix H: Changing Your PC's IP Address ..... 135

# Table of Figures

Figure 1: Ethernet Port for Network Connection ..... 8
Figure 2: Status Button ..... 9
Figure 3: Port Setup Settings ..... 10
Figure 4: Login Page ..... 13
Figure 5: Landing Page/Dashboard ..... 14
Figure 6 - Resized Dashboard Screen ..... 16
Figure 7: Power Summary Page ..... 17
Figure 8: Outlet Monitoring Page ..... 17
Figure 9: Environmental Page ..... 18
Figure 10: Security Page ..... 18
Figure 11: SNMP Management ..... 19
Figure 12: SNMP General ..... 20
Figure 13: SNMP Port ..... 21
Figure 14: Setup SNMP Port and Trap Port ..... 22
Figure 15: Define SNMP V1/V2c User ..... 22
Figure 16: Edit V1/2c Manager ..... 23
Figure 17: SNMP V3 Manager ..... 24
Figure 18: SNMP V3 Edit ..... 25
Figure 19: SNMPv2 Configuration Information ..... 26
Figure 20: SNMPv3 Trap Server Information. ..... 27
Figure 21: Connect the RJ-45 end of the cable to the PDU In/Serial connector ..... 30
Figure 22: Serial Cable Pinout ..... 31
Figure 23: iNC Display ..... 32
Figure 24: iNC Menu Structure ..... 34
Figure 25: Main Menu Selections ..... 34
Figure 26: Setup Menu ..... 35
Figure 27: Network Submenu ..... 36
Figure 28: Device Submenu ..... 37
Figure 29: Screen Submenu ..... 38
Figure 30: Language Submenu ..... 39
Figure 31: USB Submenu ..... 40
Figure 32: Units Submenu ..... 41
Figure 33: Alarms Menu ..... 42
Figure 34: Power Menu ..... 43
Figure 35: Device Submenu ..... 44
Figure 36: Phase Submenu ..... 45
Figure 37: Breaker Submenu ..... 46

Figure 38: Outlet Submenu ..... 47
Figure 39: Sensors ..... 48
Figure 40: Changing Your Password ..... 49
Figure 41: After Login ..... 49
Figure 42: Change User Password ..... 50
Figure 43: Change Password ..... 50
Figure 44: User Settings ..... 53
Figure 45 Radius Configuration ..... 53
Figure 46: LDAP Configuration ..... 55
Figure 47: Enable Role Privileges ..... 56
Figure 48: Test LDAP Configuration ..... 57
Figure 49: System Management ..... 61
Figure 50: System Management Configuration ..... 62
Figure 51: Rack Location Configuration ..... 63
Figure 52: Power Panel & Core Location ..... 64
Figure 53: NTP Configuration ..... 65
Figure 54: Daylight Saving Time Configuration ..... 66
Figure 50: Control & Manage PDU ..... 67
Figure 51: Outlet Control Enabled ..... 68
Figure 52: Edit Outlets ..... 68
Figure 53: One-Delay Time ..... 69
Figure 54: Saved Sequence ..... 70
Figure 55: Power Threshold ..... 72
Figure 56: Energy Threshold ..... 74
Figure 57: Phase Current Alarm ..... 75
Figure 58: Phase Voltage Alarm ..... 77
Figure 59: Load Segment Breaker ..... 79
Figure 60: Device Detection Threshold Information ..... 80
Figure 61: Outlet Information ..... 81
Figure 62: Email Setup ..... 83
Figure 63: SMTP Account Settings ..... 84
Figure 64: Email Recipients ..... 85
Figure 65: Data Log ..... 86
Figure 66: Data Log Configuration ..... 87
Figure 67: Sensor Ports for vertical PDU ..... 90
Figure 68: Sensor Ports for Horizontal PDU ..... 91
Figure 69: Rack Access Control ..... 92
Figure 70: Rack Access Control ..... 93

Figure 71: Actions ..... 94
Figure 72: Smart Rack ..... 94
Figure 73: Remote Control ..... 95
Figure 74: AutoLock ..... 95
Figure 75: Local Rack Access ..... 97
Figure 76: Door Switch Sensor Configuration ..... 114
Figure 77: Dry Contact Cable ..... 115
Figure 78: Water Rope Sensor ..... 115
Figure 79: Water Spot Sensor ..... 116
Figure 80: Temperature and Humidity Sensors ..... 117
Figure 81: Upload Firmware ..... 119
Figure 82: Uploading Firmware ..... 120
Figure 83: Unscrew Intelligent Network Controller ..... 130
Figure 84: Remove Intelligent Network Controller from PDU ..... 131
Figure 85: Inserting New Intelligent Network Controller ..... 132
Figure 86: Removing Top and Bottom Screw from Intelligent Network Controller ..... 133
Figure 87: Disconnecting and Reconnecting the Intelligent Network Controller ..... 134
Figure 88: Control Panel ..... 135
Figure 89: Network Status and Tasks ..... 136
Figure 90: Change Adapter Settings ..... 137
Figure 91: Properties ..... 137
Figure 92: Ethernet Properties ..... 138
Figure 93: Internet Protocol Version 4 ..... 139
Figure 94: DNS Server ..... 140
Figure 95: Confirmation ..... 141

# Section 1 – System Overview

## Intelligent Network Controller

Panduit G5 Intelligent PDUs have an integral, hot swappable Intelligent Network Controller. The Intelligent Network Controller contains an OLED display, control buttons, USB Interface, Serial and Sensor ports, and a recessed Reset Button.

### Reset Button

Pressing the Reset Button only reboots the Intelligent Network Controller. It does not change the Energy (kWh) value and does not affect the output voltage. It also **does not** reset the Intelligent Network Controller to factory default settings.

#### *Using the Reset Button*

Press and hold the Reset Button for 8 seconds to recover from an Intelligent Network Controller communication failure.

## Connecting the PDU to a LAN Ethernet Port

The PDU is defaulted to DHCP. If you are connected to a network with a DHCP server, the PDU automatically get an IP address and display it on the LCD screen. If there is no DHCP server, the default IP address is 192.168.0.1, which will be displayed on the PDU.

Connecting the PDU to a LAN provides communication through an Internet or Intranet connection. You can monitor the PDU from any computer connected to the same network.

1. Locate an Ethernet cable.
2. Connect one end of the cable to the Ethernet port on the PDU (see Figure 1). Connect the other end of the cable to the Ethernet port on the router (or another LAN device).

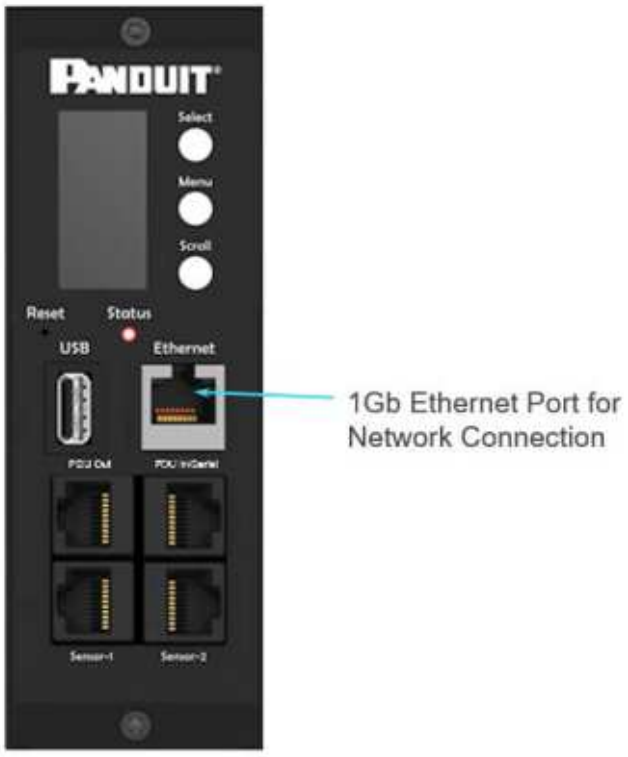



**Figure 1: Ethernet Port for Network Connection**

## Connecting the PDU to a Computer Serial Port

If unable to connect to network, you can change the network setting using the serial interface.

To configure the network setting, perform the following steps:

1. Serial connect the PDU to a computer's serial port. Set baud rate for a terminal emulation program.
2. Using a CLI command to enable DHCP or set a static IP.
3. Verify access to the Web interface. The Ethernet LED on the PDU front panel provides communication status by color and display activity.




**Figure 2: Status Button**

**Setup Serial Communication**

You may configure the network settings using the Command Line Interface (CLI) with a serial connection. Users can connect serially using the optional RJ45-DB9 cable Panduit p/n: MA001 (or make your own cable by creating a unique pinout as described below in the "Serial Cable Pinout to Create Your Own Cable" in Section 4).

1. Verify that the computer has a serial port. If your computer does not have a DB9 serial connector, but does have a USB connector, obtain a USB-to-DB9 Adapter to convert the USB to a DB9 serial port.
2. Using the optional RJ45-DB9 cable (Panduit p/n: MA001), connect the RJ-45 end to the port labeled "PDU In/Serial" on the front panel of your PDU model (see Figure 1). Connect the DB9 end of the cable to the computer.
3. Open the terminal emulation program (HyperTerminal or PuTTY) on the computer and select the serial port connection (such as COM1).
4. Set the communications port as follows:
    - Bits per second: 115200
    - Data bits: 8

- Parity: None
- Stop bits: 1
- Flow control: None

(See **Port Settings** example below).

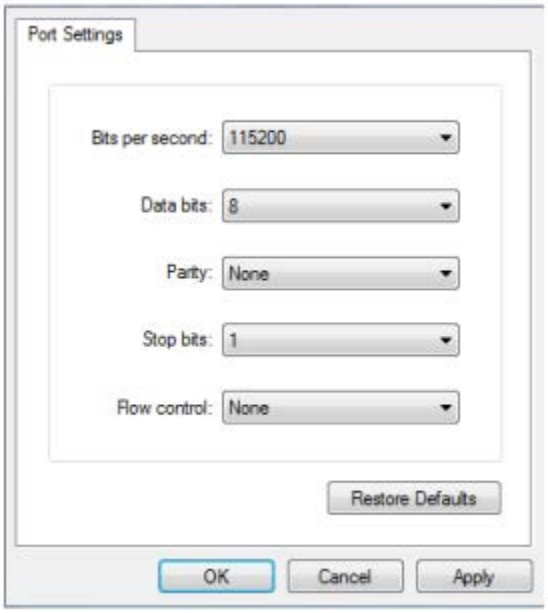



**Figure 3: Port Setup Settings**

5. Use the default initial login indicated below. Note that the username and password are both case sensitive:
   - Username: admin
   - Password: 12345678 (or your new password)
6. If this is the first time logging into the PDU, you will need to change the default password. You will be prompted to enter the current password, 12345678. Then enter your new password. You will need to confirm the new password a second time.
7. The “Panduit>” prompt appears after you have logged in, ready to enter the CLI command.
8. To configure network settings, enter the appropriate “net” command and press

**Enter**. All commands are case sensitive. You can type **?** to access the commands.

9. To enable the IPv4 DHCP by default, run:
   - net tcpip dhcp
   - Enter **Y** to confirm and the PDU's Intelligent Network Controller will reboot.
10. To set a static IPv4 configuration, run:
   - net tcpip static x.x.x.x (ipaddress) x.x.x.x (netmask) x.x.x.x (gateway)
   - Example: net tcpip static 192.168.1.100  255.255.255.0  192.168.1.1
   - Enter **Y** to confirm and the PDU's Intelligent Network Controller will reboot.

# Section 2 – Web Graphical User Interface (GUI) Configuration

## Internet Protocol (IP) Address

The PDU is by default configured Dynamic Host Configuration Protocol (DHCP). The PDU automatically obtains an IP address via a DHCP server when connected to a network. The IP address the PDU received is displayed on the OLED screen. After the PDU received the address, login to the Web interface to configure the PDU and assign a static IP address (if desired). If there is no DHCP server, the default IP address is 192.168.0.1, which will be displayed on the PDU.

If the network does not use a DHCP server, see the Connecting the PDU to a Computer Serial Port section to configure a static IP address.

1. Connect a standard Ethernet patch cable to the Ethernet port on the PDU.
2. Connect the other end of the Ethernet cable to the LAN.
3. Make sure the Ethernet port on the PDU shows a solid green light on the left and a flashing yellow light on the right to indicate successful connectivity to the network.
4. Use the menu buttons to look up the IP address of the device on the OLED display by selecting Setup > Network > IPv4 or IPv6 as applicable.
5. In a standard web browser, enter the PDU IP address and proceed to configure the PDU as shown in the Web Configuration section.

## Web Configuration

### Supported Web Browsers

The supported Web browsers are Mozilla Firefox, Microsoft Internet Explorer Version 11, Microsoft Edge, and Google Chrome mobile and desktop, Apple Safari mobile and desktop.

### Logging in to the Web Interface

*Logging In*

- Open a supported web browser and enter the IP address of the PDU.
  - If username and password were configured during the Network Configuration Setup: enter the username and password in the appropriate fields. Press **Login** or **Enter**.

- If username and password were NOT configured during the Network Configuration Setup, use the default username: ***admin*** and password: ***12345678***. For security purposes, change the password upon login.

## Introduction to the Web GUI

*Login Page*



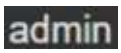

**Figure 4: Login Page**

## *Landing Page/Dashboard*




**Figure 5: Landing Page/Dashboard**

| Number | Icon | Description |
|---|---|---|
| 1 | | The home icon provides an overview of the PDU with access to the Dashboard, Identification, and Control & Manage. |
| 2 | | The Alarm icon provides details of the active critical alarms and active warning alarms. |
| 3 | | This icon lets you select a Language. There are seven languages available to choose from: English, Chinese, French, Italian, German, Spanish, Korean and Japanese. |
| 4 | | This icon provides the logs of the PDU which can be viewed and downloaded. |

| Number | Icon | Description |
|---|---|---|
| |  | • The Data Log is a log of the Power, Environmental, and Security values. |
| 5 |  | The settings icon allows a user to setup the Network Settings, System Management, SNMP Manager, Email Setup, Event Notifications, Trap Receiver, Thresholds, and Rack Access Control. |
| 6 |  | The search icon allows you to input key words and search for the related results. |
| 7 |  | Information about the PDU can be found using this icon. You also can also click user guide and license to ask for help. |
| 8 |  | This icon shows who is logged in (user or admin). Account passwords can be changed, and user accounts managed through this page. |

## Screen Resize Due to Multiple PDU Configuration

*Resizing a Screen*

Multiple PDUs can now cause the user to resize the screen to fit the information on the dashboard due to the update.




**Figure 6 - Resized Dashboard Screen**

## Menu Dropdowns

| Overview | Alarms | Help | Language | Logs | Settings | Admin |
|---|---|---|---|---|---|---|
| Dashboard | Active Critical Alarms 9 | User Guide | English | Event Log | Network Settings | admin |
| Identification | Active Warning Alarms 4 | License | Français | Download Event Log | System Management | Change Password |
| Control & Manage | | | Italiana | Data Log | SNMP Manager | User Accounts |
| | | | 한국어 | Download Data Log | Email Setup | Log Out |
| | | | Deutsch | | Event Notifications | |
| | | | Español | | Trap Receiver | |
| | | | 日本語 | | Thresholds | |

# Introduction to the Dashboard

## *Power Summary Page*

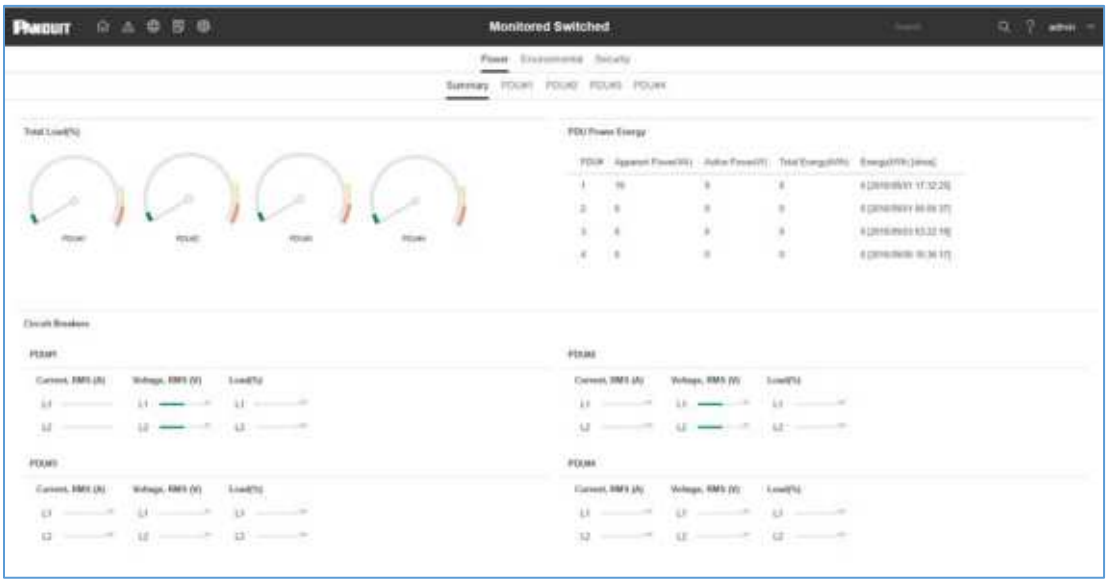



**Figure 7: Power Summary Page**

## *Outlet Monitoring Page*

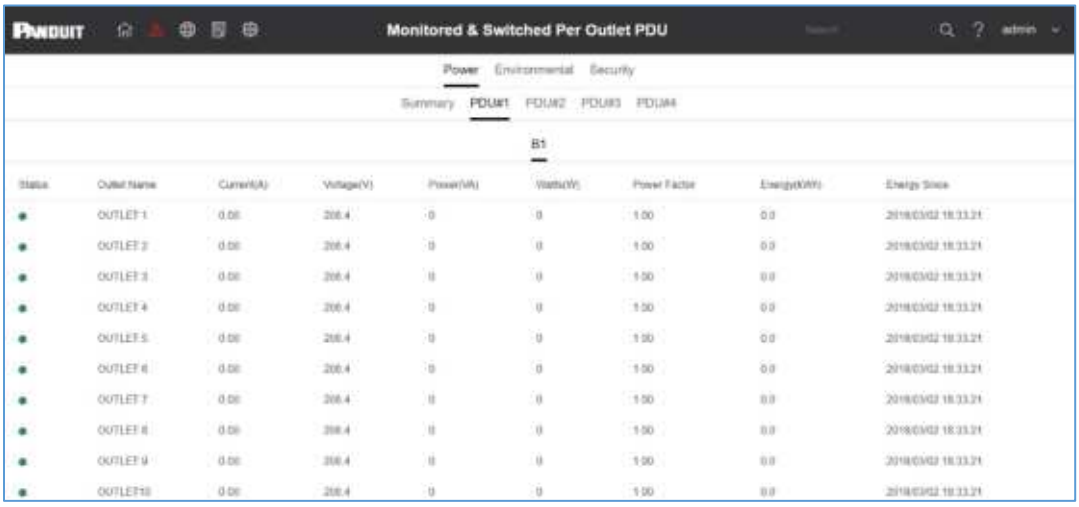



**Figure 8: Outlet Monitoring Page**

## *Environmental Page*

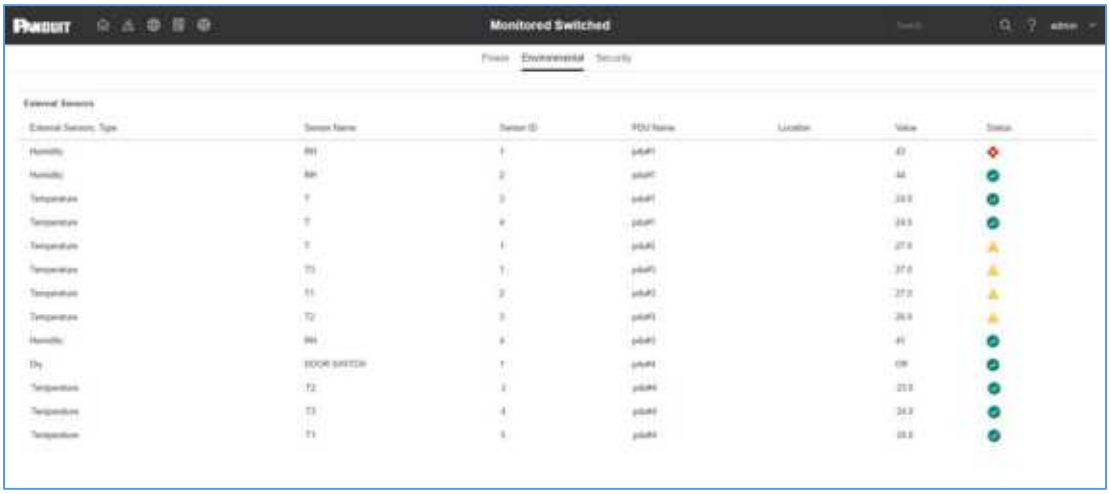



**Figure 9: Environmental Page**

## *Security Page*

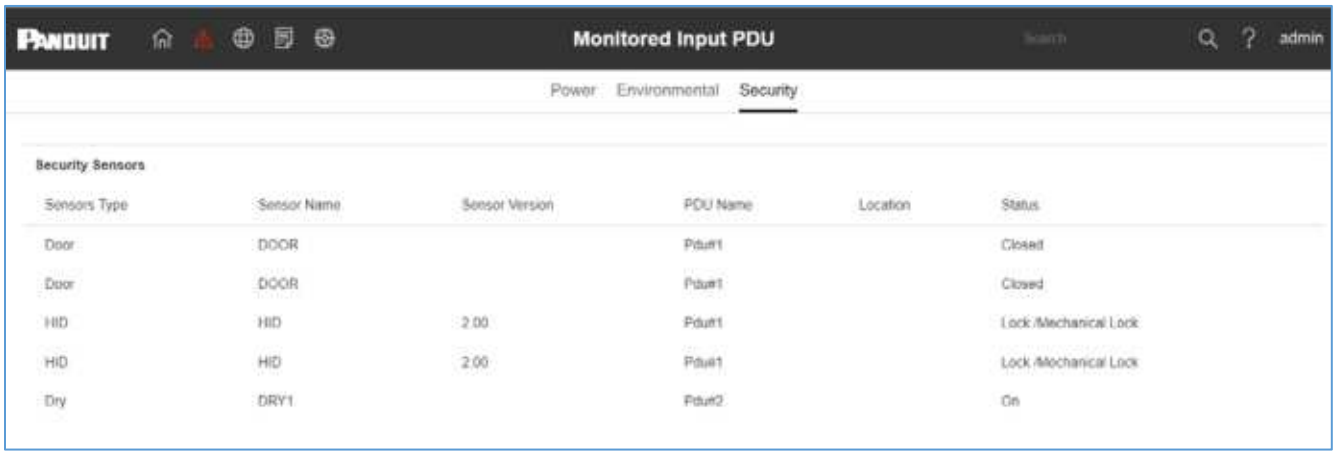



**Figure 10: Security Page**

# Section 3 – Simple Network Management Protocol (SNMP)

## SNMP Management Configuration

*Setup SNMP*

1. Access the Web interface and login.
2. Under SNMP Managers, select SNMP General (or type SNMP in the search). The SNMP General page displays.




**Figure 11: SNMP Management**

3. The SNMP General includes SNMP Access and Version.

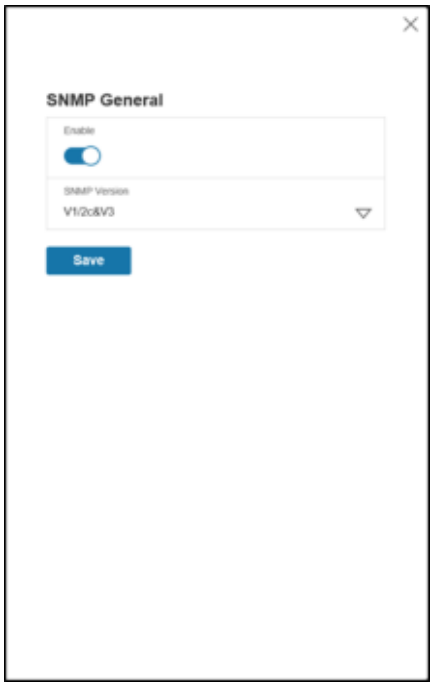



**Figure 12: SNMP General**

### *Setup SNMP Port*

1. Access the Web interface and log in.
2. Under SNMP Managers, select **SNMP Port**. The SNMP Port page displays.

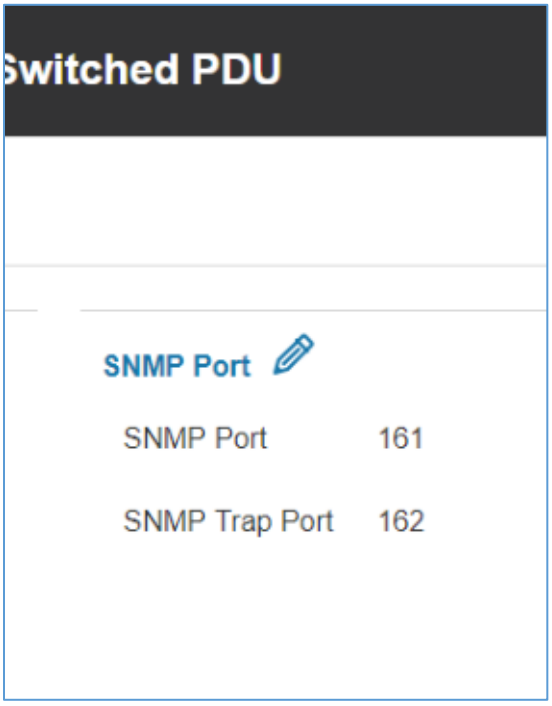



**Figure 13: SNMP Port**

3. Set up SNMP Port and SNMP Trap Port.

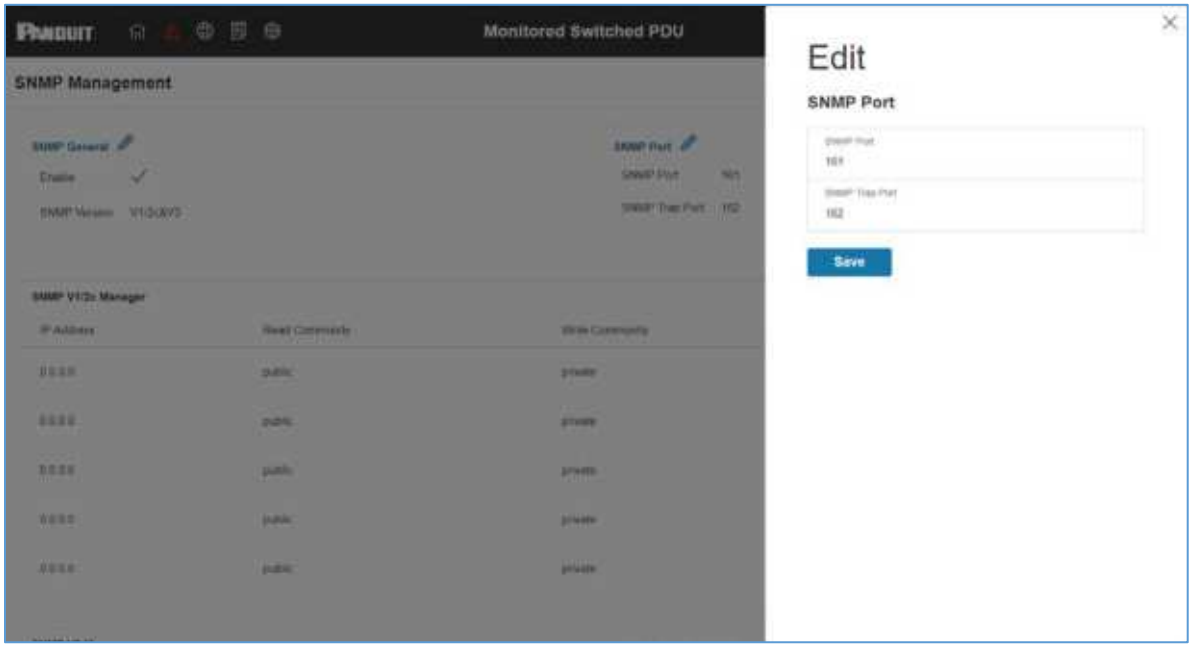



**Figure 14: Setup SNMP Port and Trap Port**

### *Define SNMP V1/V2c User*

1. Access the Web interface and log in.
2. Under SNMP Manager, select **SNMP V1/V2c**.
3. In the SNMP V1/V2c panel, select the SNMP V1/V2c manager to configure. Select the **pencil** icon.




**Figure 15: Define SNMP V1/V2c User**

4. The Edit panel pop up displays.

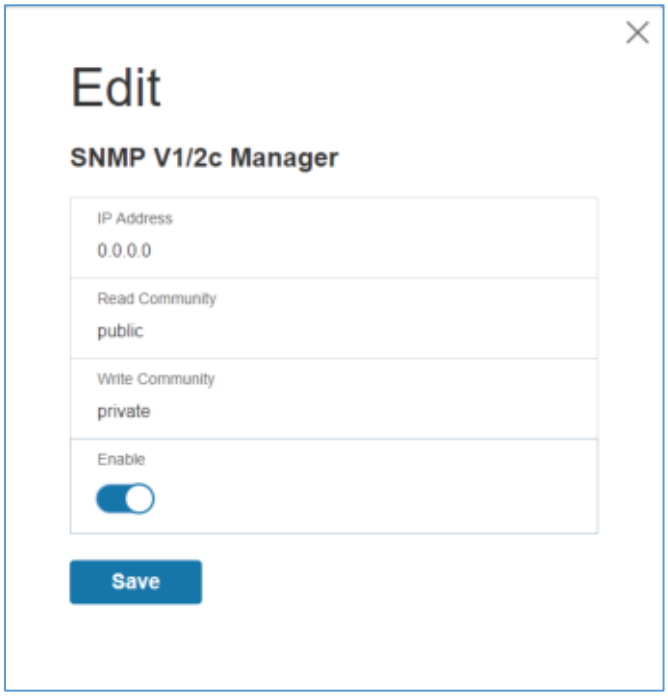



**Figure 16: Edit V1/2c Manager**

5. Set the following options:
   - IP Address: the IP address of the host for this SNMP V1/V2 manager. Only requests from this address will be acted upon.

     **Note**: An IP address configured to 0.0.0.0 will act as a wildcard and all requests will be acted upon.
   - Read Community: the read-only community string to allow an SNMP V1/V2c manager to read a SNMMP object.
   - Write Community: the write-only community string to allow an SNMP V1/V2c manager to write an SNMMP object.
6. Click **Enable** and **Save**.

## Configuring Users for SNMP v3 Communications

1. Access the Web interface and log in.
2. Under SNMP Managers, select **SNMP V3**.

3. In the SNMP V3 panel, select the **SNMP V3** manager to configure. Select the **pencil** icon in the last column.




**Figure 17: SNMP V3 Manager**

4. The Edit panel pop-up displaying the configurable options.

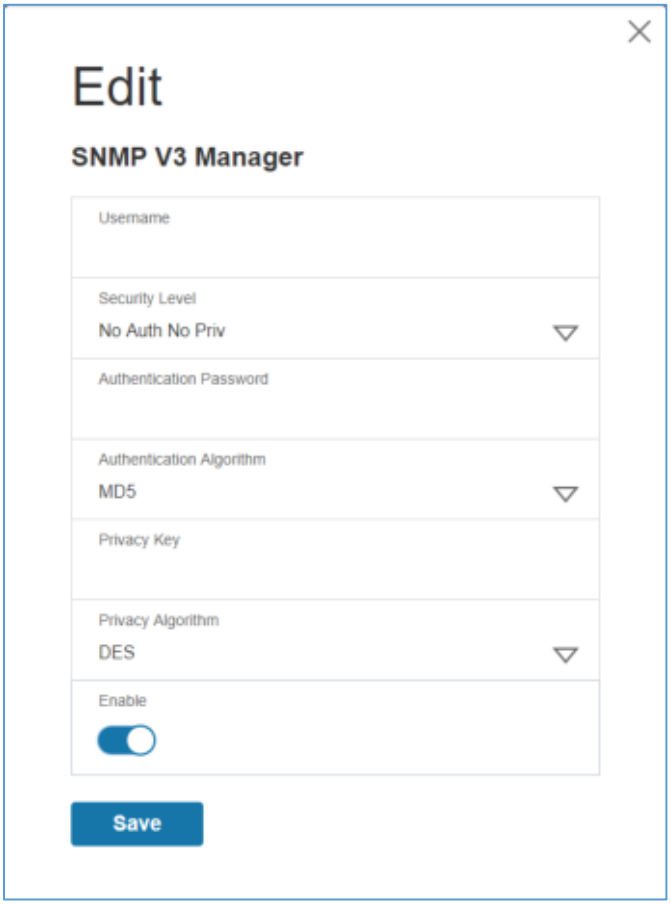



**Figure 18: SNMP V3 Edit**

5. Configure the SNMP username
6. Choose a Security Level from the dropdown menu
   - NoAuthNoPriv: No authentication and no privacy. This is the default.
   - AuthNoPriv: Authentication and no privacy.
   - AuthPriv: Authentication and privacy.
7. Enter a new unique password to be used for authentication
8. Select the desired authentication algorithm.
   - MD5
   - SHA

9. Enter a new unique key for privacy algorithm
10. Select the desired privacy algorithm
    - AES-128
    - AES-192
    - AES-256
11. Click **Enable** and **Save**.

## Configuring SNMP Traps

The M-Series PDU keeps an internal log of all events. These events can be used to send SNMP traps to a third-party manager. To set up the PDU to send SNMP traps, follow the following procedure:

### *Configuring SNMP v1 Trap Settings*

1. Go to Device Configuration > Network Services > SNMP
2. Click the Pencil next to SNMPV1 Trap Receiver you want to update.




**Figure 19: SNMPv2 Configuration Information**

3. Enter the **Name**, **Host**, and a **community name** in the fields provided.
    a. The name is a user assigned name to help distinguish the different receivers.
    b. The host name is the IP Address to which the traps are sent by the SNMP

system agent.

c. Community is the password on the SNMP management stations.

4. Select Enable to enable the receiver.
5. Select **Save** to save and exit.

### *Configuring SNMP v3 Trap Settings*

1. Go to Device Configuration > Network Services > SNMP
2. Click the Pencil next to SNMPV3 Trap Server you want to update.




**Figure 20: SNMPv3 Trap Server Information.**

3. Enter the **Name**, **Host**, and a **community name** in the fields provided.
   a. The name is a user assigned name to help distinguish the different receivers.
   b. The host name is the IP Address to which the traps are sent by the SNMP system agent.
4. Choose a Security Level from the dropdown menu
   - NoAuthNoPriv: No authentication and no privacy. This is the default.

- AuthNoPriv: Authentication and no privacy.
- AuthPriv: Authentication and privacy.

5. Enter the password from the SNMP Server to be used for authentication.
6. Select the desired authentication algorithm.
   - MD5
   - SHA
7. Enter the key from the SNMP Server for privacy algorithm
8. Select the desired privacy algorithm
   - AES-128
   - AES-192
   - AES-256
9. Select **Enable** to enable the receiver.
10. Select **Save** to save and exit.

# Section 4 – Connecting to CLI Connection

The Command Line Interface (CLI) is an alternate method used to manage and control the PDU status and parameters, as well as basic admin functions. Through the CLI a user can:

- Reset the PDU
- Display PDU and network properties
- Configure the PDU and network settings
- Switch outlets on/off
- View user information

Connecting to the CLI requires a terminal emulation program such as HyperTerminal or PuTTY

**Supported Commands**
The PDU CLI command set for managing and monitoring the PDU includes the following commands:

- **?** command: PDU help query
- sys command: PDU system configure and setting
- net command: PDU net application configure and setting
- usr command: PDU user operation
- dev command: PDU device setting
- pwr command: PDU power setting

**NOTE:** Command variables are represented in command input syntax surrounded by angle braces (< >). Optional parameters are represented in command input syntax surrounded by straight brackets ([ ]). For data of type array, the 'x' character as index of array in command input syntax means all indexes. You must be logged into the PDU before commands can be sent. See Appendix A for a list of all CLI commands.

## Connecting to the CLI through the serial interface

Communicating through the serial port requires a specialized optional RJ45-DB9 cable or you can create your own cable as described in the “Serial Cable Pinout to Create Your Own Cable” section.




**Figure 21: Connect the RJ-45 end of the cable to the PDU In/Serial connector**

### *To connect the PDU to a computer:*

Using the optional RJ45-DB9 cable, connect the RJ-45 end to the port labeled “PDU In/Serial” on the front panel of your PDU model. Connect the DB9 end of the cable to the serial connector on the computer.

### *Logging in with HyperTerminal*

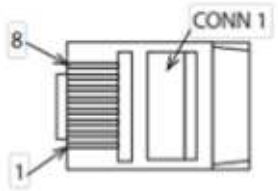
To login through HyperTerminal, set the COM settings to the following parameters:

- Bits per second: 115200
- Data bits: 8

- Parity: None
- Stop bits: 1
- Flow control: None

*Serial Cable Pinout to Create Your Own Cable*

To make your own RJ45-to-DB9 Serial cable, the connections are wired as shown:




| CONN 1 | | CONN 2 |
|---|---|---|
| Pin | Description | Pin |
| 1 | | 1 |
| 2 | RS232 RX | 2 |
| 3 | RS232 TX | 3 |
| 4 | | 4 |
| 5 | Ground | 5 |
| 6 | | 6 |
| 7 | | 7 |
| 8 | | 8 |
| | | 9 |

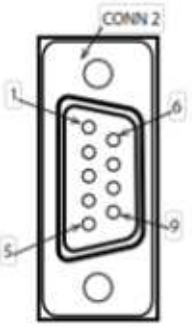



**Figure 22: Serial Cable Pinout**

**Logging in with SSH via PuTTY**

1. Ensure SSH has been enabled: On GUI, go to Device Configuration > Network Service > SSH. Select the **Enable SSH Access** checkbox. Select **OK**.
2. Open an SSH client (PuTTY).
3. Enter the IP address in the Host Name field. Select the connection type: SSH
    - For SSH, enter 22 in the Port field.
4. Select **Open**.
5. Enter your Username. Press **Enter**.
6. Enter your password. Press **Enter**.
7. You are now logged into the SSH. Refer to the CLI Commands table below for available commands.

**NOTE:** SSH connection is not available when serial connection is enabled.

# Section 5 – Local Display

## Onboard Display and Intelligent Network Controller (iNC)

The Onboard Display provides information about the PDU and connected devices. The PDU has a three-button, graphical iNC panel (see Figure 23). Use the buttons to change the screen display and retrieve specific data.




**Figure 23: iNC Display**

The iNC Display has three modes:

1. **Menu mode** (iNC Display main menu): When the PDU is powered up or when a button is pushed while in Standby Mode or Power Save mode.
2. **Standby mode**: This happens when a PDU is idle (no buttons pushed) for 30 seconds while in Menu mode.
    - In Standby mode, the PDU scrolls through key power values (Frequency, Amps, Volts, Watts, and kVA) and IP addresses (for both IPv4 and IPv6).
3. **Power Save mode**: The PDU enters Power Save mode when it has been in Standby mode for an hour. To exit Power Save mode, press any button on the display.

### Control Buttons

The table below summarizes how to use the control buttons on the iNC display.

| Button | When in Menu Mode | When in Screensaver Mode |
|---|---|---|
| **Menu** | Select from the four main menus. | Returns to the previous display screen before entering the screensaver mode. |
| **Scroll** | Scrolls down through the list of menu items.<br>**NOTE:** A highlighted menu item is ready to be selected. | Returns to the previous display screen before entering the screensaver mode. |
| **Select** | Opens the selected menu. | Returns to the previous display screen before entering the screensaver mode. |

### LED Unit Status

The LED will change colors depending on the state of the PDU.

| LED State | Description |
|---|---|
| Solid Green | Normal Operation |
| Solid Red | Critical or Warning Alarm |
| Flashing Orange | No network connection |

## iNC Menu Structure

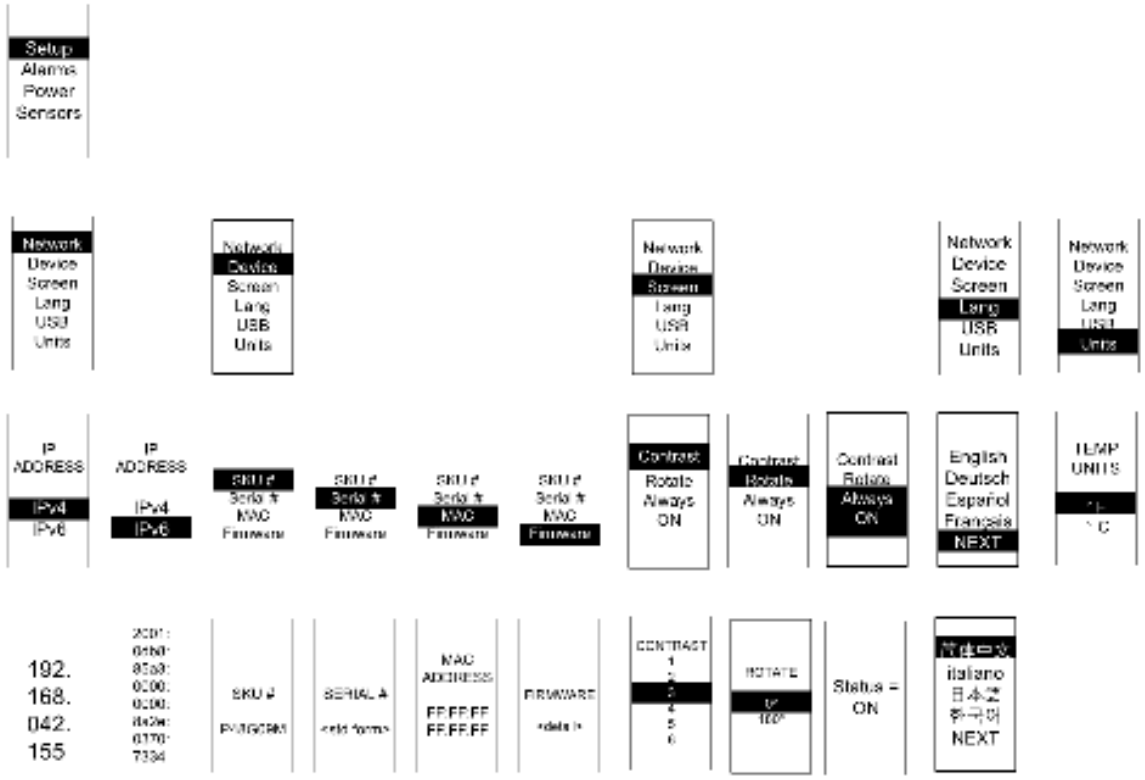



**Figure 24: iNC Menu Structure**

### Main Menu Selections

The PDU menu selection hierarchy consists of Setup, Alarms, Power, and Sensors. On the main menu, scroll down to highlight Setup. Press **Select**. Scroll down to select a submenu and press **Select** to display the submenu options. Press **Menu** to return to the previous menu.

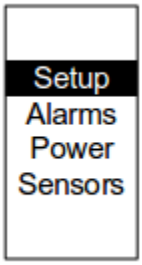



**Figure 25: Main Menu Selections**

**Setup Menu**

The Setup menu provides user configuration options including Network, Device, Screen, Language, USB, and Units.

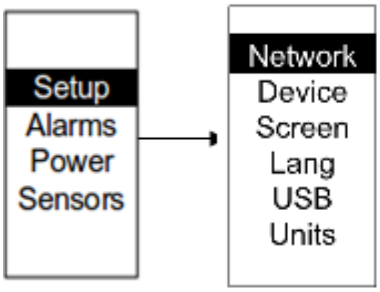



**Figure 26: Setup Menu**

*Network Submenu*

The Network submenu allows you to view IP address IPv4 or IPv6. On the Setup menu, scroll down to Network. Press **Select** to enter the Network Submenu. Scroll down to highlight the selected option from the menu. Press **Select** to display the screens that display the IP address. Press **Menu** to return to the previous menu.

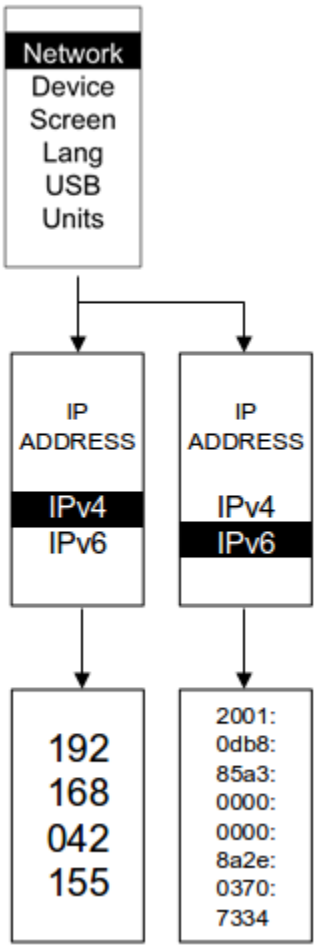



**Figure 27: Network Submenu**

### *Device Submenu*

The Device submenu provides the SKU number, Serial number, MAC address and Firmware version. On the Setup menu, scroll down to highlight Device submenu. Press **Select** to enter the Device Submenu. Scroll down to the item you wish to display, and press **Select**. Press **Menu** to return to the previous menu.

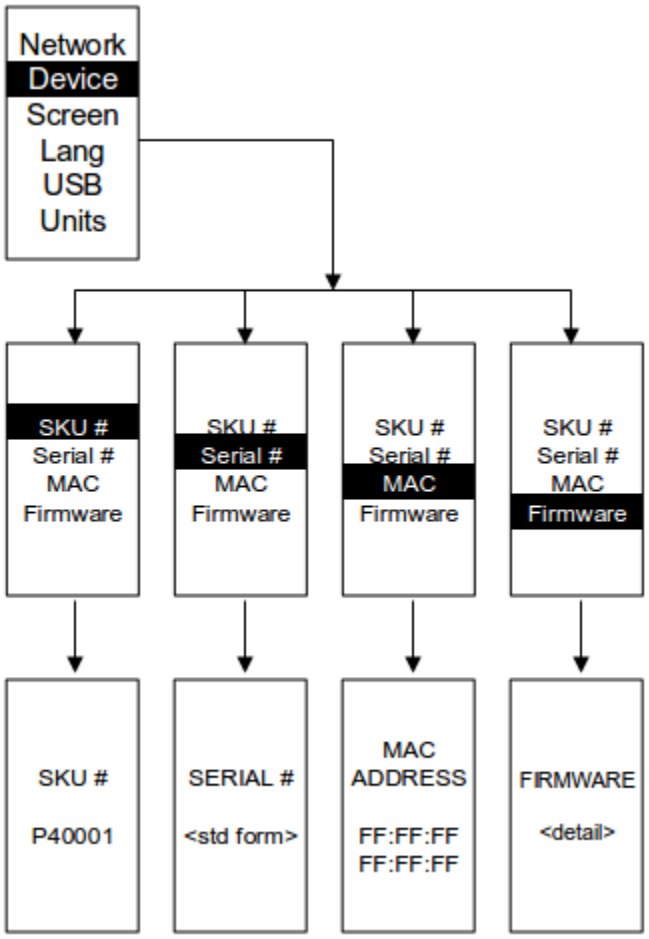



**Figure 28: Device Submenu**

### *Screen Submenu*

The Screen submenu allows you to customize settings for Contrast, Rotate, and Always on. In the Setup menu, scroll down to highlight Screen. Press **Select** to select the submenu. Press **Menu** to return to the previous menu.

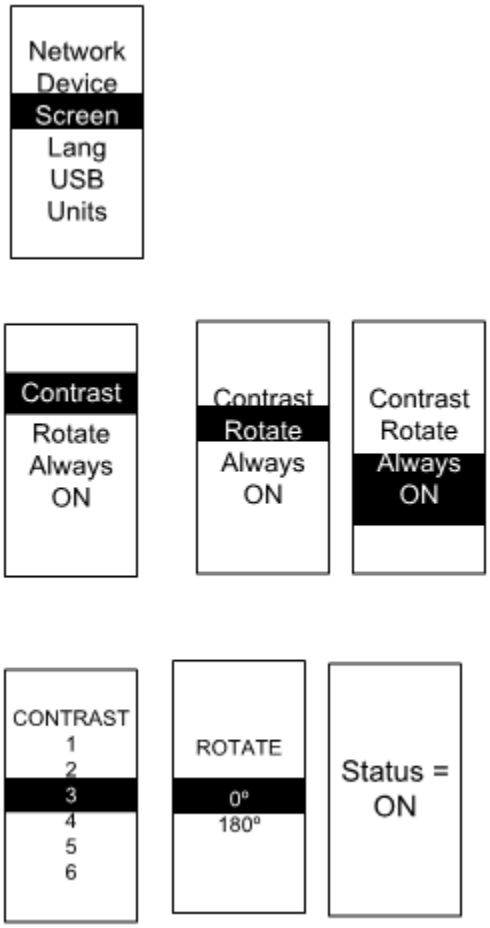



**Figure 29: Screen Submenu**

### *Language Submenu*

The Language submenu allows you to select the language you need to use. On the Setup menu, scroll down to highlight Lang. Press **Select** to display the screens to select the submenu. After you select the values, press **Select** to set the values as displayed on the screen. Press **Menu** to return to the previous menu.




**Figure 30: Language Submenu**

### *USB Submenu*

The USB submenu allows you to upload firmware file and download event log or data log. On the Setup menu, scroll down to highlight USB. Press **Select** to enter the USB Submenu. The user will be asked to verify the want to the enter the USB operation and Configuration Mode. After you select Yes, the system will reset in to the USB operation and Configuration Mode, or Boot Loader mode.

**Note**: If a USB drive is not present in the USB slot the PDU will enter normal operation after the reset.

**Note**: If you are in USB mode and you want to exit USB mode, you must remove the USB drive before existing USB mode. Otherwise, the PDU will reset and re-enter USB mode.

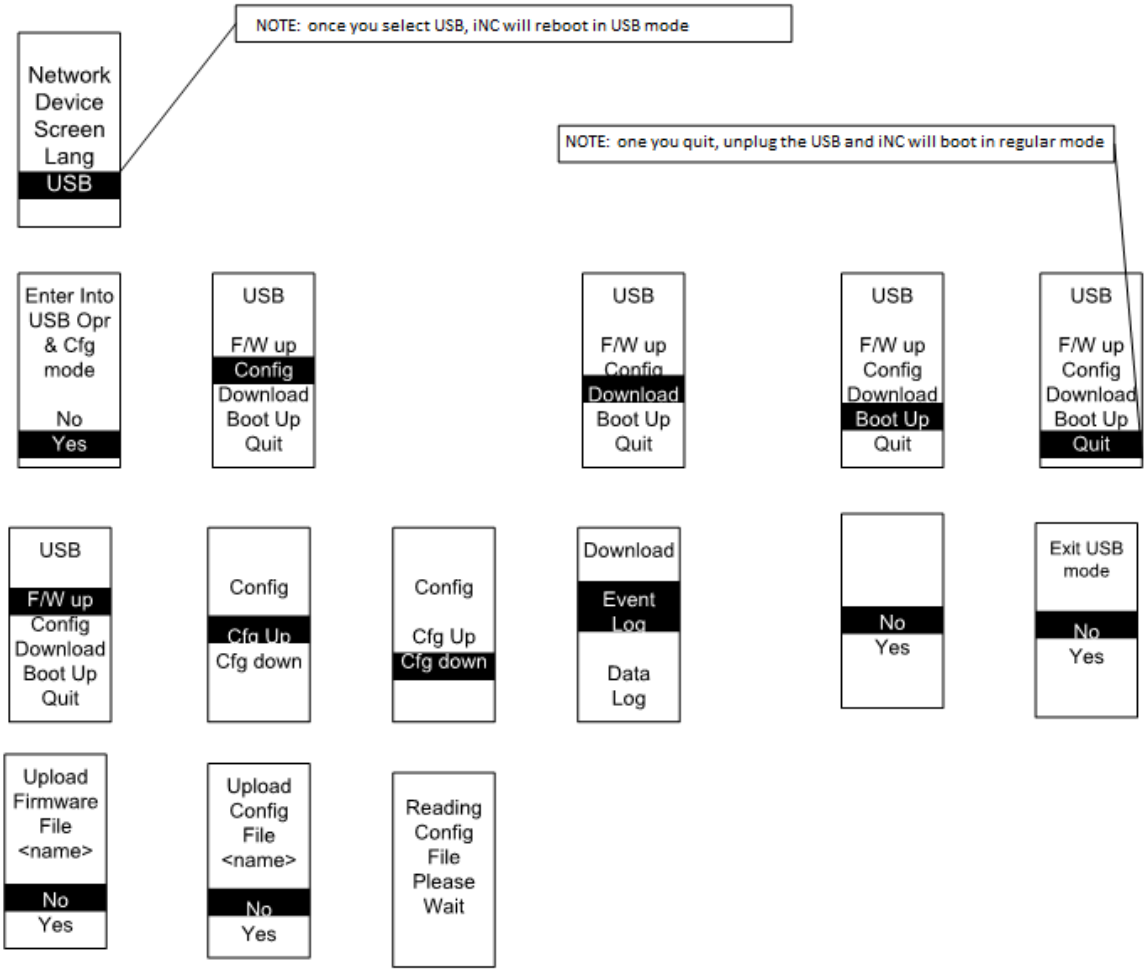



**Figure 31: USB Submenu**

*Units Submenu*

The Units submenu displays the temperature units. On the Setup menu, scroll down to highlight Units. Press **Select** to enter the Units Submenu. After you select the values, press **Select** to set the values as displayed on the screen. Press **Menu** to return to the previous menu.

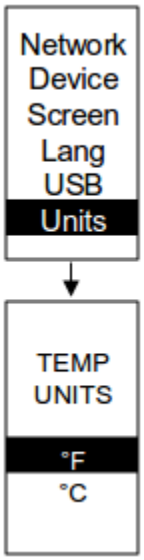



**Figure 32: Units Submenu**

### *Alarms Menu*

The Alarms menu displays active alarms for the PDU. On the Main Menu, scroll down to highlight Alarms. Press **Select** to display the Alarm Screen. When you finish your review, press **Menu** to return to the main menu.




**Figure 33: Alarms Menu**

*Power Menu*

The Power menu manages device, phase, breaker and outlet. On the Main Menu, scroll down to highlight Power. Press **Select**. Scroll down to select a submenu and press **Select** to display the submenu options. Press **Menu** to return to the previous menu.

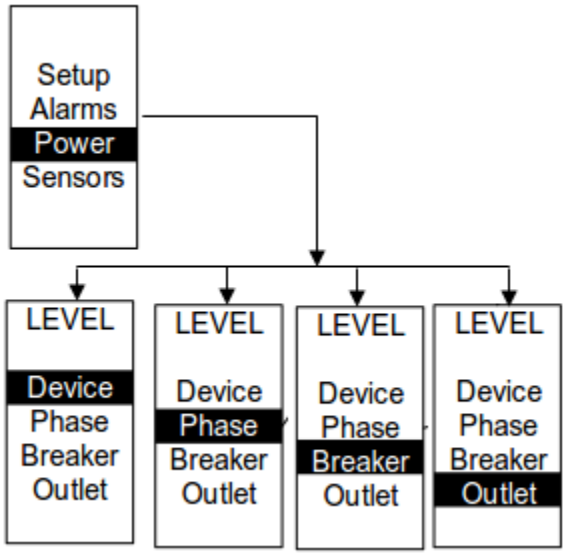



**Figure 34: Power Menu**

*Device Submenu*

The Device submenu is to display current, voltage and power. On the Power menu, scroll down to highlight Device. Press **Select** to display the power values for the entire PDU. Press **Menu** to return to the previous menu.

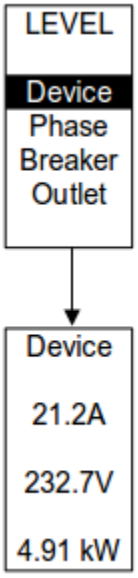



**Figure 35: Device Submenu**

*Phase Submenu*

The Phase submenu is to display the status of 3-Phase. On the Power menu, scroll down to highlight Phase. Press **Select** to display the screens to set the values for the submenu. After you select the phase, press **Select** to display the values for that phase on the screen. Press **Menu** to return to the previous menu.

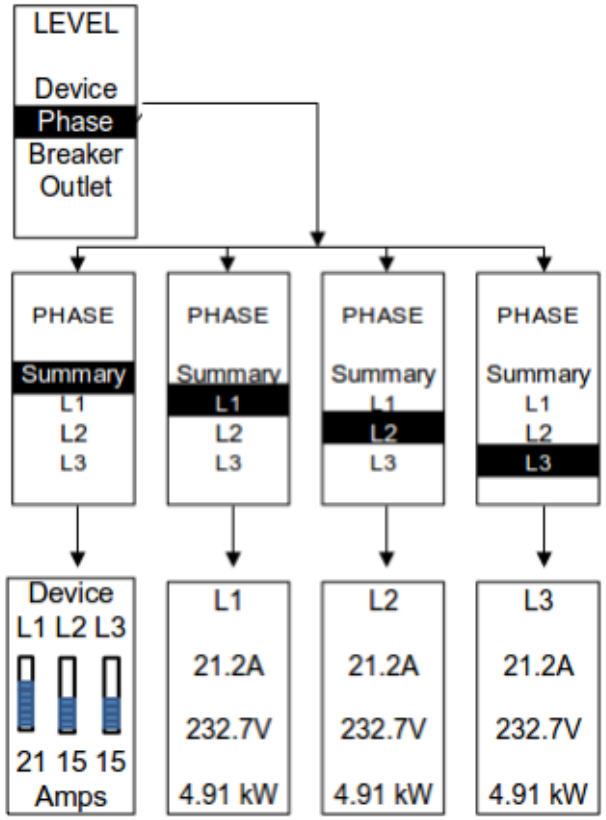



**Figure 36: Phase Submenu**

### *Breaker Submenu*

The Breaker submenu is to display power values for the breakers. Press **Select** to display the values of the first breaker. To go to the next breaker, **Select** next. Press **Menu** to return to the previous menu.

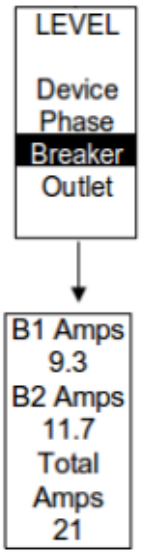



**Figure 37: Breaker Submenu**

### *Outlet Submenu*

The Outlet submenu is to display voltage, current and power from outlet number 1 to number n. On the Power menu, scroll down to highlight Outlet. Press **Select** to display values for the first outlet. To go to the next outlet, **Select** next. Press **Menu** to return to the previous menu.

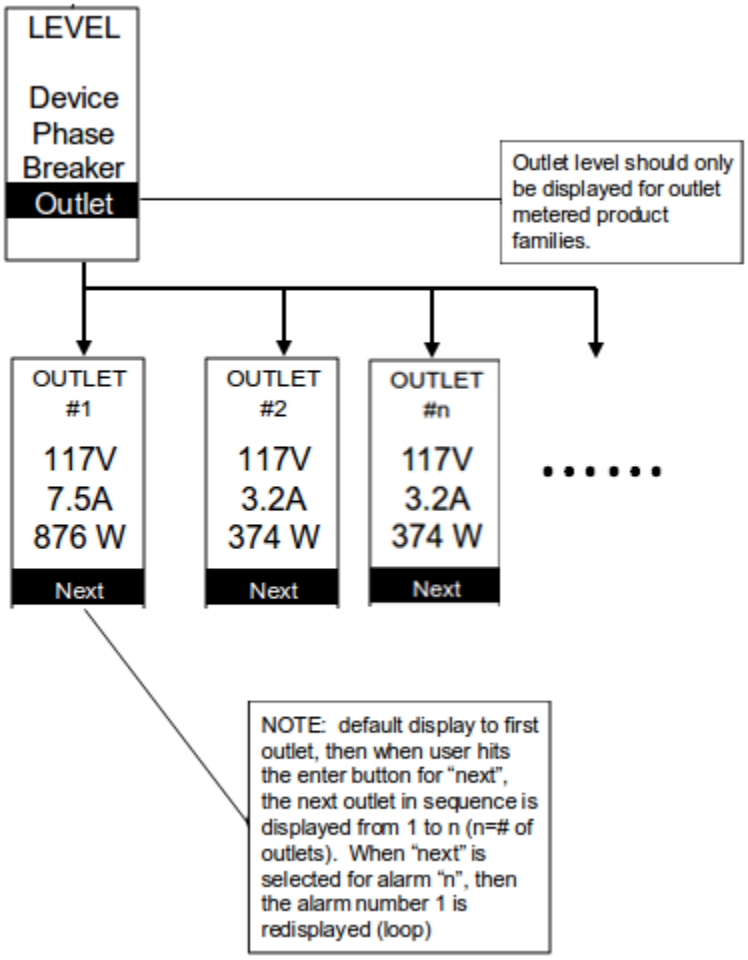



**Figure 38: Outlet Submenu**

## Sensors Menu

The Sensor menu is to display temperature, humidity, door switch, fluid leak etc. On the Main Menu, scroll down to highlight Sensor. Press **Select**. This will display the sensor data for the first sensor. To go to the next sensor, **Select** next. Press **Menu** to return to the previous menu.

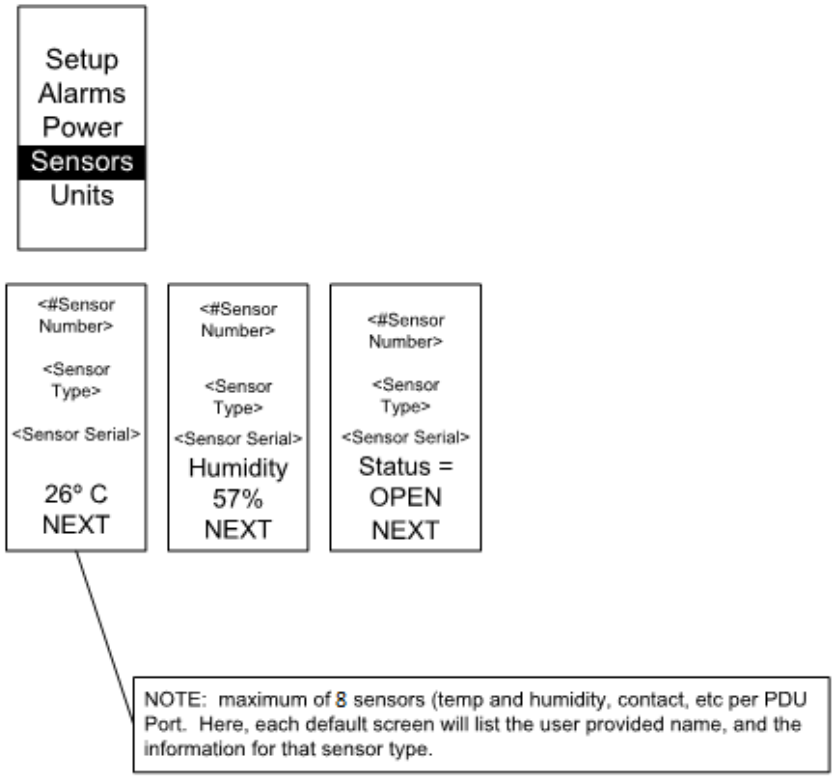



**Figure 39: Sensors**

**NOTE:** Maximum of 8 sensors are configured per PDU.

# Section 6 – User Access

## *Changing Your Password*

At initial login, you are required to change the default password:

1. Enter the current password and new password twice to confirm. By default, passwords must be between 8 and 32 characters.

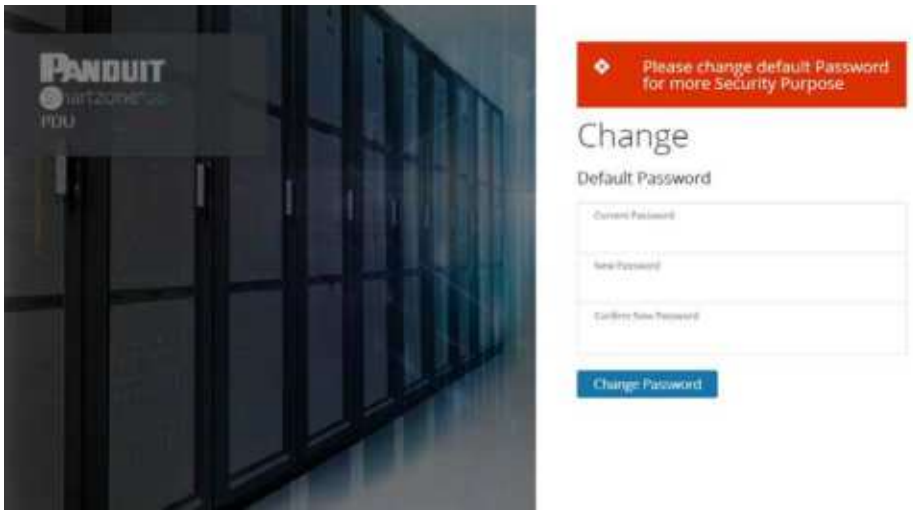



**Figure 40: Changing Your Password**

2. Click **Change Password** to complete the password change.

After the initial login, change the password by the following steps:

1. Go to **User Name** and select **Change Password**.




**Figure 41: After Login**

2. The Change User Password window opens.

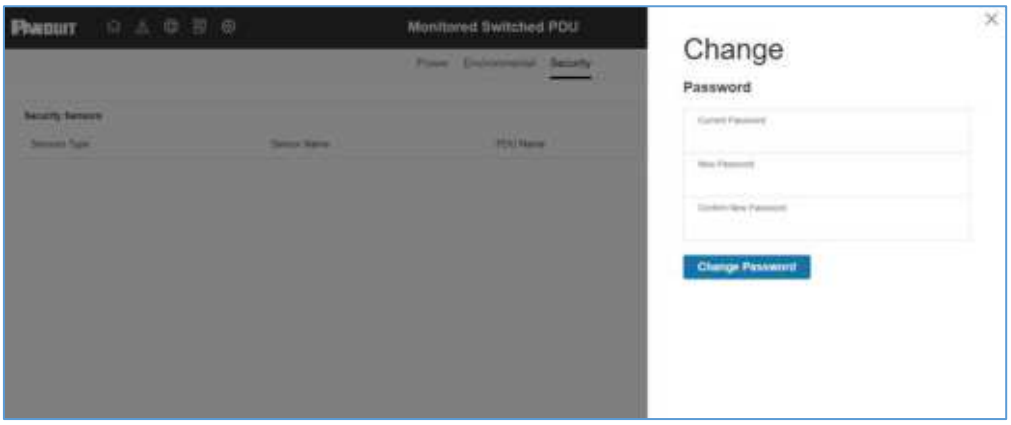



**Figure 42: Change User Password**

3. Enter the old password and then new password twice to confirm. By default, passwords must be between 8 and 32 characters.

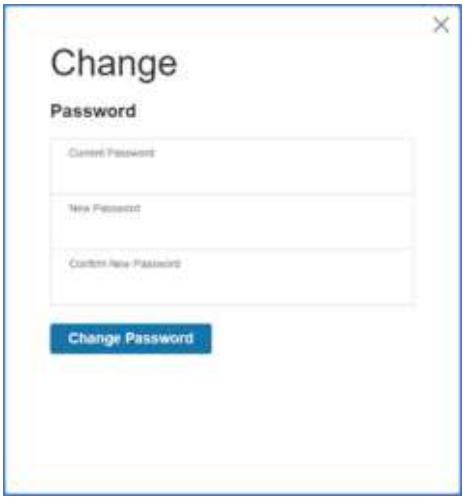



**Figure 43: Change Password**

4. Click **Change Password** to complete the password change.

### *Logging Out*

Users should logout after each session to prevent unauthorized changes to the system.

1. Click the **user name icon** in the top right corner of the screen (see Introduction to the Web Menu).
2. Click **Log Out** in the drop-down menu.

**Access Types**
There are two levels of access privileges:

- Administrator Privileges
- Read Only

The Panduit PDU comes with a standard **Administrator Privileges** profile and a standard **Read Only** profile. The “Admin Role” is typically the system administrator and has the Administrator Privileges with full operating permissions. By default, the User Role is a Read Only profile. All other users must be added by a user with administrator privileges. Users are defined by their unique login credentials and by their user role. The level of access privilege determines what the user will see and what actions the user can perform. The level of access privilege determines which menu items the user can access, or which fields display on individual setting and configuration dialogs. Before setting up users, determine the Roles that will be required. Each user must be given a Role. These Roles define the permissions granted to the user.

| Role | Default Permissions |
|---|---|
| admin | Full permissions that cannot be modified or deleted. |
| user | Read-only permissions. Can monitor the system but cannot change any configuration |
| manager | Full permissions that can be modified and deleted |

### *User Accounts*

Add a user with the following steps:

1. Go to **User Administration** and select **User Accounts**.
2. Select **Add User** to create a new user profile.
3. Use the Settings tab to enter the following information:
    - User Name (required)
    - Password (required)
    - Confirm Password (required)

**NOTE:** Set password requirements in the required field. By default, passwords must be 8-32 characters in length, and have at least one numeric character, and at least one special character.

4. Use the **Roles** tab to set full or read only privileges.
5. Select **Add User** to save the new user profile.

Modify user profile:

1. Go to **User Administration** and select **Users**.
2. Select the **User Name**.
3. Select **Edit**. Make changes to the user profile.
4. Select **Update**.

Delete user profile with the following steps:

1. Go to **User Administration** and select **Users**.
2. Select the red **X** next to user name.

## Setting Up the System for Radius Authentication

1. Go to **User Settings** in the admin menu.

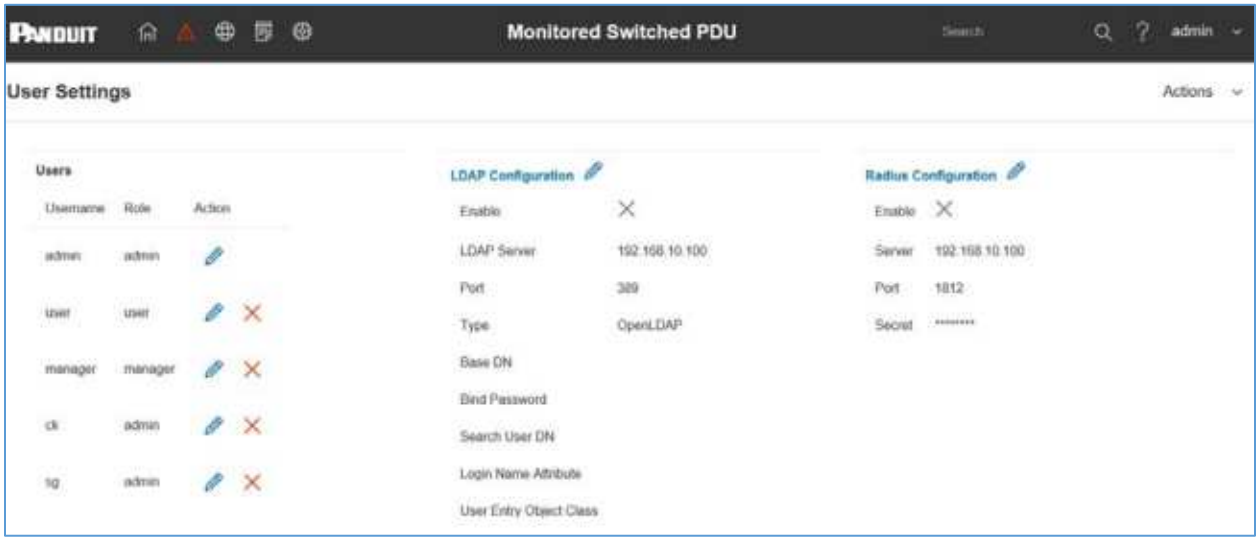



**Figure 44: User Settings**

2. Go to **Radius Configuration** and click the edit pencil.

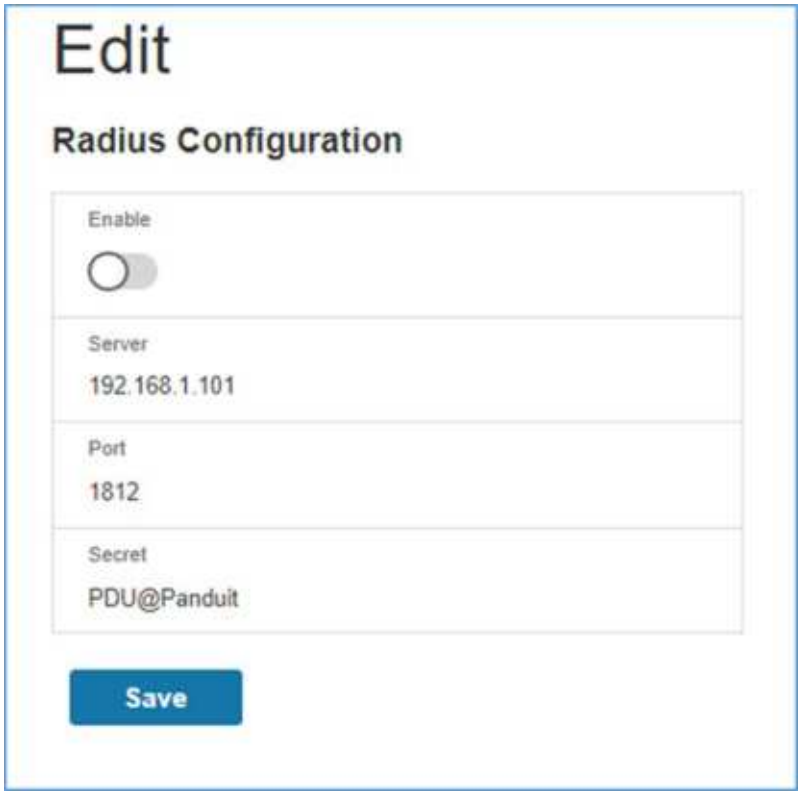



**Figure 45 Radius Configuration**

3. Select the **Enable** button.
4. Enter Server IP address field, Port number field, and Secret field.
5. Click save and your Radius authentication is complete.

## Configuring the system with LDAP Server Settings

To setup LDAP to access the Active Directory (AD) and provide authentication when logging into the PDU via the Web Interface:

1. Go to User Settings (under the ADMIN Menu) > LDAP Configuration.
2. Select the LDAP Enable checkbox.
3. Use the drop-down menu to choose the Type of LDAP Server. Choose Microsoft Active Directory.
4. Enter an IP Address of the domain controller/Active Directory (AD) Server.
   *i.e.: 192.168.1.101 (example)*
5. Enter a Port.
   **Note**: For Microsoft, this is typically 389.
6. In the Base DN field, enter in the account to be used to access AD.
   *i.e. CN=myuser, CN=Users, DC=EMEA, DC=mydomain, DC=com*
7. Enter the password in the Bind Password and Confirm Password fields.
8. In the Search User DN field:
   DC=subdomain
   DC=mydomain
   DC=com 10
9. In the Login Name Attribute field, enter **sAMAccountName** (typically).
10. In the User Entry Object Class field, enter person.

With these LDAP settings configured, the Bind is complete.

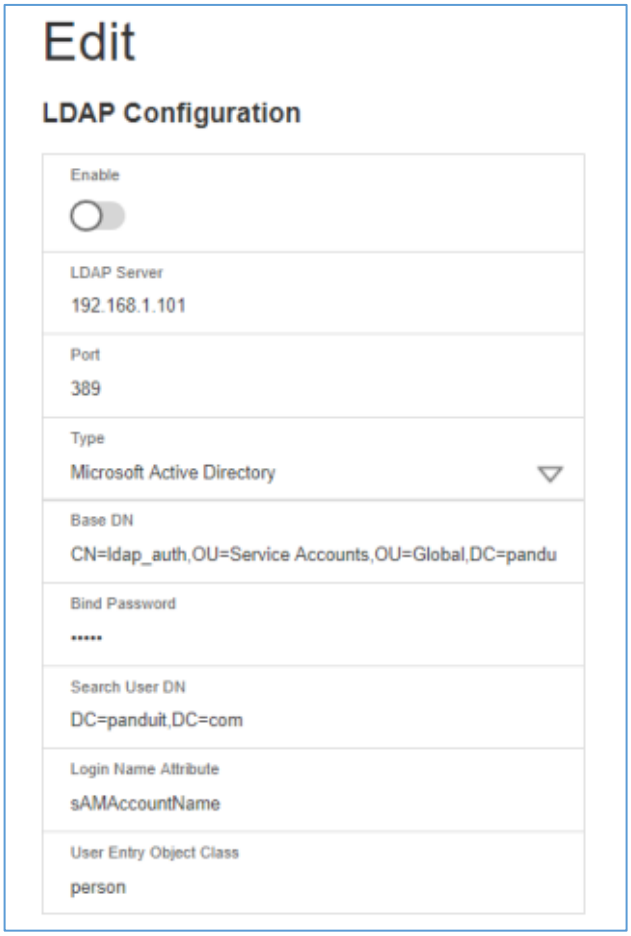



**Figure 46: LDAP Configuration**

Once LDAP is configured, the PDU must understand for which group authentication occurs. A role must be created on the PDU to reference a group within the Active Directory (AD).

1. Within the Active Directory, create a group for the users that you wish to be PDU administrators. *i.e. admins*
2. Within the G5 PDU Web Interface, go to **User Settings** (under admin menu) > **Roles**. Enter the **Role Name** that was created in AD. *i.e. admins*
3. Enable role privileges as needed (pictured below).

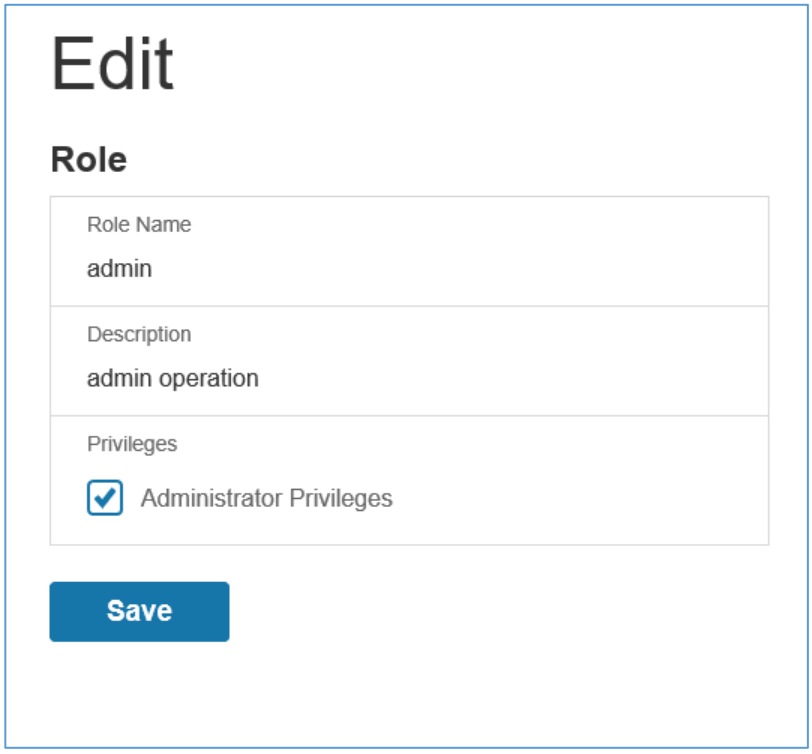



**Figure 47: Enable Role Privileges**

4. LDAP authentication is ready to use.
5. Click save to test and click **LDAP Configuration** again.
6. Type an Active Directory user name/password into the test box.
7. Click **Test LDAP Configuration**.
    - If a box pops up with all green **SUCCEEDED** (no X's), the LDAP is successfully configured.

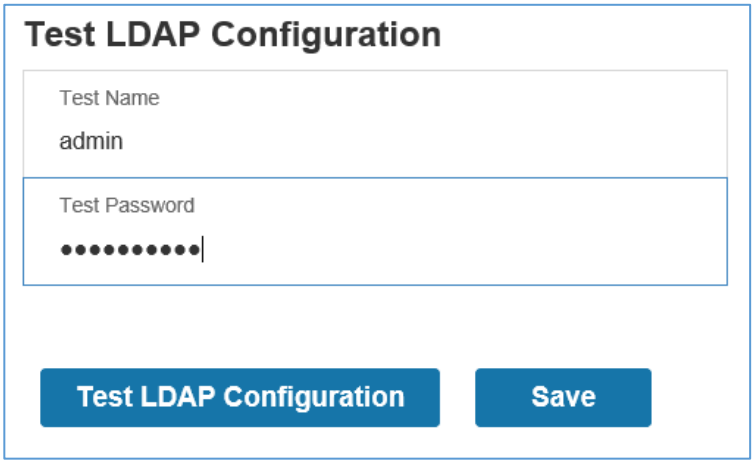



**Figure 48: Test LDAP Configuration**

**Note**: Be sure to log in without a domain name.

# Section 7 – Daisy Chain Configuration

## Daisy-Chain Overview

In daisy chain mode, up to four PDUs of the same SKU number can be connected via one IP address. This allows users to gather information and data on all daisy-chained PDUs from the master PDU. The daisy chain functionality reduces network cost for PDUs. For example, a standard network switch used in a data center may contain 24 ports. Without using the daisy chain function, each port would supply network connection to one PDU. However, if using the daisy chain features, a typical network switch with 24 ports can supply network connections for up to 96 PDUs.

## Daisy-Chain Setup

1. After the initial PDU is configured, connect an Ethernet cord from the **PDU Out** port on the configured PDU to the **PDU In/Serial port** on the second PDU in the daisy chain line.
2. Repeat step 2, connecting PDUs from the **PDU Out** port to the **PDU In/Serial** port for up to 4 PDUs.

   **Note:** The total length of the Ethernet cords connecting the PDUs must be less than 15m (49 ft.).
3. Go to the Web interface (or management software) to manage and control the PDUs in the daisy chain.

## RNA (Redundant Network Access) Functionality

RNA allows secure access of PDU data and statistics on two separate, private networks. RNA must be used with a redundant power delivery design including two rack PDUs for each IT rack. PDUs used in RNA applications must be the same SKU/Part Number.

How it works:

- Using RNA, the main and expansion unit maintain two separate private networks that do not overlap.
- RNA works using a redundant power delivery design (two rack PDUs for each IT rack).

- Each PDU is separately connected to the expansion and main unit's private communications network.
- The two PDUs relate to a data communications bus to allow PDUs to share user-defined information.

  Each PDU acts like a main PDU to report PDU data to both networks.

## RNA Setup

To set up RNA mode on two PDUs, the user must (1) configure the PDUs for RNA Mode (using CLI) and then (2) connect the LAN Network cords and Ethernet cords between PDUs.

**To Configure RNA Mode in the CLI**

1. Log in to the CLI and enter the command 'dev daisy rna.'
2. The following message will appear:
   - Reboot Required for change to take effort.
   - System Reboot now, Are you sure? (Y/N).
3. Enter **Y** to confirm reboot.
4. After reboot, the PDU will be setup to RNA Mode.
5. Repeat this process for the second PDU.

**To Connect the PDUs for RNA Setup**

After the PDUs are configured for RNA:

1. Connect an Ethernet cable from the Landlord LAN Network to the Ethernet port of the first PDU. This will have limited access/permissions.
2. Connect an Ethernet cable from the Tenant LAN Network to the Ethernet port of the second PDU. This will have full access to both PDUs.
3. Connect an Ethernet cable from the **PDU In/Serial** port on first PDU to the **PDU Out** port on the second PDU.

4. Connect another Ethernet cable from the **PDU Out** port on the first PDU to the **PDU In/Serial** port on the second PDU.
5. In RNA mode, the default account username is ‘landlord’ and password is ‘12345678’. This account is configured for proper access and control in RNA mode.
6. To enable this account, login to the CLI with admin credentials.
7. Enter the command ‘**dev daisy rna init**’.
8. The following message will appear to confirm the landlord account is enabled: SUCCESS.
9. RNA is now configured and enabled.

# Section 8– Web GUI configuration

## System Management Information

The system management information is a way to distinguish the PDU system's name and location inside the data center.

To configure the system management information, select **System Management** under the **gear** icon.




**Figure 49: System Management**

### *System Info*

The system information includes the name of the PDU system and information of the person to contact in case an issue arises. Follow the steps below to set up the system information:

1. Select the **pencil** icon next to **System Management.**

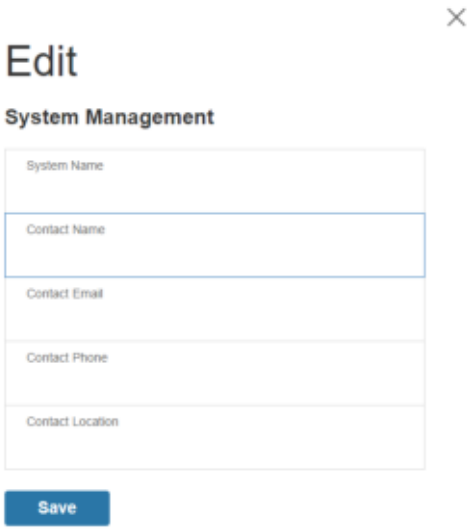



**Figure 50: System Management Configuration**

2. Enter the **System Name**: The “system” is the main PDU and all daisy-chained PDUs. A system can have 4 PDUs.
3. Enter the name of the person who should be contacted if there is a problem with the system into the **Contact Name** section.
4. Enter the email of the contact person into the **Contact Email**.
5. Enter the phone number of the contact person into **Contact Phone**.
6. Enter the location of the contact person into the **Contact Location**.
7. Press **Save**.

### *Rack Location*

The rack location describes the physical location of the rack or cabinet where the PDU system resides. To setup the system information, follow these steps.

1. Select the **pencil** icon next to **Rack Location.**




**Figure 51: Rack Location Configuration**

2. Enter the room location of the rack or cabinet that contains the PDU system into **Room Name.**
3. Enter the name of row where the PDU is located in **Row Name**.
4. Enter the position of the row where the PDU is positioned in **Row Position**.
5. Enter the ID of the rack/cabinet where the PDU is located into **Rack ID**.
6. Enter the height of the rack/cabinet where the PDU is located into **Rack Height**.
7. Press **Save**.

### *Power Panel & Core Location*

The **Power Panel & Core Location** describes the name of each PDU that is part of the PDU system. It also indicates the location of the PDUs inside the rack or cabinet. To configure, follow these steps:

1. Select the **pencil** icon next to **Power Panel & Core Location**.

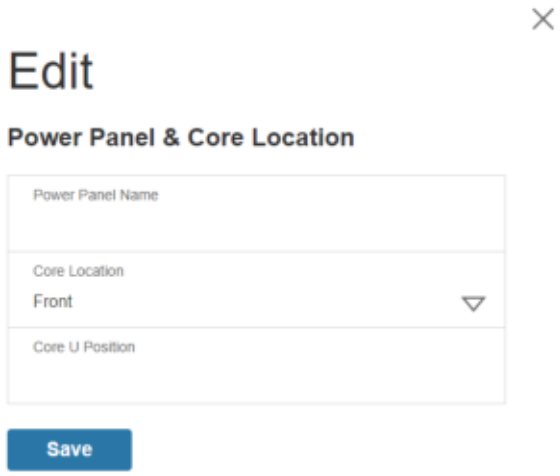



**Figure 52: Power Panel & Core Location**

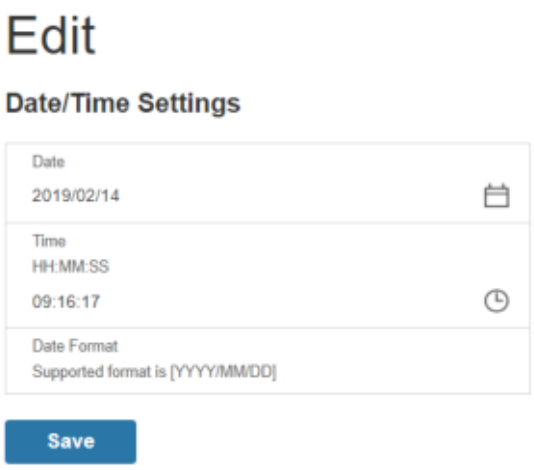
2. Enter the name of the PDU in the **Power Panel Name**.
3. Select **Front** or **Back** for the **Core Location.** The **Core Location** is the side of the rack/cabinet where the PDUs are installed. For vertical PDUs, they are typically installed in the back.
4. Enter the rack unit (RU) location into the **Core U Position**. Vertical PDUs are usually installed in the 0 RU space.
5. Press **Save**.

## Setting Time and Date on the PDU

You can set the internal clock manually or link to a Network Time Protocol (NTP) server and set the date and time:

### *Manually Setting Time and Date*

1. Go to **Network Settings** and select **Date/Time Settings**.




2. Enter the date using the YYYY-MM-DD format or use the calendar icon to select a date.
3. Enter the time in the three fields provided: the hour in the first field, minutes in the next field, and seconds in the third field. Time is measured in 24-hour format. Enter 13 for 1:00pm, 14 for 2:00pm, etc.
4. Press **Save**.

### *Link to a Network Time Protocol (NTP)*

1. Go to **Network Settings** and select **Network Time Protocol** (NTP).

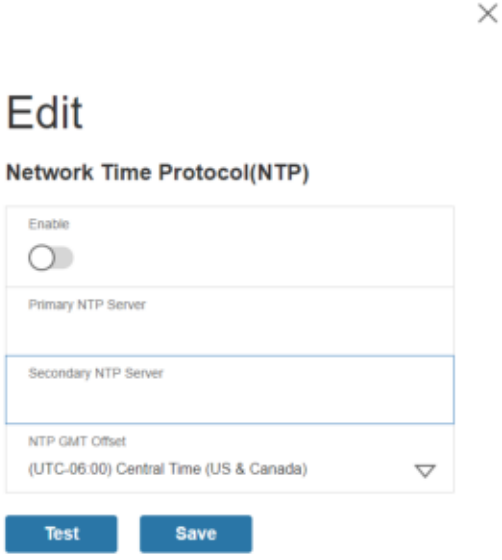



**Figure 53: NTP Configuration**

2. Click **Enable** to enable NTP.
3. Enter the IP address of the primary NTP server in the **Primary NTP Server** field.
4. Enter the IP address of the primary NTP server in the **Secondary NTP Server** field.
5. Select the appropriate time zone from the Time Zone drop-down list.
6. Press **Save**.

### *Setting Daylight Saving Time*

1. Go to **Network Settings** and select **Daylight Saving Time**.




**Figure 54: Daylight Saving Time Configuration**

2. Ensure **Enable** is selected.
3. Select the specifics of the **Start Month**:
   - Month
   - Week
   - Day
   - Time

4. Select the specifics of the **End Month**:
   - Month
   - Week
   - Day
   - Time
5. Set the **Time Offset**.

## G5 iPDU Outlet Power Sequence Setup

1. From the **PDU GUI Home Menu,** select **Control & Manage**.

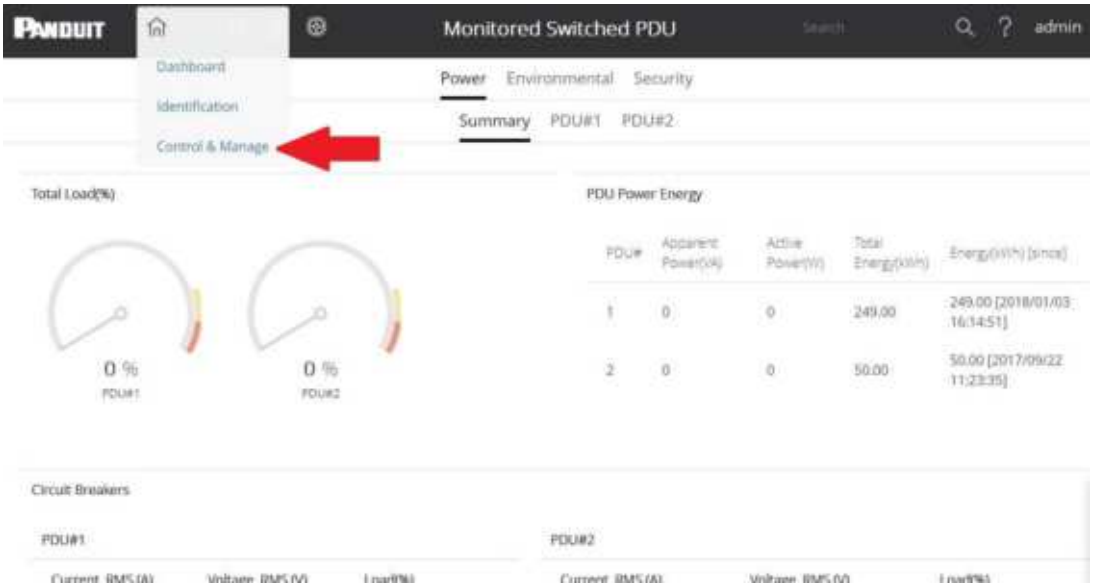



**Figure 55: Control & Manage PDU**

2. Select **Outlet Control Enabled**.

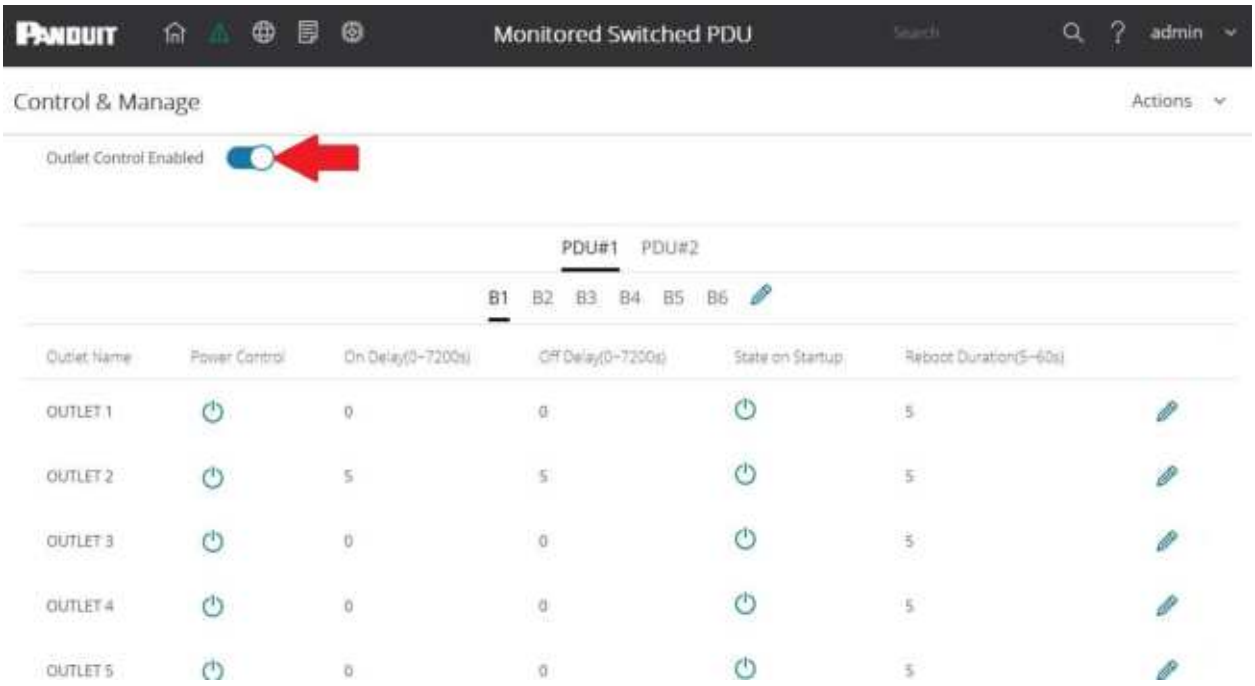



**Figure 56: Outlet Control Enabled**

3. For each Outlet select the **Edit** pencil.

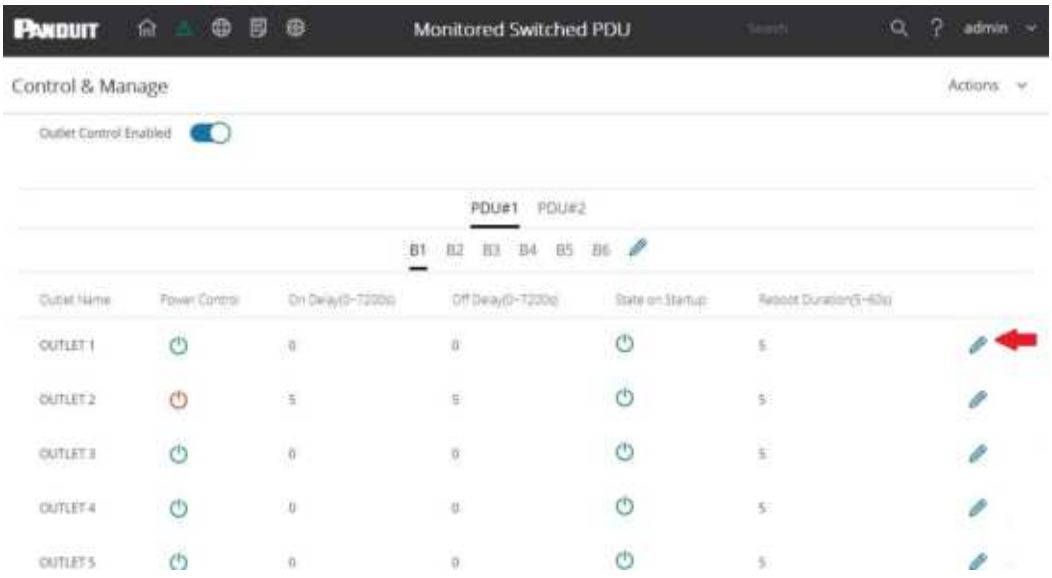



**Figure 57: Edit Outlets**

4. In the Edit Outlet window enter the **On-Delay** time (0-7200 seconds) then select **Save**.

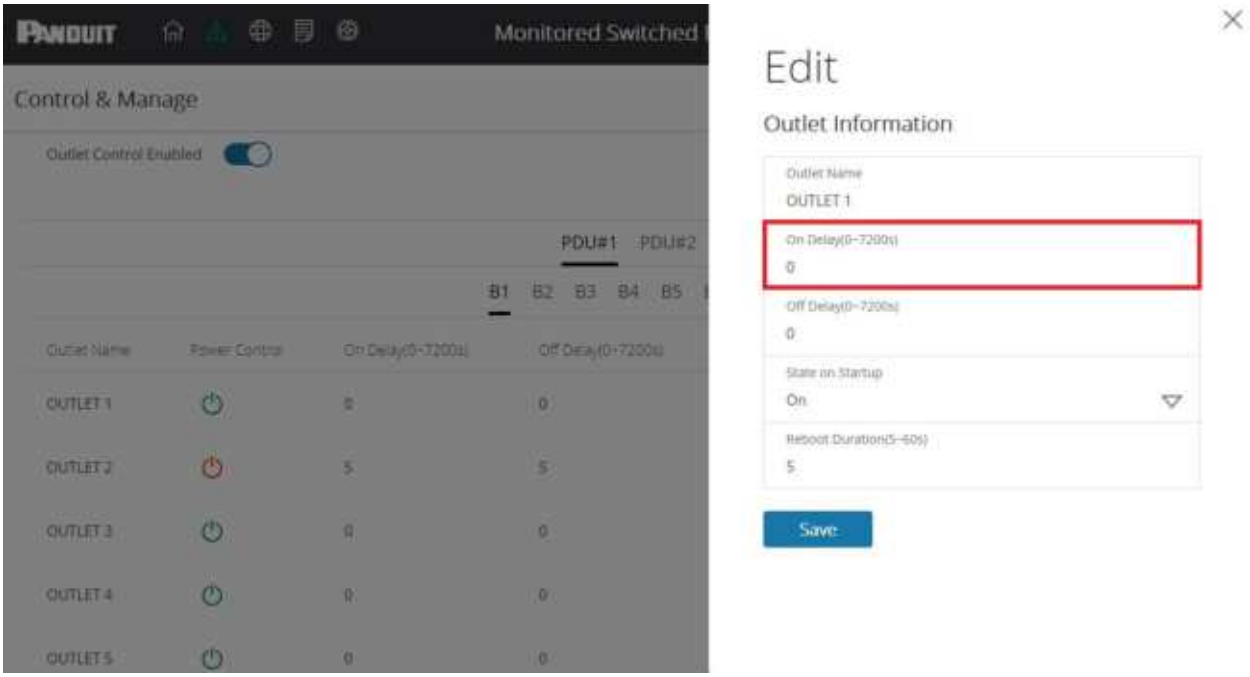



**Figure 58: One-Delay Time**

5. Your Outlet Power Sequence has been set.

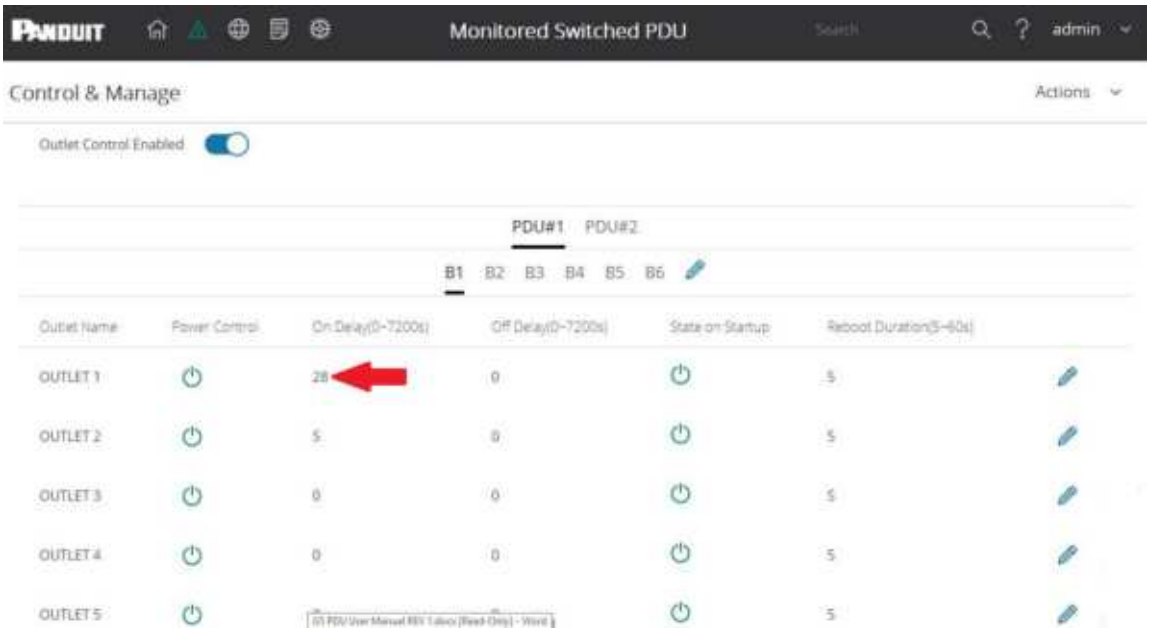



**Figure 59: Saved Sequence**

# Outlet Power Management

## *Naming an Outlet*

For Panduit G5 iPDUs with outlet level control or monitoring, you can customize each outlet and view all circuit breaker to outlet associations through the G5 M-Series GUI.

1. In the Control & Manage tab, expand the **Outlet Information** folder by clicking the pencil icon.
2. Select the outlet to name. In the data panel, select the value field for the Outlet Name.
3. Delete the default name and type the new name.
4. Press **Enter**.

## *Setting the Outlet Default State*

Setting the Outlet Default State on Panduit G5 iPDUs with outlet level control allows the user to determine the initial power status of an individual outlet upon PDU power up.

1. Expand the Outlet Information folder from the Control & Manage tab.
2. In the PDU settings dialog box, choose a selection from the State on Startup dropdown menu:
   - **On**: this will turn an outlet on upon initial startup

- **Off**: this will turn an outlet off upon initial startup
- **Last Known**: this will restore outlets to the last known power states before the device was shut down

### *Switching an Outlet On or Off*

This is only applicable to outlet-switched PDUs.

- Outlets on the switched PDU models in the Panduit G5 iPDU are easily switched on, switched off, or power cycled. This action requires the user to have Administrator Privileges.

1. Select the Control & Manage folder from the Home icon.
2. In the Power Control panel, select the outlet that must be switched on, switched off, or reboot.
3. Select the desired Power Control from the dropdown menu.
4. Select Apply.

### *Setting the Outlet Power On/Off Delay for Panduit G5 iPDUs*

This is only applicable to outlet-switched PDUs. When the PDU is turned ON, outlets will consecutively power on from Outlet 1 to the highest available outlet number.

1. Select the **Home Icon** then **Control & Manage** from the drop-down menu in the Web UI.
2. Select the outlet(s) for which to set a delay by clicking on the pencil icon.
3. Configure the length of the delay and/or length of reboot.
4. Select **Save.**

## Setting Metering Thresholds

### *Power Threshold*

The G5 iPDU will send alert notifications when a power threshold wattage crosses above or below the settings you specify in the Power Threshold configuration:

1. Go to the **Thresholds** > **Input Page**.
2. Click the pencil for the Power Threshold to update.

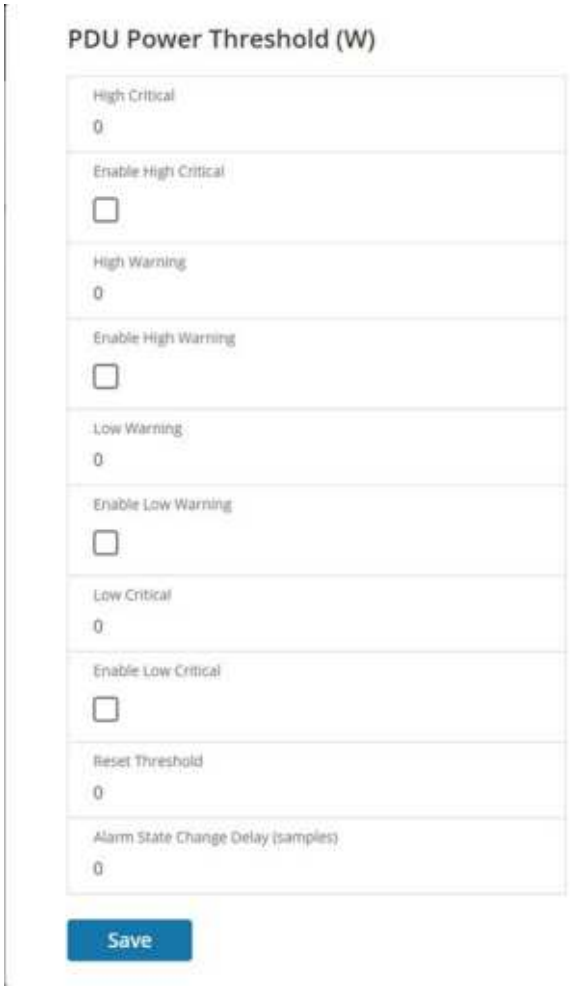



**Figure 60: Power Threshold**

3. Select and enter the appropriate thresholds in amps and click **Save**.
    - Lower Critical (W)
    - Lower Warning (W)
    - Upper Warning (W)
    - Upper Critical (W)
    - Reset Threshold (W)

      The Reset threshold is the number of watts the reading needs to fall below the threshold setting for the condition to be cleared.
      For example, the current critical threshold for the input phase is set to 19

watts (W). The current draw rises to 20W, triggering a Current Critical alert. The current then continues to fluctuate between 18.1W and 20W. With the reset threshold set to 1W, the PDU continues to indicate that the current on the input phase is above critical. Without a reset threshold (that is, the reset threshold is set to zero), the PDU would de-assert the condition each time the current dropped to 18.9W and re-assert the condition each time the current reached 19W or higher. With the fluctuating current, this could result in repeating event notifications, such as SNMP traps, SMTP alerts or Syslog notifications.

- Alarm State Change Delay (samples)

  If enabled, the PDU asserts any warning or critical condition only after a specified number of consecutive samples that cross a threshold are generated. This prevents several threshold alerts from being generated if the measurements return to normal immediately after rising above an upper threshold or dropping below a lower threshold.

4. Repeat steps 1 - 3 for all PDUs.

### *Energy Threshold*

The G5 iPDU will send alert notifications when an energy threshold kilowattage crosses above or below the settings you specify in the Energy Threshold configuration:

1. Go to the **Thresholds** > **Energy Page**.
2. Click the pencil for the Energy Threshold to update.




**Figure 61: Energy Threshold**

3. Select and enter the appropriate thresholds in kilowatts and click **Save**.
    - Upper Critical (kWh)
    - Upper Warning (kWh)
    - Reset Threshold (kWh)
    - Alarm State Change Delay (samples)

      If enabled, the PDU asserts any warning or critical condition only after a specified number of consecutive samples that cross a threshold are generated. This prevents several threshold alerts from being generated if the measurements return to normal immediately after rising above an upper threshold or dropping below a lower threshold.
4. Repeat steps 1 - 3 for all PDUs.

### *Phase Current Alarm Threshold*

The G5 iPDU will send alert notifications when a phase current alarm amp crosses above or below the settings you specify in the Phase Current Alarm configuration:

1. Go to the **Thresholds** > **Phase Page**.
2. Click the Pencil for the Phase Current Alarm to update.

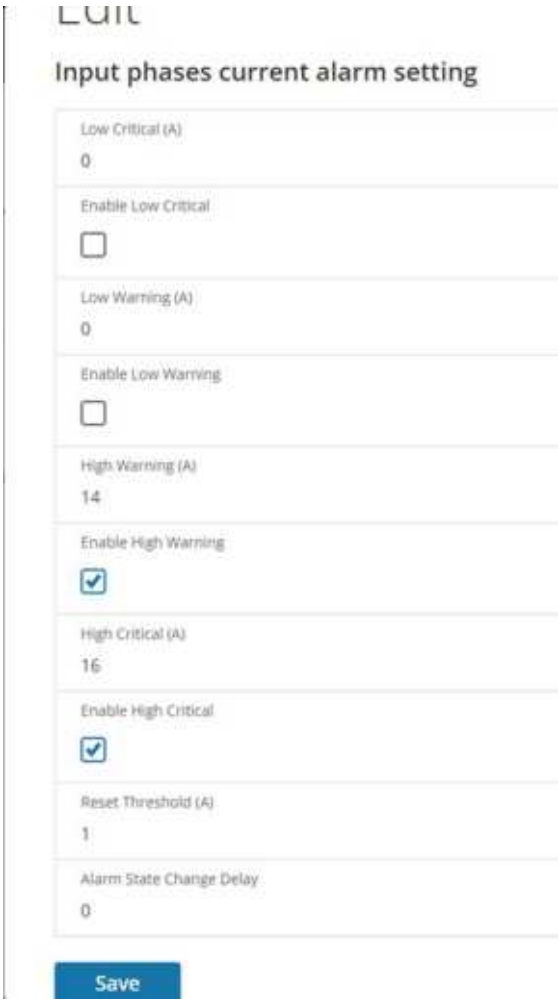



**Figure 62: Phase Current Alarm**

3. Select and enter the appropriate thresholds in amps and click **Save**.
    - Lower Critical (A)
    - Lower Warning (A)

- Upper Warning (A)
- Upper Critical (A)
- Reset Threshold (A)
- Alarm State Change Delay (A)

  The Reset threshold is the number of amperage the reading needs to fall below the threshold setting for the condition to be cleared.
  For example, the current critical threshold for the input phase is set to 19 amps (A). The current draw rises to 20A, triggering a Current Critical alert. The current then continues to fluctuate between 18.1W and 20W. With the reset threshold set to 1A, the PDU continues to indicate that the current on the input phase is above critical. Without a reset threshold (that is, the reset threshold is set to zero), the PDU would de-assert the condition each time the current dropped to 18.9A and re-assert the condition each time the current reached 19A or higher. With the fluctuating current, this could result in repeating event notifications, such as SNMP traps, SMTP alerts or Syslog notifications.

- Alarm State Change Delay (samples)

  If enabled, the PDU asserts any warning or critical condition only after a specified number of consecutive samples that cross a threshold are generated. This prevents several threshold alerts from being generated if the measurements return to normal immediately after rising above an upper threshold or dropping below a lower threshold.

4. Repeat steps 1 - 3 for all phases.

### *Phase Voltage Alarm Threshold*

The G5 iPDU will send alert notifications when a phase voltage crosses above or below the settings you specify in the Phase Voltage Alarm configuration:

1. Go to the **Thresholds** > **Phase Page**.
2. Click the pencil for the Phase Voltage to update.

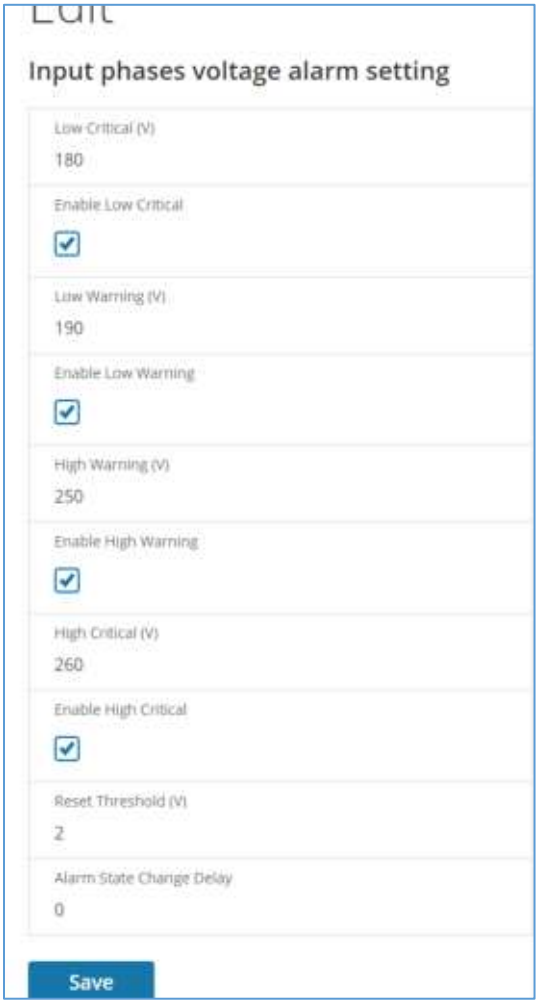



**Figure 63: Phase Voltage Alarm**

3. Select and enter the appropriate thresholds in voltage and click **Save**.
    - Lower Critical (V)
    - Lower Warning (V)
    - Upper Warning (V)
    - Upper Critical (V)
    - Reset Threshold (V)

      The Reset threshold is the number of amps the reading needs to fall below the threshold setting for the condition to be cleared.

For example, the current critical threshold for the input phase is set to 19 voltage (V). The current draw rises to 20V, triggering a Current Critical alert. The current then continues to fluctuate between 18.1V and 20V. With the reset threshold set to 1V, the PDU continues to indicate that the current on the input phase is above critical. Without a reset threshold (that is, the reset threshold is set to zero), the PDU would de-assert the condition each time the current dropped to 18.9V, and re-assert the condition each time the current reached 19A or higher. With the fluctuating current, this could result in repeating event notifications, such as SNMP traps, SMTP alerts or Syslog notifications.

- Alarm State Change Delay (samples)

  If enabled, the PDU asserts any warning or critical condition only after a specified number of consecutive samples that cross a threshold are generated. This prevents several threshold alerts from being generated if the measurements return to normal immediately after rising above an upper threshold or dropping below a lower threshold.

4. Repeat steps 1 - 3 for all phases.

### *Circuit Breaker Alarm Threshold*

The G5 iPDU will send alert notifications when a circuit breaker amperage crosses above or below the settings you specify in the Circuit Breaker Alarms configuration:

1. Go to the **Thresholds** > **Circuit Breaker Page**.
2. Click the pencil for the Circuit Break to update.

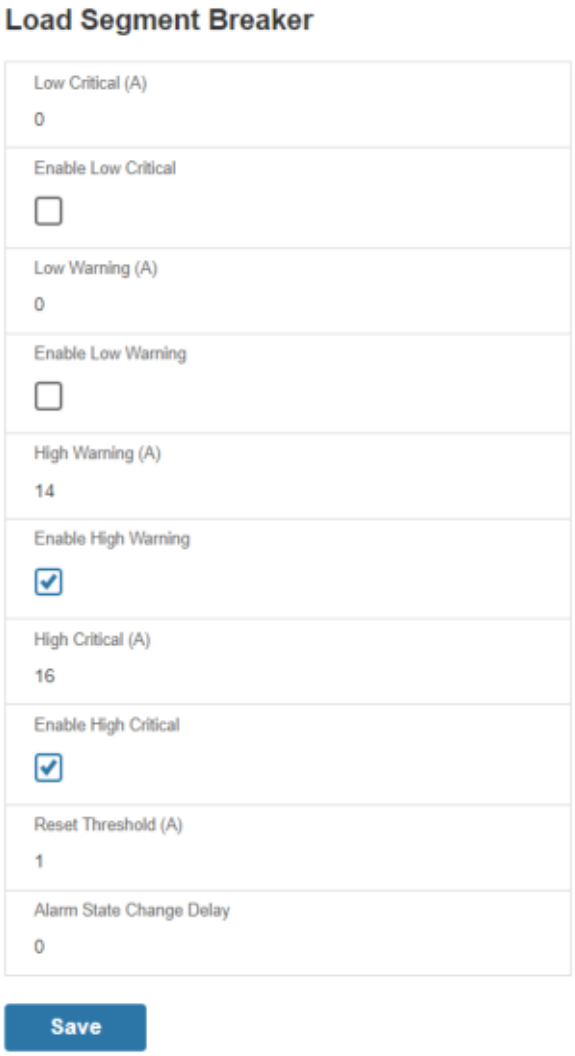



**Figure 64: Load Segment Breaker**

3. Select and enter the appropriate thresholds in amps and click **Save**.
    - Lower Critical (A)
    - Lower Warning (A)
    - Upper Warning (A)
    - Upper Critical (A)
    - Reset Threshold (A)

The Reset threshold is the number of amps the reading needs to fall below the threshold setting for the condition to be cleared.
For example, the current critical threshold for the input phase is set to 19 amps (A). The current draw rises to 20A, triggering a Current Critical alert. The current then continues to fluctuate between 18.1A and 20A. With the reset threshold set to 1A, the PDU continues to indicate that the current on the input phase is above critical. Without a reset threshold (that is, the reset threshold is set to zero), the PDU would de-assert the condition each time the current dropped to 18.9A and re-assert the condition each time the current reached 19A or higher. With the fluctuating current, this could result in repeating event notifications, such as SNMP traps, SMTP alerts or Syslog notifications.

- Alarm State Change Delay (samples)

  If enabled, the PDU asserts any warning or critical condition only after a specified number of consecutive samples that cross a threshold are generated. This prevents several threshold alerts from being generated if the measurements return to normal immediately after rising above an upper threshold or dropping below a lower threshold.

Repeat steps 1 - 3 for all circuit breakers.

### *Device Detection Threshold*

The Device Detection Threshold is the minimum threshold before current will be reported. Any detected current below the threshold will be reported as zero. To change this threshold, follow the following steps:

1. Go to the **Thresholds** > **Outlet Page**.
2. Click the pencil next to **Device Detection Threshold**.

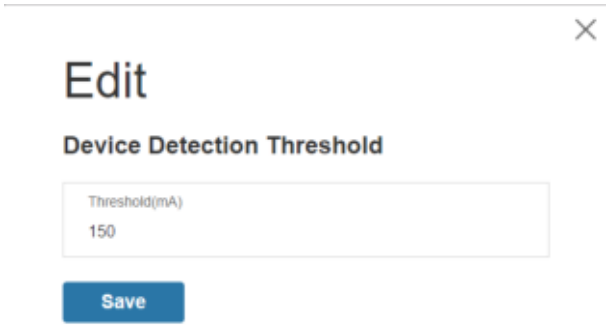



**Figure 65: Device Detection Threshold Information**

3. Change the value for the number of milli-amps to set the threshold.

### *Outlet Alarm Threshold*

The G5 iPDU will send alert notifications when an outlet amperage crosses above or below the settings you specify in the Outlet Alarms configuration:

1. Go to the **Thresholds** > **Outlet Page**.
2. Click the pencil for the Outlet to update.




**Figure 66: Outlet Information**

3. Select and enter the appropriate thresholds in amps and then click Save.
    - Lower Critical (W)

- Lower Warning (W)
- Upper Warning (W)
- Upper Critical (W)
- Reset Threshold (W)

  The Reset threshold is the number of amps the reading needs to fall below the threshold setting for the condition to be cleared.
  For example, the current critical threshold for the input phase is set to 19 watts (W). The current draw rises to 20W, triggering a Current Critical alert. The current then continues to fluctuate between 18.1W and 20W. With the reset threshold set to 1A, the PDU continues to indicate that the current on the input phase is above critical. Without a reset threshold (that is, the reset threshold is set to zero), the PDU would de-assert the condition each time the current dropped to 18.9W and re-assert the condition each time the current reached 19W or higher. With the fluctuating current, this could result in repeating event notifications, such as SNMP traps, SMTP alerts or Syslog notifications.

- Alarm State Change Delay (samples)

  If enabled, the PDU asserts any warning or critical condition only after a specified number of consecutive samples that cross a threshold are generated. This prevents several threshold alerts from being generated if the measurements return to normal immediately after rising above an upper threshold or dropping below a lower threshold.

Repeat steps 1 - 3 for all outlets.

# Email Setup

The G5 iPDU will send email (SMTP) notifications when thresholds are crossed.

1. From the top ribbon of the dashboard, go to the gear settings and select **Email Setup**.

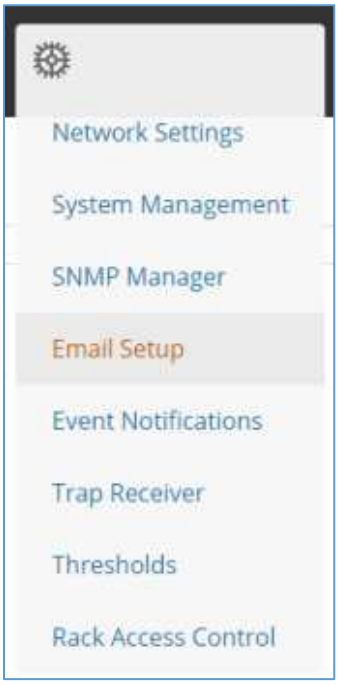



**Figure 67: Email Setup**

2. Select the pencil icon next to SMTP Account Settings and begin filling out the **Edit** screen.

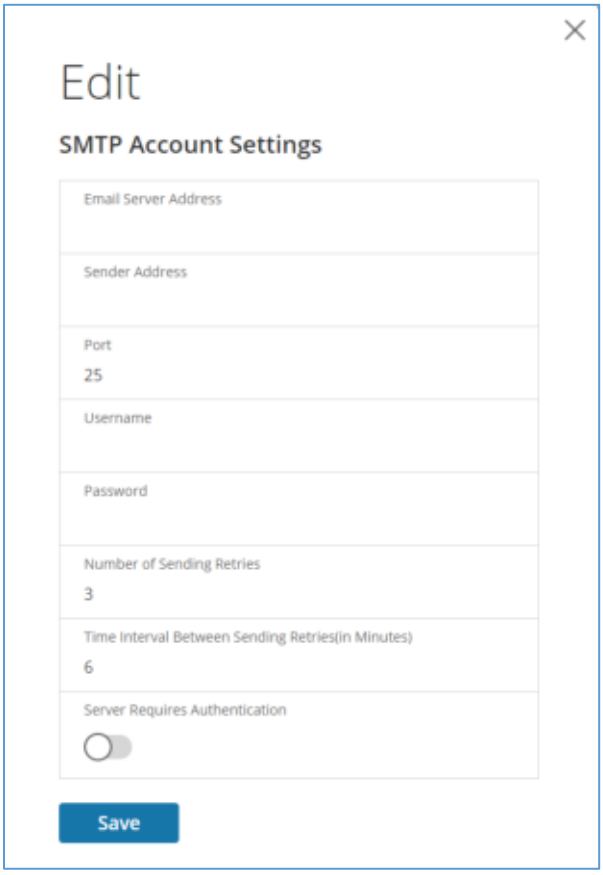



**Figure 68: SMTP Account Settings**

- Email Server Address
- Sender Address
- Port
- Username
- Password
- Number of Sending Retries
- Time Interval Between Sending Retires (In Minutes)
- Server Requires Password Authentication

3. Press **Save** when done.

Now the Email Recipients list must be filled out.

1. Select the pencil icon to display the Email Recipients screen.

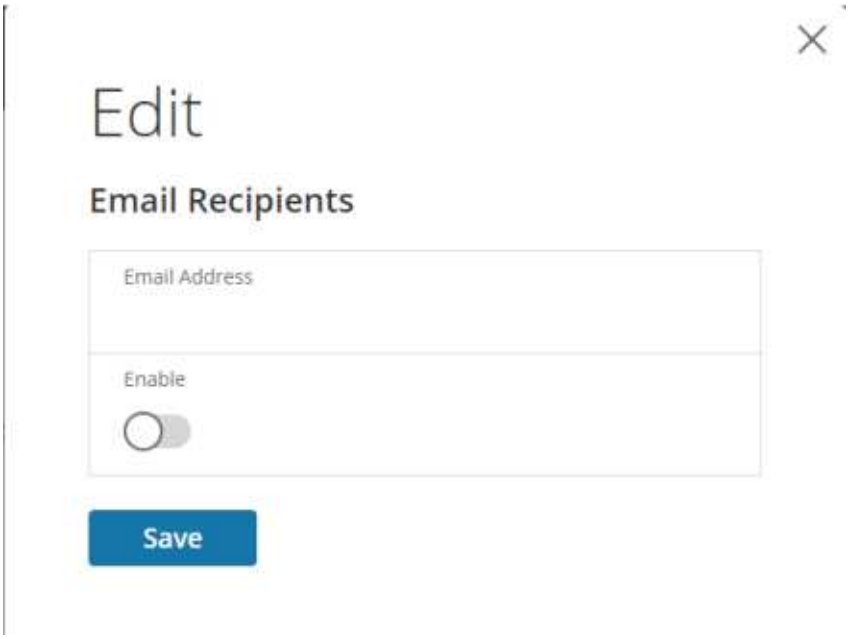



**Figure 69: Email Recipients**

2. Enter the desired email address and press **Enable**.
3. Press **Save**.

**Note**: Only five users are supported for email alerts.

# Data Log

The G5 PDU maintains a data log of 2000 records.

The period visible in the data log at any one time depends on the time between data log entries. The time range of each record can be configured from 1 to 1440 minutes. (As an example, if a data log is in an interval of 10 minutes, the entire data log contains 2000 records with up to 13.89 days of data.) Once the data log reaches the maximum of 2000 records, the oldest entries ae overwritten by the newer entries.

1. Go to **Logs** and select **Data Log**.

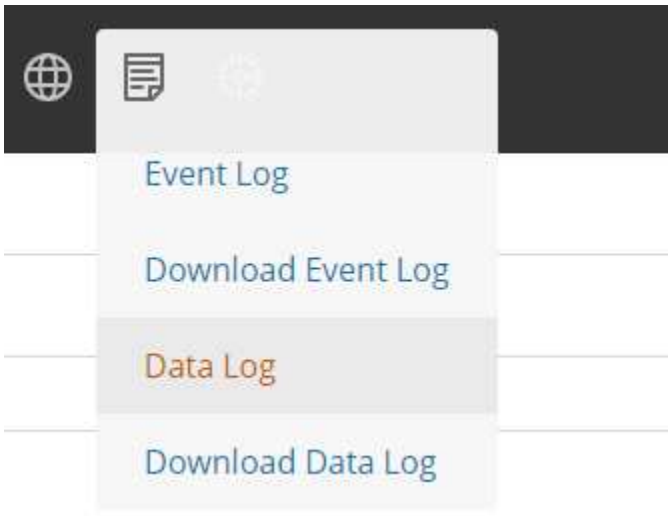



**Figure 70: Data Log**

2. Select the **Actions** drop-down menu and choose **Data Log Configuration**.

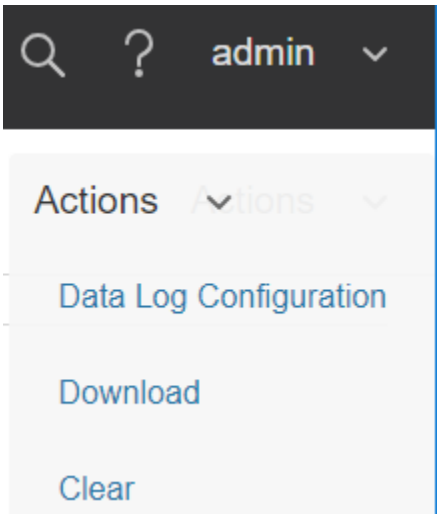



**Figure 71: Data Log Configuration**

3. **Enable** must be selected and enter an interval number in the **Log Interval** field. (Valid range is from 1 to 1440 minutes. The default time is 10 minutes.)
4. Select **Save**.

# Section 9 – Connecting and Configuring Optional Hardware

## Accessory Hardware Overview

All Panduit SmartZone G5 Intelligent PDUs can monitor environmental conditions of a rack with the addition of optional SmartZone G5 environmental sensors. Conditions such as temperature, humidity, leak detection, and intrusion can be monitored with the sensors. These are all vital aspects of maintaining an efficient-working data center atmosphere. Users and administrators to can monitor the status, view reports, and alarms of specific conditions in and around a PDU, and server rack.

**Note**: Only SmartZone G5 type sensors work with the SmartZone G5 iPDUs.

The following sensors are available:

- SmartZone G5 Temperature Sensor (EA001)
- SmartZone G5 Temperature + Humidity Sensor (EB001)
- SmartZone G5 Three Temperature + Humidity Sensor (EC001)
- SmartZone G5 Door Sensor (ACA01)
- SmartZone G5 Water - Rope Sensor (ED001)
- SmartZone G5 Water - Spot Sensor (EE001)
- SmartZone G5 Sensor Hub (EF001)
- SmartZone G5 Water Rope Sensor Extension (EG001)

| Sensor | Description | Sensor Measurement |
|---|---|---|
| Temperature Sensor | Monitors the temperature in the rack. | 1 |
| Temperature + Humidity Sensor | Monitors the temperature and relative humidity in the rack. | 2 |
| Three Temperature + Humidity Sensor | Monitors the temperature in three areas using three separate probes and the | 4 |

| Sensor | Description | Sensor Measurement |
|---|---|---|
| | relative humidity using one probe. | |
| Door Sensor | Sends an alarm or notification when a door on which the sensor is installed has been opened more than 10 mm. | 1 |
| Water - Rope Sensor | Monitors for early detection of liquid with a resistivity of less than 2 megaohms (including distilled water) in the monitored area. The kit includes a 6m rope and optional additional ropes can be added with an option. | 1 |
| Water – Spot Sensor | Monitors for early detection of liquid with a resistivity of less than 2 megaohms (including distilled water) in the monitored area. | 1 |
| Sensor Port Hub | Allows for up to three environmental sensors to be connected to the PDU. | N/A |
| Leak Detection Sensor Extension | The kit includes one additional 6m length rope to pair with the leak detection sensor. A total of four extensions can be added to the leak detection sensor for a total length of 30m. | N/A |

The optional environmental sensors can be installed before or after completing the PDU installation, startup, and can be installed without turning off power to the PDU or the devices connected. Panduit G5 Monitored Input, Monitored Switched, Monitored per Outlet, and Monitored & Switched per Outlet PDUs are designed to collect a maximum of eight environmental sensor measurements per PDU. For example, the Environmental Three Temperature + Humidity Sensor collects four sensor measurements. See the table above for the sensor measurement collected from each environmental sensor.

All Panduit G5 PDUs have two physical sensor ports, and each PDU can collect a total of eight sensor measurements (or readings). For example, if a PDU has a Door Sensor and an Environmental Three Temperature + Humidity Sensor connected, both physical sensor ports are used with a total of five sensor measurements recorded. Up to six physical sensors can be supported per PDU with the addition of the optional sensor hub.




**Figure 72: Sensor Ports for vertical PDU**




**Figure 73: Sensor Ports for Horizontal PDU**

## Configuring Environmental Sensors

To configure the sensor location, alarms, notifications, and details, open the WEB Interface:

1. Open the **Settings**.
2. View the Threshold section on the Settings page. Select **Threshold** to configure sensors.
3. Go to **External Sensors**.
4. Select **Edit** button to configure the desired sensors.
5. In the **Edit** dialog box, type value of up critical, up warning, low warning, and low critical.
6. Select **Save** to exit the sensor setup. Repeat this process for additional sensors.

# Section 10 – Rack Access Control

The G5 iPDUs allow users to electronically secure and control access to cabinets. See Figure below for a diagram of a typical Rack Access Control setup.

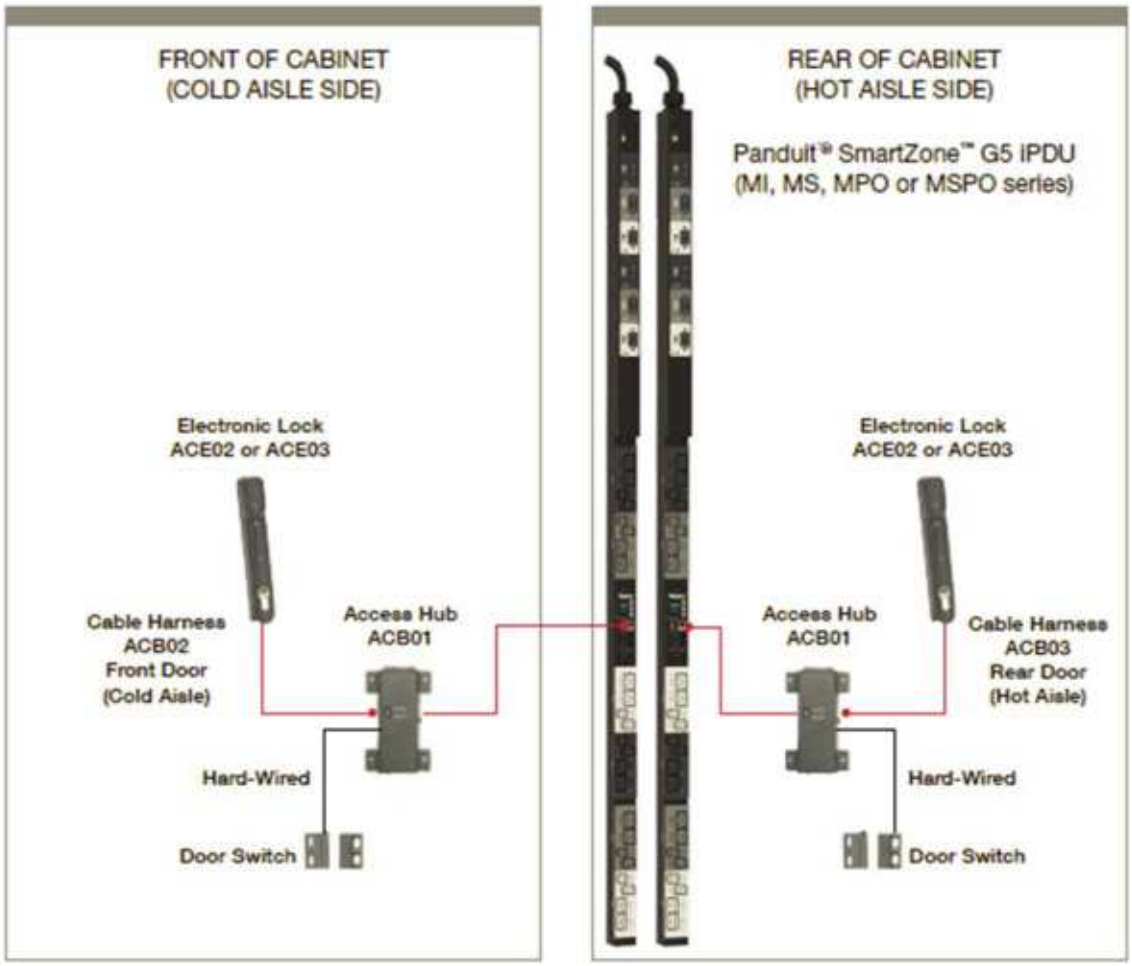



**Figure 74: Rack Access Control**

**Note**: For details on the RFID cards supported, please see the specification sheets for the respective Panduit G5 Electronic Swinghandles.

## Configuring Rack Access Control

All Rack Access Control configuration can be done under the Rack Access Control Page from the Web GUI. To access the Rack Access Control Page from the Web GUI, follow the following steps.

**Note**: The Hot Aisle or Cold Aisle is selected at the Access Hub (ACB01) through a DIP Switch. Not a configuration item in the Web Interface.

1. Log into the PDU.
2. Go to the **Gear** icon > **Rack Access Control**.

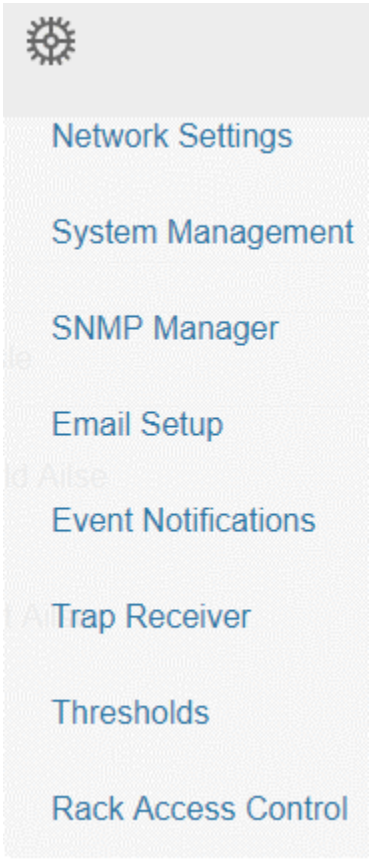



**Figure 75: Rack Access Control**

3. The Actions Menu on the right side of the page will allow the user to add a new Electronic handle, Remote Control the handle, or Configure the AutoLock setting of the handle.




**Figure 76: Actions**

4. The **New** option allows you to add authorized users to access the cabinet.

   See the next section for instructions on how to add a new user.

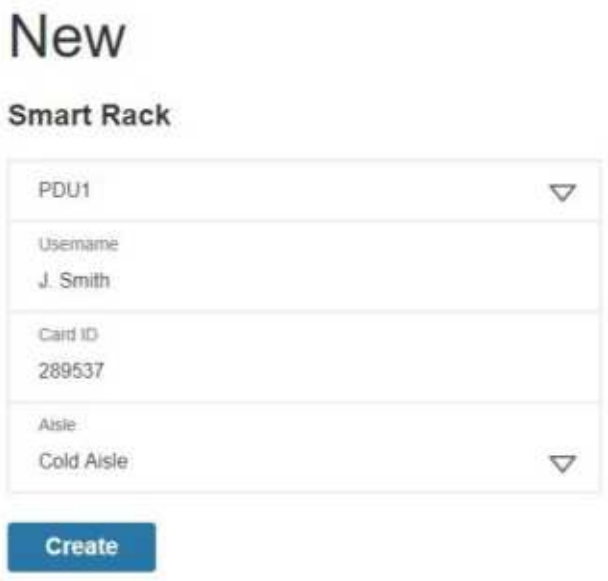



**Figure 77: Smart Rack**

5. The remote control allows you to lock or unlock the Electronic Handle.

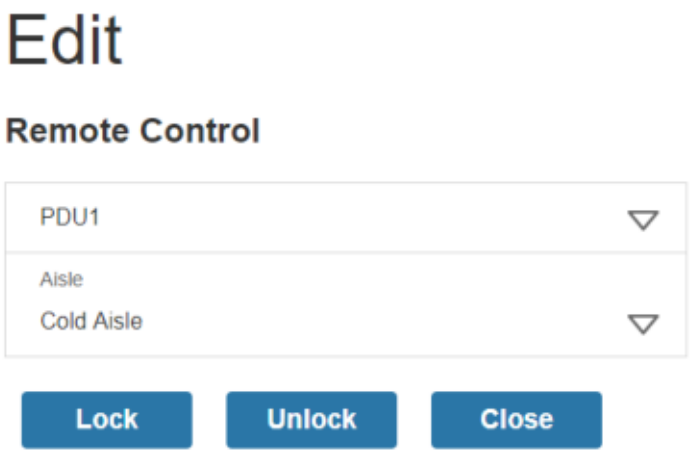



**Figure 78: Remote Control**

6. The AutoLock setting allows the user to set a redefined time interval (between 1-30 minutes) after which the Electronic Handle will lock.

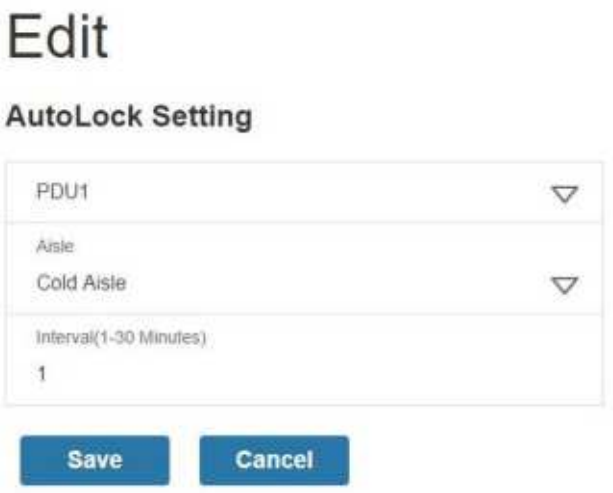



**Figure 79: AutoLock**

## Configuring User for Local Rack Access

1. Click the **Actions** option from the drop-down menu and select **New**.
2. Here you must enter a username, card ID, and aisle which will display on the Rack Access screen.

**Note**: A maximum of 8 HID Cards can be programmed per Access Hub.

- A typical cabinet will have two electronic Swinghandles. One for the front (cold aisle) and one for the back (hot aisle).
- If a user requires access to both the hot and cold aisles, you will need to add two entries in the table. One for the front door and one for the back door.

3. To determine the card ID, follow these steps:
   a. Place the card near the reader (top portion of the Swinghandle).
   b. Go to the event logs on the PDU.
   c. Look for a message about non-authorized card.

**Example**:

Smart Cabinet with PDU 1 Cold Aisle Lock is swiped by non-authorized card 258563

   d. The number in the message is the card ID.
4. Select **New** from the Actions menu.

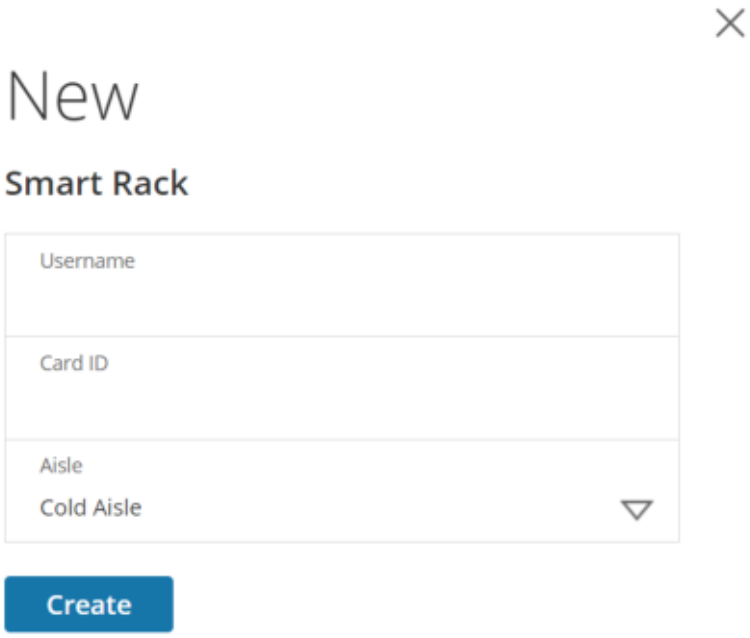



**Figure 80: Local Rack Access**

5. Enter a name to identify the user, the determined card ID, the PDU instance and aisle location.

**Note**: In the above example, the card ID is 258563

6. The card is now authorized to control the swing handle.
7. Select **Create**.

## Handle and Compatible Cards Types

The below table lists which cards supported on the different swing handle.

| | MIFARE® Classic 4k | MIFARE Plus® 2k | MIFARE® DESFire® 4k | HID® iCLASS | HID® 125kHz Prox | EM 125kHz Prox | Output |
|---|---|---|---|---|---|---|---|
| ACE01 | - | - | - | - | - | - | Wiegand |
| ACE02 | - | - | - | - | CSN | - | Wiegand |
| ACE03 | UID | UID | UID | UID | - | - | Wiegand |

**CSN** = Card Serial Number / **UID = Unique Identifier**

**Note:** Only 26 bits of the 34 bits are used when using the UID.

# Warranty and Regulatory Information

## Warranty Information

(http://www.Panduit.com)

## Regulatory Information

**Safety and regulatory compliance**

For important safety, environmental, and regulatory information, see *Safety and Compliance Information* at the Panduit website (http://www.Panduit.com)

# Support and Other Resources

## Accessing Panduit Support

- For live assistance, go to the Panduit.com website
- To access documentation and support services, go to the Panduit website.

# Acronyms and Abbreviations

**A**

Amps/Amperes

**AC**

Alternating Current

**AES**

Advanced Encryption Standard

**CLI**

Command Line Interface

**DHCP**

Dynamic Host Configuration Protocol

**Gb**

Gigabyte

**GUI**

Graphical User Interface

**iNC**

Intelligent Network Controller

**IP**

Internet Protocol

**iPDU**

Intelligent Power Distribution Unit

**kVA**

Kilo-Volt-Ampere

**kW**

Kilowatts

**kWH**

Kilowatt Hour

**LAN**

Local Area Network

**LCD**

Liquid-Crystal Display

**LDAP**

Lightweight Directory Access Protocol

**OLED**

Organic Light-Emitting Diode

**PDU**

Power Distribution Unit

**QNA**

Quad-Network Interface

**RNA**

Redundant Network Interface

**SHA**

Secure Hash Algorithms

**SNMP**

Simple Network Management Protocol

**TCP/IP**

Transmission Control Protocol/Internet Protocol

**USB**

Universal Serial Bus

**V**

Volts

**W**

Watts

# Documentation Feedback

Panduit is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (CS@Panduit.com). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.

# Appendix A: CLI Commands

### Help Commands

| Command | Description | Example |
|---|---|---|
| Panduit>? | List all available PDU CLI commands. | Panduit>?<br><br>**sys** PDU system configure and setting.<br><br>**net** PDU net application configure and setting.<br><br>**usr** PDU user operation.<br><br>**dev** PDU device setting.<br><br>**pwr** PDU power setting. |

### System Commands

| Command | Description | Example |
|---|---|---|
| sys date [year-month-day] | Query or set system's date. | Panduit>sys date 2013-09-19<br>SUCCESS<br>Panduit>sys date<br>SUCCESS<br>Date: 2013-09-19<br>Time: 03:49:46 |
| sys time [hour:min:sec] | Query or set system's time. | Panduit>sys time<br>Panduit>sys time 14:35:34 |
| sys ntp <IP Address> | Synchronize system date and time, with ntp server you set. | >sys ntp 69.25.96.13<br>**NOTE:** IP Address must be a valid ntp, server address otherwise, executes, failed |

| Command | Description | Example |
|---|---|---|
| sys ver | Query system's version information including firmware, bootloader, and Web. | Panduit>sys ver<br>SUCCESS<br>Firmware version: 0.41<br>Bootloader version: 2.10<br>LANGUAGE version: 3.01<br>WEB version: 6.30 |
| sys def | Recover PDU to default configuration. | Panduit>sys def<br>SUCCESS<br>Recover<br>Press any key to cancel |
| sys rst | Reset system. | Panduit>sys rst<br>Reboot required for change to take effort.<br>System Reboot now, Are you sure? (Y/N):Y |
| sys upd all | Update system's firmware with existing pdu bin file. | Panduit>sys upd lan<br>SUCCESS<br>system will enter upgrade mode after reboot<br>System Reboot now, Are you sure? (Y/N):Y<br><br>**NOTE 1:** There must be a valid file named Panduit.bin existing under directory/fw.<br>**NOTE 2:** If in daisy chain configuration, master will also upgrade its all slave's firmware. |
| sys upd boot | Update system's bootloader. | Panduit>sys upd boot<br>SUCCESS<br>system will enter upgrade mode after reboot<br>System Reboot now, Are you sure? (Y/N):Y |

| Command | Description | Example |
|---|---|---|
| | | **NOTE 1:** There must be a valid file named boot.bin existing under directory/fw.<br>**NOTE 2:** If in daisy chain configuration, master will also upgrade its all slave's bootloader. |
| sys upd conf | Update system's configuration. | Panduit>sys upd conf<br>SUCCESS<br>system will enter upgrade mode after reboot<br>System Reboot now, Are you sure? (Y/N):Y<br><br>**NOTE:** There must be a valid file named conf.ini existing under directory/fw. |
| sys log del event | Delete event log file. | Panduit>sys log del event,<br>SUCCESS |
| sys log edit data [on <interval> \| off] | Configure data log collection parameters | PANDUIT>sys log edit data on 1<br>SUCCESS<br>PANDUIT>sys log edit data off<br>SUCCESS |
| sys log del data | Delete data log file. | Panduit>sys log del data,<br>SUCCESS<br>Panduit> |

**Network Commands**

| Command | Description | Example |
|---|---|---|
| net ssh [on/off] | Query or on/off SSH. | Panduit>net ssh<br>SUCCESS,<br>SSH Port: 22<br>SSH Server is running |

| Command | Description | Example |
|---|---|---|
| | | Panduit>net ssh on<br>SUCCESS<br>Panduit>net ssh off<br>SUCCESS |
| net ftps [on/off] | Query or on/off FTPs. | Net ftps<br>SUCCESS<br>FTPS Port: 21<br>Service is running<br>Is Ftps |
| net http [on/off] | Query or on/off net http. | Panduit>net http<br>SUCCESS,<br>HTTP Port: 80<br>HTTPS Port: 443<br>WEB Protocol: HTTP<br>Panduit>net http off<br>E801<br>WEB protocol is changed, Please reboot to validate<br>System Reboot now, Are you sure? (Y/N):Y |
| net mac | Query MAC address. | Panduit>net mac<br>SUCCESS<br>MAC Addr: C8-45-44-66-2B-26 |
| net tcpip | Query network's IP information. | Panduit>net tcpip<br>SUCCESS<br>IPv4 Addr: 192.168.30.39 |
| net tcpip <dhcp> | Set network to dhcp mode. | Panduit>net tcpip dhcp<br>SUCCESS<br>Network is reconfigured, Please reboot to validate<br>System Reboot now, Are you sure? (Y/N): Y |
| net tcpip <static ip, mask, gateway> | Set static IP, mask and gateway. | Panduit>net tcpip static 192.168.30.39 255.255.255.0 |

| Command | Description | Example |
|---|---|---|
| | | 192.168.30.1<br>SUCCESS<br>Network is reconfigured, Please reboot to validate<br>System Reboot now, Are you sure? (Y/N): Y |

**User Commands**

| Command | Description | Example |
|---|---|---|
| User List | List all users account existing. | Panduit>usr list<br>SUCCESS<br>Usr Role<br>----------<br>admin admin<br>user user |
| User unlock<username> | Unlock specified user. | Panduit>usr unlock user<br>SUCCESS<br>Panduit>usr unlock admin<br>SUCCESS<br><br>**NOTE:** 1. Account would be locked temporarily if login failure excess "Maximum number of failed logins". Use this command to unlock it. |

**Device Commands**

| Command | Description | Example |
|---|---|---|
| dev usb [on\|off] | Query or on/off USB. | Panduit>dev usb<br>Panduit>dev usb off<br>Panduit>dev usb on |

| Command | Description | Example |
|---|---|---|
| dev daisy [rna\|qna] | Query or set daisy chain mode. | Panduit>dev daisy<br>SUCCESS<br>daisy chain unit number: 1<br>daisy chain address list: 000<br>Daisy Mode: RNA<br>Panduit>dev daisy qna<br>SUCCESS<br>System Reboot now, Are you sure? (Y/N): N |
| dev daisy <rna\|qna> init | Initialize daisychain. | Panduit>dev daisy qna init<br>SUCESS<br>System Reboot now, Are you sure? (Y/N):N |
| dev hid <PDUID> <hot \| cold> <lock \| unlock> | Remote locking and unlocking the cabinet. | PANDUIT>dev hid 1 cold unlock<br>SUCCESS |
| dev outlet <PDUID> status | Query all outlets' status with specified PDUID. | Panduit>Dev outlet 1 status<br>SUCCESS<br>Relay Outlet Status<br>Outlet#1: Close Outlet#2: Close Outlet#3: Close<br>Outlet#4: Close<br>Outlet#5: Close Outlet#6: Close Outlet#7: Close<br>Outlet#8: Close<br>Outlet#9: Close Outlet#10: Close Outlet#11: Close<br>Outlet#12: Close<br><br>**NOTE 1:** For M pdu, this command is in valid.<br>**NOTE 2:** PDUID index from 1; if in daisy chain, the master's PDUID is 1, others is ,2,3, |

| Command | Description | Example |
|---|---|---|
| dev outlet <PDUID> <outlet index> [on\|off] | Query or set specified PDUID and outlet-index's outlet status. | Panduit> dev outlet 1 1 off<br>SUCCESS<br><br>**NOTE:** For Monitored PDUs, this command is invalid. |
| dev sensor | List all sensors equipped. | Panduit> dev sensor<br>SUCCESS<br>Sensor count 4<br>----------<br>Name Type, SN Value<br>----------<br>T1,TEMP 012345678 27.5<br>T3,TEMP 012345678 27.2<br>T2,TEMP 012345678 27.3<br>RH HUMI 012345678 44 |
| dev ver <slipaddr> | Query sensor/power/delay's firmware version. | Panduit> dev ver 1<br>Panduit> dev ver 15<br>Panduit> dev ver 35<br><br>**NOTE:** relay: start from 1<br>power: start from 15<br>sensor: start from 35 |

**Power Commands**

| Command | Description | Example |
|---|---|---|
| pwr unit [idx] | Query device information, Query specified index unit's electric information. | Panduit> pwr unit<br>SKU: P9S20A , , , ,<br>Serial: , , , , ,<br>FuncType: PDU Monitored<br>Rating :220-240V, 16A, 3.5-3.8kVA, 50/60Hz<br>Mac :C8:45:44:66:2B:26<br>Tcpip :192:168:30:38 |

| Command | Description | Example |
|---|---|---|
| | | Panduit>pwr unit 1<br>SUCCESS<br>PDU UNIT 1 power Feature<br>voltage: 0V<br>current : 0.0A<br>active power: 0W<br>apparent power: 0W<br>power factor: 0.00<br>energy: 0.000kWh |
| pwr phase <idx> | Query specified phase's electric information. | Panduit> pwr phase 1<br>SUCCESS<br>PDU PHASE 1 power Feature<br>voltage: 0V<br>current : 0.0A<br>active power: 0W<br>apparent power: 0W<br>power factor: 0.00<br>energy: 0.000kWh |
| pwr cb <idx> | Query specified circuit breaker's<br>Electric information. | Panduit> pwr cb 1<br>SUCCESS<br>PDU CB 1 power Feature<br>voltage: 0V<br>current : 0.0A<br>active power: 0W<br>apparent power: 0W<br>power factor: 0.00<br>energy: 0.000kWh |
| pwr outlet <idx> | Query specified outlet's electric information. | Panduit> pwr outlet 1<br>SUCCESS<br>PDU OUTLET 1 power Feature<br>voltage: 0V<br>current : 0.0A<br>active power: 0W |

| Command | Description | Example |
|---|---|---|
| | | apparent power: 0W<br><br>**NOTE:** For Monitored PDUs, this command is invalid. |

# Appendix B: Sensor Configuration

### *Door Switch Sensor*

Door Switch Sensor is designed to send an alarm or notification signal when the door on which it is installed had been opened more than 10mm. This provides added security. The door switch can be configured to alert when the door is opened, alert when the door is closed, or the alerts can be disabled.

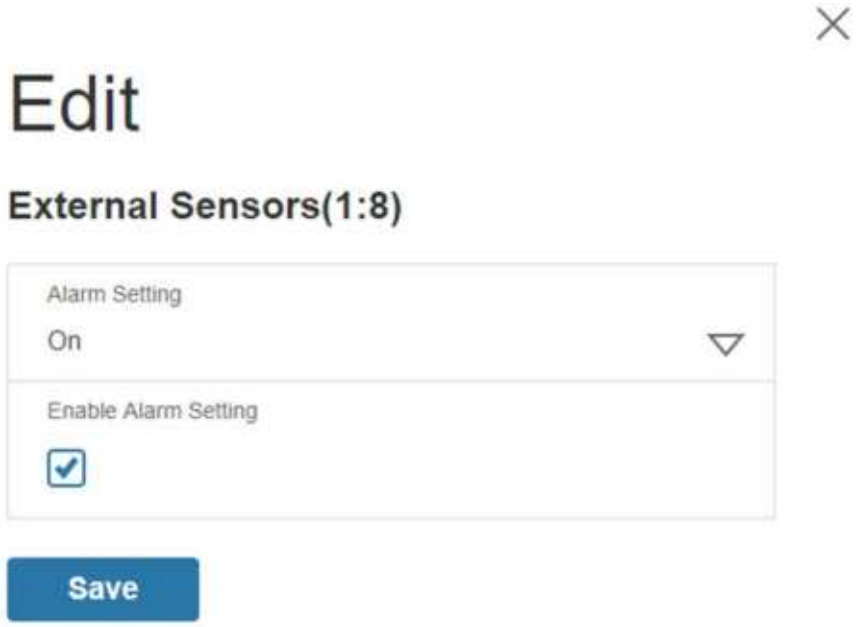



**Figure 81: Door Switch Sensor Configuration**

**Note**: The Door Switch Sensor is only designed to connect to a Panduit G5 iPDU. Connecting it to another device may result in damage.

### *Dry Contact Input Sensor*

The Dry Contact Input is designed to monitor the contact state of the sensor conditions such as moisture, motion, door status, and access through external dry contact sensors. This allows you to control vital data center and IT equipment with minimal effort. The dry contact cable can be configured to alert when the when the contact is opened, alert when the contact is closed, or the alerts can be disabled.

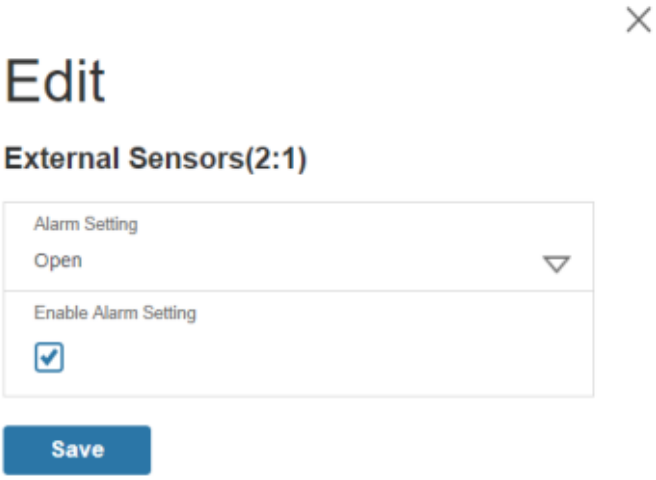



**Figure 82: Dry Contact Cable**

**Note**: The dry contact cable is only designed to connect to a Panduit G5 iPDU. Connecting it to another device may result in damage.

### *Water - Rope Sensor*

The Water - Rope Sensor is designed to provide early detection of fluid along the entire length of the sensor cable. The rope sensor's alarm can be enabled or disabled.

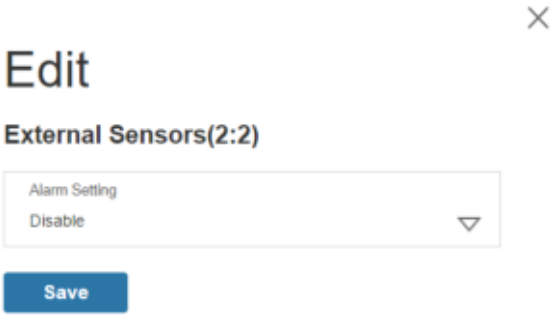



**Figure 83: Water Rope Sensor**

**Note**: The Water - Rope Sensor is designed to connect only to a Panduit G5 iPDU. Connecting it to another device may result in damage.

**Note**: If the rope extension is not fully engaged to the rope sensor, the sensor will report “no-leak” even if a leak is present.

### *Water - Spot Sensor*

The Water - Spot Sensor is designed to provide early detection of fluid at the sensor. The spot sensor’s alarm can be enabled or disabled.

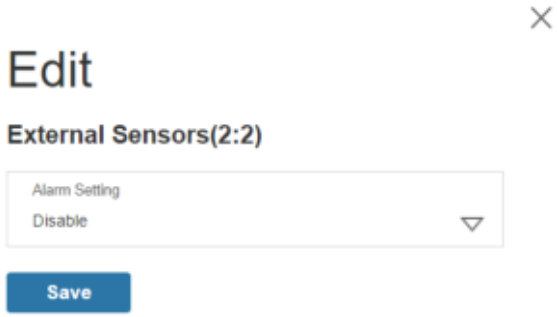



**Figure 84: Water Spot Sensor**

**Note**: The Water - Spot Sensor is designed to connect only to a Panduit G5 iPDU. Connecting it to another device may result in damage.

### *Temperature & Humidity Sensors*

Temperature and humidity sensors are designed to add comprehensive environmental monitoring to any Panduit G5 iPDU.

This smart design also enables easy plug & play installation that takes just moments to complete. Installation of the sensors and ongoing equipment maintenance is further facilitated using the Quick Disconnect Coupler and Ethernet cable, which allow for the convenient extension of sensors, movement of equipment, and an easy disconnect method for removing rack enclosure doors.

The temperature and humidity sensors can be configured with upper critical, upper warning, lower warning and lower critical threshold levels. Each alarm can also be disabled.

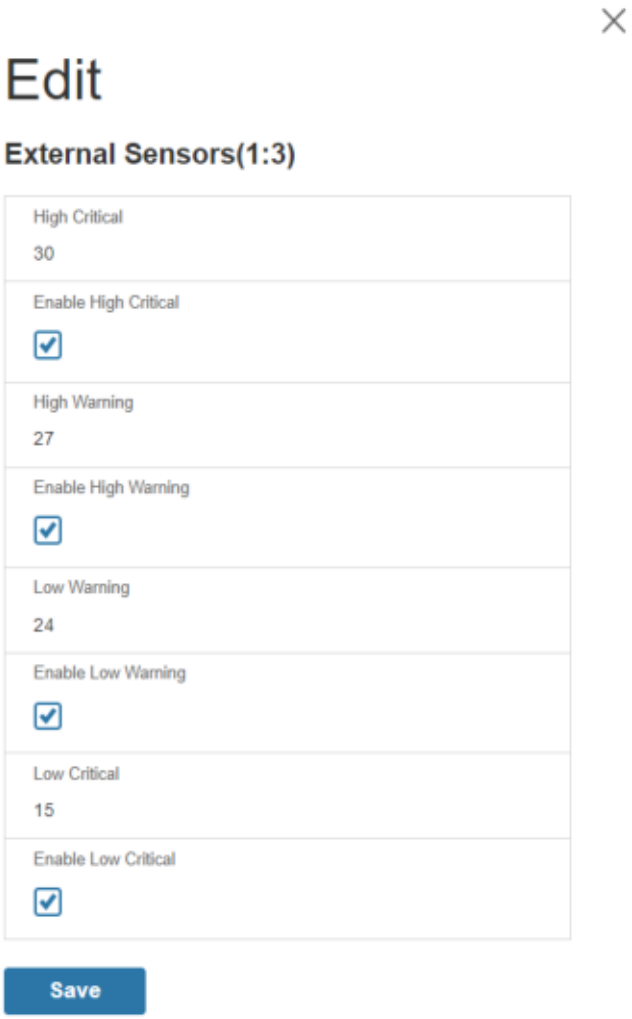



**Figure 85: Temperature and Humidity Sensors**

**Note**: It is recommended that the EA001, the SmartZone G5 Temperature Sensor, not be plugged into the access hub.

**Note**: It is recommended that the EC001, SmartZone G5 Three Temperature + Humidity Sensor, be plugged directly into the Panduit G5 iPDU.

**Note:** The Temperature and Humidity sensors are only designed to connect to a Panduit G5 iPDU. Connecting it to another device may result in damage.

# Appendix C: Firmware Update Procedure

The firmware upgrade procedure verifies the image by validating the signature of the images. If the signature does not match, the firmware upgrade procedure will ignore the image and remain on the current version.

## USB Method

**Note**: Verified to work with Toshiba or Sandisk up to 16GB USB Drives. Others USB drives *may* work as well.

1. Go to **www.Panduit.com** and download the most recent Firmware version, 'Panduit.FW'. Save this file to a USB drive.
2. Insert the USB drive into the USB port of the Intelligent Network Controller (iNC).
3. Enter USB mode on the PDU: Press **Select**. Go to **Setup**>**USB**>**Yes**. Select **Yes** to confirm entering USB mode.
4. Select **F/W Up**>**Yes** to upload the new Firmware.
5. The OLED will show the Firmware update progress.
6. When the update is complete, remove the USB.
7. From the USB Menu, select **Quit** to exit USB mode. Select Yes to confirm exit.
8. The PDU will automatically reboot.
9. To confirm that the Firmware was uploaded successfully, go to **Setup**>**Device**>**Firmware**.

## Web Interface Method

1. Open the User interface in a web browser by entering the PDU IP address.
2. Login to with Administration credentials.
3. Go to **System Management**>**Update Firmware**.
4. In the Firmware Update dialog box, browse to **Panduit.FW** firmware file.

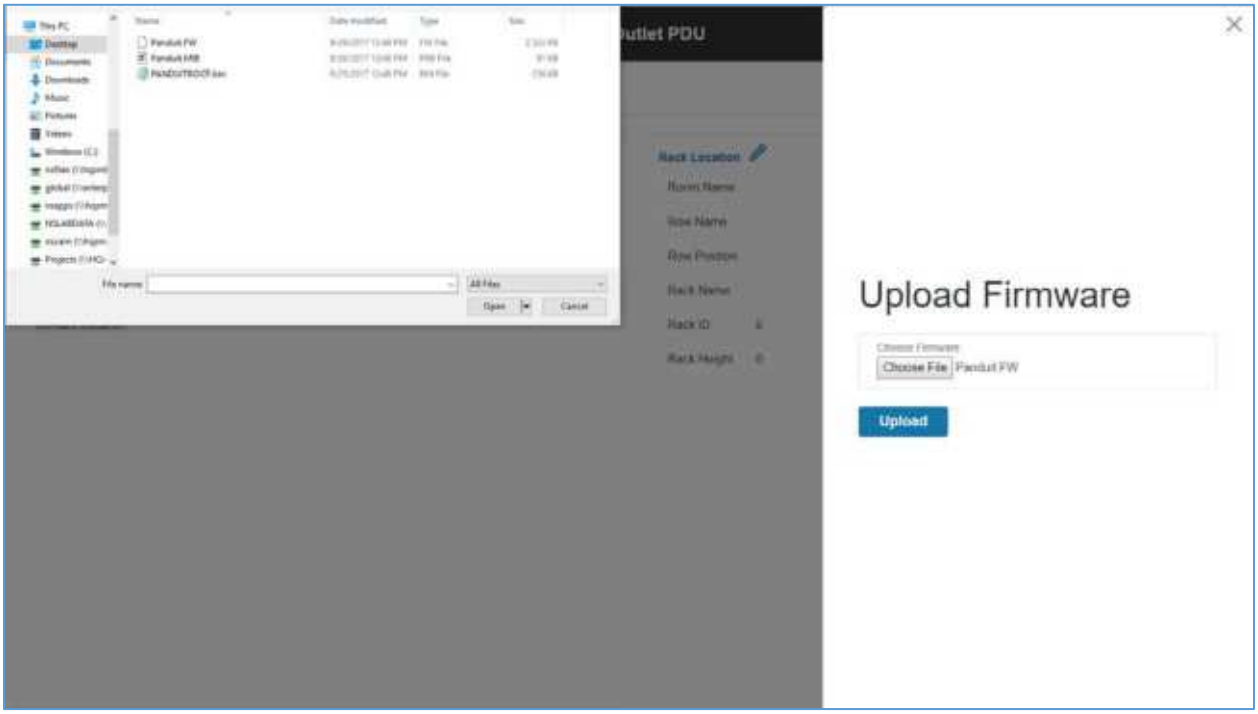



**Figure 86: Upload Firmware**

**NOTE:** the firmware file must be named Panduit.FW.

5. Select Upload. The system will update the newest firmware to the Intelligent Network Controller.

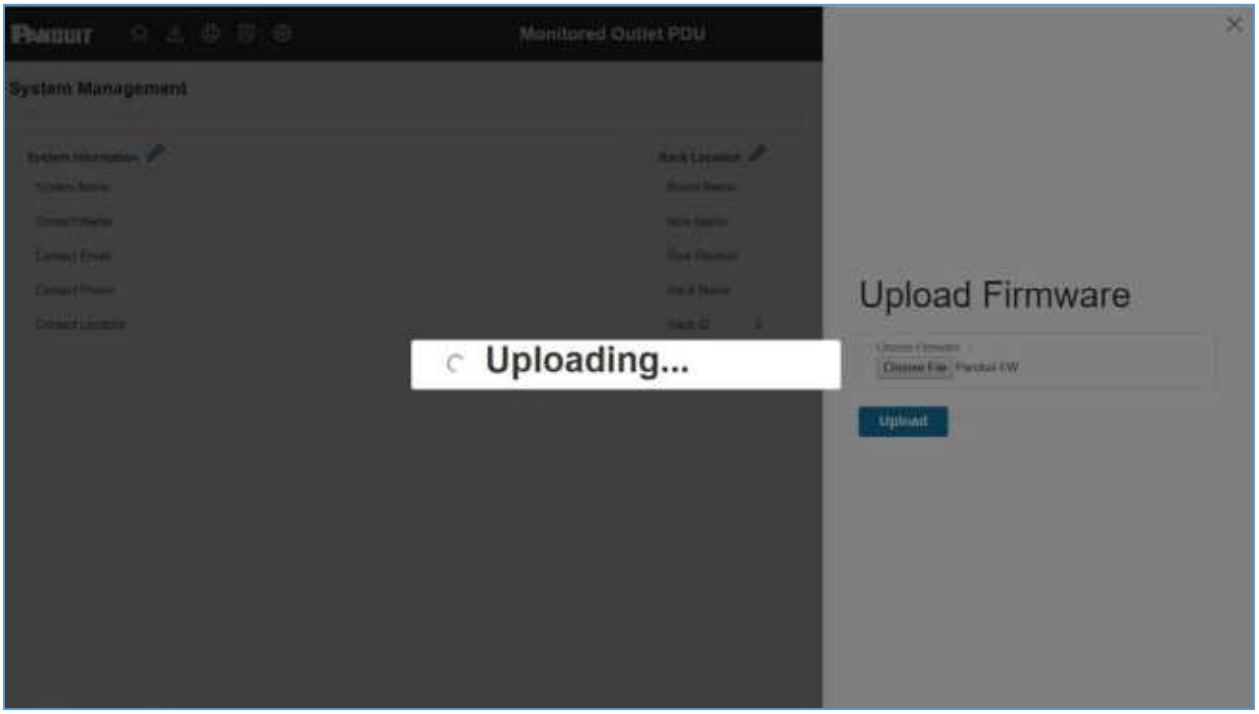



**Figure 87: Uploading Firmware**

6. When the upload is finished, the system will reboot automatically.

## FTPs Method

To access a PDU using a FTPs program, FTPs must be enabled through the PDU Web Interface or CLI. In the Web Interface, go to Network Settings >SSH/**FTPs Configuration**. Select the check box to enable FTPs Access. In the CLI, login as an administrator and use the command net tcpip FTPs open

1. Login to a FTPs program with a role with administration privileges.
2. Transfer the updated Panduit.fw file to the root directory. Close the FTPs.
3. Connect to the PDU via SSH using a program such as HyperTerm or PuTTY.
4. Login using a role with administration privileges.
5. Enter the command **sys upd all**.
6. It will show the message: System will enter upgrade mode after reboot, System Reboot now, Are you sure? (Y/N).

7. Enter Y.
8. When the upload is finished, the system will reboot automatically. It is not always required to update Web or Bootloader files when the Firmware is updated. However, a user can upload these file types in SSH:
    a. Login to a FTPs program.
    b. Overwrite the outdated files with the updated web files (found on the customer login at www.Panduit.com or from your regional sales manager).

## Bootloader Mode

1. Go to www.Panduit.com and download the most recent Firmware version, 'Panduit.bin'. Save this file to a USB drive.
2. Insert the USB drive into the USB port of the Intelligent Network Controller.
3. Enter USB mode on the PDU: Press Select. Go to Setup>USB>Yes. Select Yes to confirm entering USB mode.
4. Select F/W Up>Yes to upload the new Firmware.
5. The OLED will show the Firmware update progress.
6. When the update is complete, remove the USB.
7. From the USB Menu, select Quit to exit USB mode. Select Yes to confirm exit.
8. The PDU will automatically reboot.
9. To confirm that the firmware was uploaded successfully, go to Setup>Device>Firmware.

## Firmware Recovery with Bootloader Mode

Firmware, configuration files, and bootloader files can be updated following the steps above, but each update type must be done separately. Web files can be updated in conjunction with any of the other updates. I.e., a user can update Firmware and Web files in a single step. But firmware and configuration files must be done separately.

# Appendix D: System or Password Recovery

If the PDU (or the Password for the PDU) needs to be defaulted to factory settings, the original conf.ini needs to be loaded to the PDU via the USB port. To locate the original conf.ini file for that PDU, please send a support email to: systemsupport@panduit.com indicating the PDU part number in the subject and body of that email.

## Upgrade Configuration with Bootloader Mode

To make the PDU accessible through the USB port on the unit, you must:

1. Go to Device Configuration > USB Settings.
2. Select the Enable USB Access Checkbox.

To upload configuration, you must:

1. Copy conf.ini to USB.
2. Insert USB to PDU.
3. Enter USB mode in OLED device.
4. Select **Conf up**.
5. After the operation is completed, remove USB, and quit USB mode.

# Appendix E: PDU Alarms

| | |
|---|---|
| PDU Unit | PDU Unit Active Power Above upper critical<br>PDU Unit Active Power Above upper warning<br>PDU Unit Active Power Below lower warning<br>PDU Unit Active Power Below Lower critical |
| Input Phase | Input Phase X Voltage Above upper critical<br>Input Phase X Voltage Above upper warning<br>Input Phase X Voltage Below lower warning<br>Input Phase X Voltage Below lower critical<br>Input Phase X Current Above upper critical<br>Input Phase X Current Above upper warning<br>Input Phase X Current Below lower warning<br>Input Phase X Current Below lower critical |
| Circuit Breaker | Circuit Breaker X Current Above upper critical<br>Circuit Breaker X Current Above upper warning<br>Circuit Breaker X Current Below lower warning<br>Circuit Breaker X Current Below lower critical<br>Circuit Breaker Status ON<br>Circuit Breaker Status OFF |
| Outlet | Outlet X Active Power Above upper critical<br>Outlet X Active Power Above upper warning<br>Outlet X Active Power Below lower warning<br>Outlet X Active Power Below lower critical |

| | |
|---|---|
| | Outlet X Immediate ON<br>Outlet X Delayed ON<br>Outlet X Immediate OFF<br>Outlet X Delayed OFF<br>Outlet X Immediate REBOOT<br>Outlet X Delayed REBOOT<br>Outlet X Cancel Pending Command |
| External Sensor | External Sensor X (numerical) Above upper critical<br>External Sensor X (numerical) Above upper warning<br>External Sensor X (numerical) Below lower warning<br>External Sensor X (numerical) Below lower critical<br>External Sensor X (state) Alarmed<br>External Sensor X (state) Communication Lost |
| System | System Event log Cleared<br>System Data log Cleared<br>System PDU configuration file Imported<br>System PDU configuration file Exported<br>System Firmware update completed<br>System Firmware update failed<br>System Firmware update started<br>System Firmware Validation failed<br>System an LDAP error occurred<br>System Network interface link state is up<br>System Sending SMTP message failed<br>System Intelligent Network Controller reset<br>System Intelligent Network Controller start<br>System Communication Lost<br>Daisy Chain state changed<br>USB Port |
| User Activity | User Activity User X Authentication failure<br>User Activity User X User logged in<br>User Activity User X Session timeout<br>User Activity User X User blocked |

| | |
|---|---|
| User Administration | User Administration Password changed<br>User Administration Password settings changed<br>User Administration User added<br>User Administration User deleted<br>User Administration User modified |
| Smart Rack Access | Smart Rack Access Door Open<br>Smart Rack Access Door Closed<br>Smart Rack Access User Card Swiped<br>Smart Rack Access Door Autolocked |

## Trap Codes assigned to Alarms List

Trap codes assigned for critical alarms:

| Trap Class | Trap Code | Trap Description |
|---|---|---|
| Critical | 1 | The PDU unit active power is ABOVE critical threshold value. |
| | 2 | The PDU unit active power is BELOW critical threshold value. |
| | 3 | The Critical Energy Alarm. |
| | 4-6 | The phase (1-3) voltage is ABOVE critical threshold value. |
| | 7-9 | The phase (1-3) voltage is BELOW critical threshold value. |
| | 10-12 | The phase (1-3) current is ABOVE critical threshold value. |
| | 13-15 | The phase (1-3) current is BELOW critical threshold value |
| | 16-27 | The circuit breaker (1-12) current is ABOVE critical threshold value |
| | 28-30 | The circuit breaker (1-12) current is BELOW critical threshold value |
| | 40-51 | The circuit breaker (1-12) is in OFF state |
| | 52-99 | The outlet (1-48) active power is ABOVE critical threshold |

| | |
|---|---|
| | value |
| 100-147 | The outlet (1-48) active power is BELOW critical threshold value |
| 148-155 | The sensor (1-8) temperature/humidity is ABOVE critical threshold value |
| 156-163 | The sensor (1-8) temperature/humidity is BELOW critical threshold value |
| 164-171 | The sensor (1-8) contact state is in alarm. |
| 172-179 | The sensor (1-8) lost communications. |
| 183 | User authentication failed. |
| 186 | Power or relay communication lost to main board |
| 187-189 | Input Phase (1-3) Frequency Asserted below lower critical. |
| 193 | Firmware update failed. |
| 194 | Failure in sending the SMTP message. |
| 195-197 | Input Phase (1-3) Frequency Asserted above upper critical |

Trap codes assigned for warning alarms:

| Trap Class | Trap Code | Trap Description |
|---|---|---|
| Warning | 200 | The PDU unit active power is ABOVE warning threshold value. |
| | 201 | The PDU unit active power is BELOW warning threshold value. |
| | 202 | The PDU warning energy alarm. |

| | |
|---|---|
| 203-205 | The phase (1-3) voltage is ABOVE warning threshold value. |
| 206-208 | The phase (1-3) voltage is BELOW warning threshold value. |
| 209-211 | The phase (1-3) current is ABOVE warning threshold value. |
| 212-214 | The phase 1 current is BELOW warning threshold value. |
| 215-226 | The circuit breaker (1-12) current is ABOVE warning threshold value. |
| 227-238 | The circuit breaker (1-12) current is BELOW warning threshold value. |
| 239-250 | The circuit breaker (1-12) is in OFF state. |
| 251-298 | The outlet (1-48) active power is ABOVE warning threshold value. |
| 299-346 | The outlet (1-48) active power is BELOW warning threshold value. |
| 347-354 | The sensor (1-8) temperature/humidity is ABOVE warning threshold value. |
| 355-362 | The sensor (1-8) temperature/humidity is BELOW warning threshold value. |

Trap codes assigned for information alarms:

| Trap Class | Trap Code | Trap Description |
|---|---|---|
| Informational | 380-391 | The circuit breaker (1-12) is in ON state. |
| | 392-439 | The outlet (1-48) IMMEDIATE ON occurred. |
| | 440-487 | The outlet (1-48) DELAYED ON occurred. |
| | 488-535 | The outlet (1-48) IMMEDIATE OFF occurred. |

| | |
|---|---|
| 536-583 | The outlet (1-48) DELAYED OFF occurred. |
| 584-631 | The outlet (1-48) IMMEDIATE REBOOT occurred. |
| 632-679 | The outlet (1-48) DELAYED REBOOT occurred. |
| 680-727 | The outlet (1-48) Cancel Pending Commands occurred. |
| 728-735 | The sensor (1-8) contact state is in cleared. |
| 740 | Event log Cleared. |
| 741 | Data log Cleared. |
| 742 | PDU configuration file Imported. |
| 743 | PDU configuration file Exported. |
| 744 | Firmware update completed. |
| 745 | Firmware update started. |
| 746 | An LDAP error occurred. |
| 747 | Network interface link state is up. |
| 748 | Communication Module reset. |
| 749 | Communication Module start. |
| 750 | Daisy Chain state changed. |
| 752 | User xxx logged in. |
| 753 | User xxx session timeout. |
| 754 | User xxx blocked. |
| 755 | User xxx password changed. |
| 756 | User password settings changed. |
| 757 | User xxx added. |
| 758 | User xxx deleted. |

| | |
|---|---|
| 759 | User xxx modified. |
| 761 | Smart Rack Access Door Opened |
| 762 | Smart Rack Access Door Closed |
| 763 | Smart Rack Access User Card Swiped |
| 764 | Smart Rack Access Door Autolocked |
| 765 | Smart Rack Mechanical Lock |
| 766 | Smart Rack Mechanical Unlock |

Trap codes assigned for information alarms:

| Trap Class | Trap Code | Trap Description |
|---|---|---|
| Clear | 770 | The PDU unit active power is alarm clear. |
| | 771 | The PDU energy alarm clear. |
| | 772-774 | The phase (1-3) voltage alarm cleared |
| | 775-777 | The phase (1-3) current alarm cleared |
| | 778-789 | The circuit breaker (1-12) current alarm cleared |
| | 790-837 | The outlet (1-48) active power current alarm cleared. |
| | 838-845 | The sensor (1-8) temperature/humidity alarm cleared. |
| | 846-853 | The sensor (1-8) lost communication alarm cleared. |
| | 854-856 | Input Phase (1-3) Frequency Deasserted above upper critical |
| | 857-859 | Input Phase (1-3) Frequency Deasserted below lower critical. |

# Appendix F: Horizontal Intelligent Network Controller Replacement

1. Unscrew the left and right captive nuts on the Intelligent Network Controller by turning them counter clockwise.

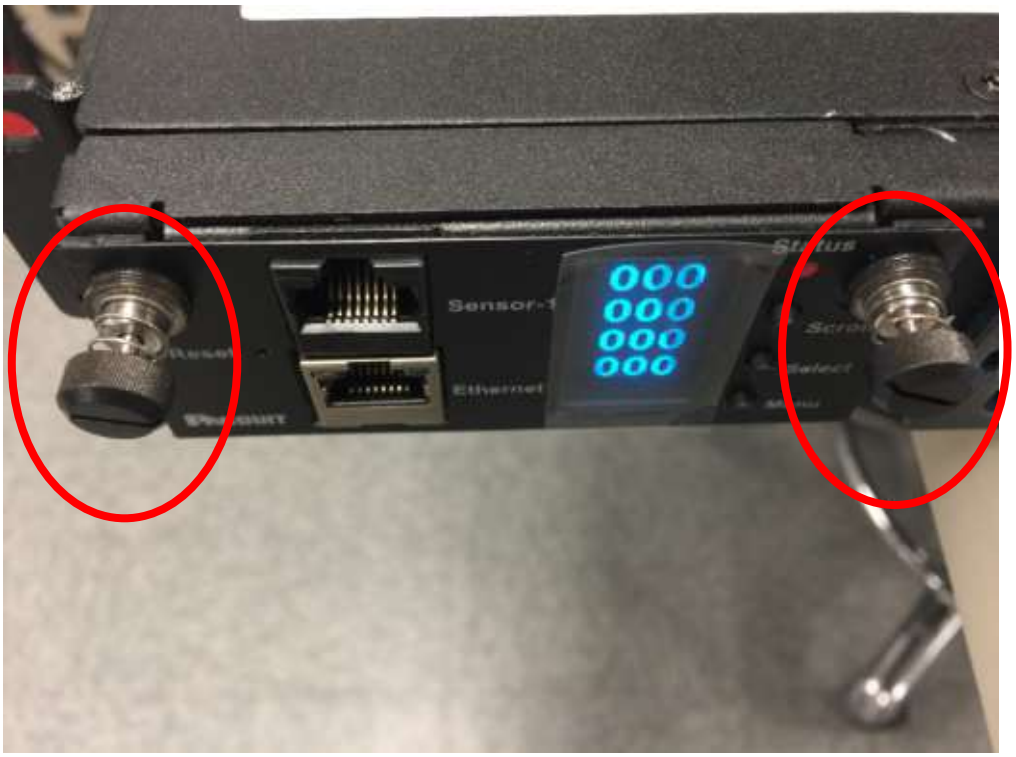



**Figure 88: Unscrew Intelligent Network Controller**

2. Pull out the Intelligent Network Controller from the PDU.

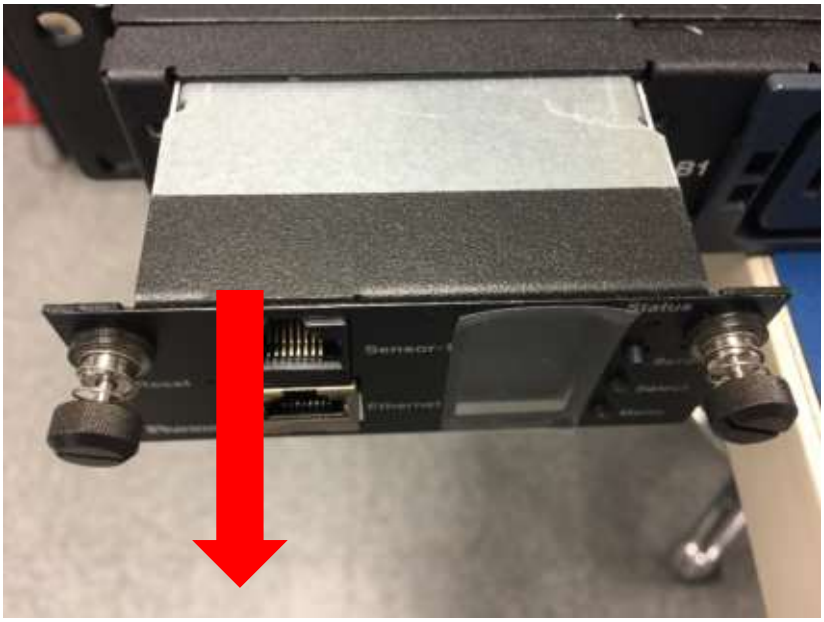


**Figure 89: Remove Intelligent Network Controller from PDU**

3. Insert the new Intelligent Network Controller.

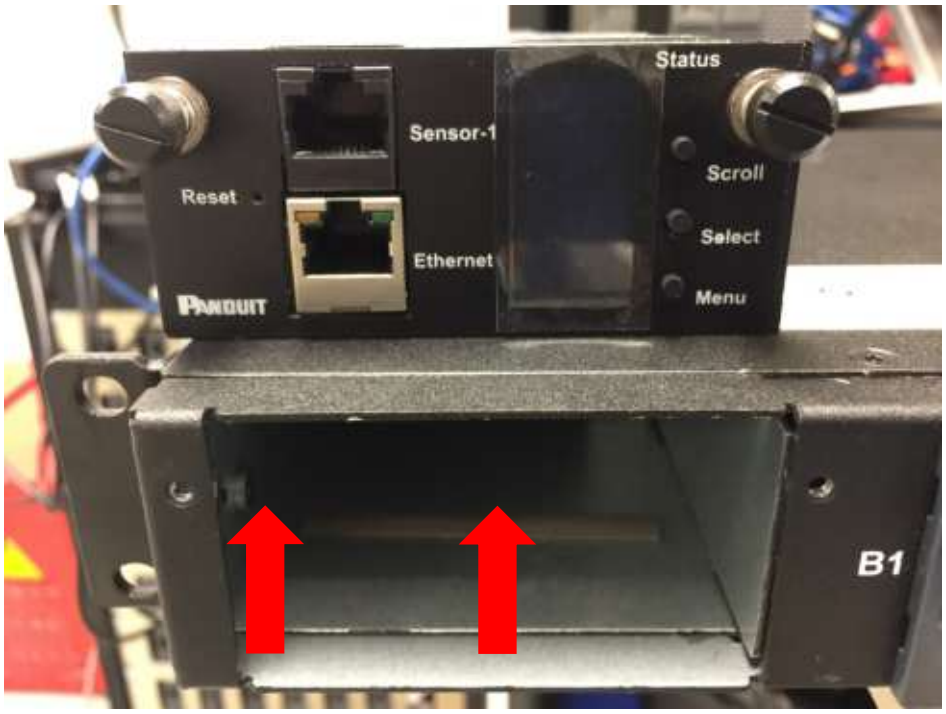



**Figure 90: Inserting New Intelligent Network Controller**

4. Align the Intelligent Network Controller and tighten the captive nuts by turning them clockwise.

# Appendix G: Vertical Intelligent Network Controller Replace or Rotate 180°

1. Use a T10 Torx screwdriver to remove the two screws from the Intelligent Network Controller.

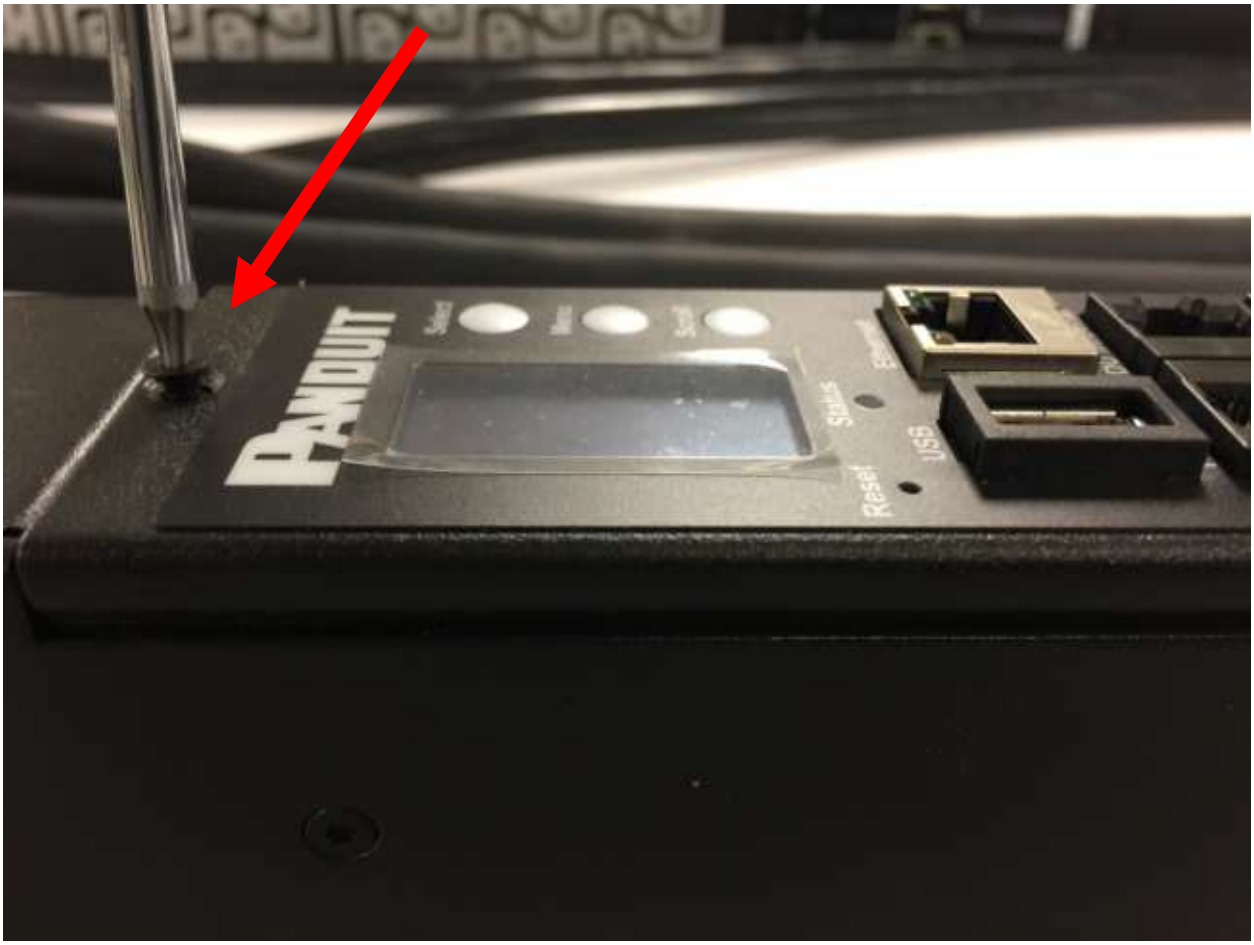



**Figure 91: Removing Top and Bottom Screw from Intelligent Network Controller**

a. Controller may be rotated to accommodate overhead or underfloor power. If rotating controller, it is recommended that you disconnect the ribbon cable. Rotate and reinstall.

2. If replacing controller, disconnect the existing ribbon cable from the Intelligent Network Controller. Connect the ribbon cable to the new Intelligent Network Controller.

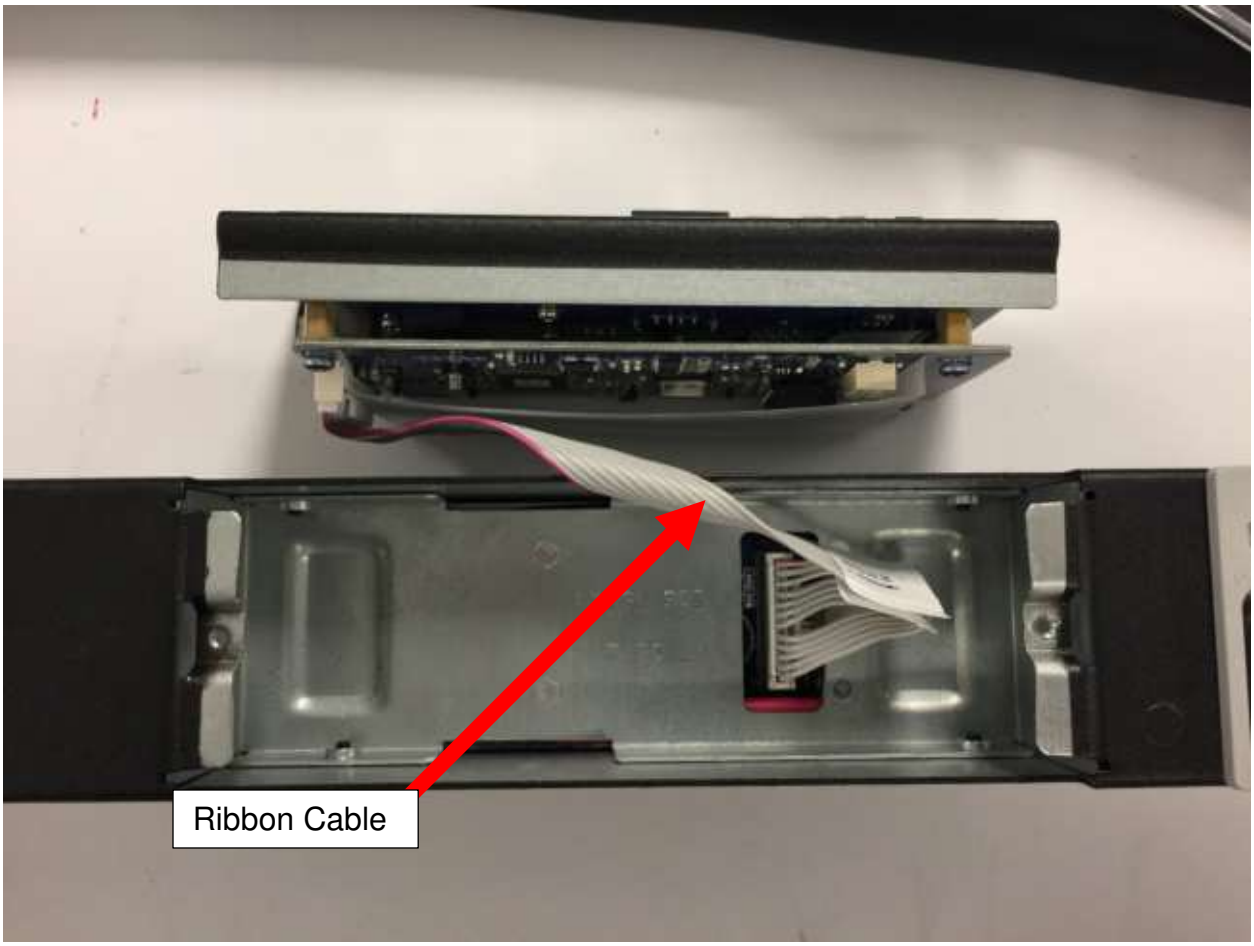



**Figure 92: Disconnecting and Reconnecting the Intelligent Network Controller**

3. Replace and tighten the two (T10) screws on the Intelligent Network Controller.

# Appendix H: Changing Your PC's IP Address

**Note**: Instructions refer specifically to Windows 10. Please refer to your operating system documentation if you are not using Windows 10.

1. Click the **Windows** button and select **Control Panel**.

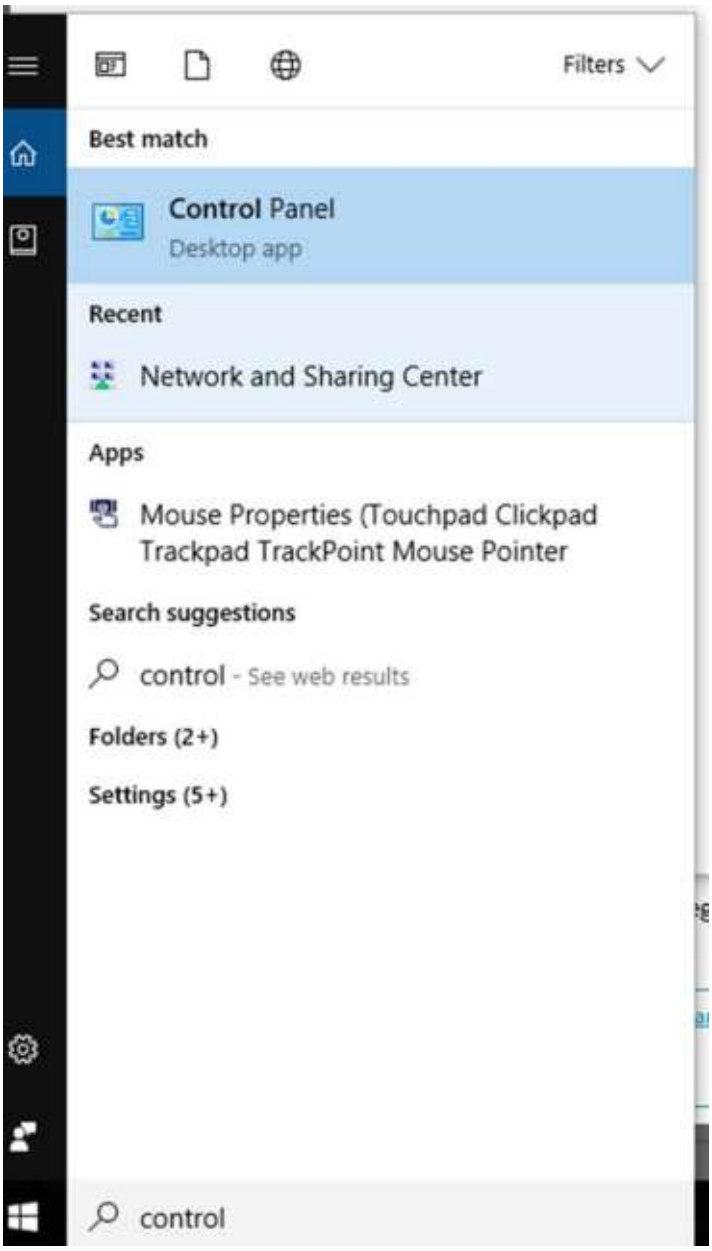



**Figure 93: Control Panel**

2. In the Control Panel window, select **View network status and tasks** under the Network and Internet heading.

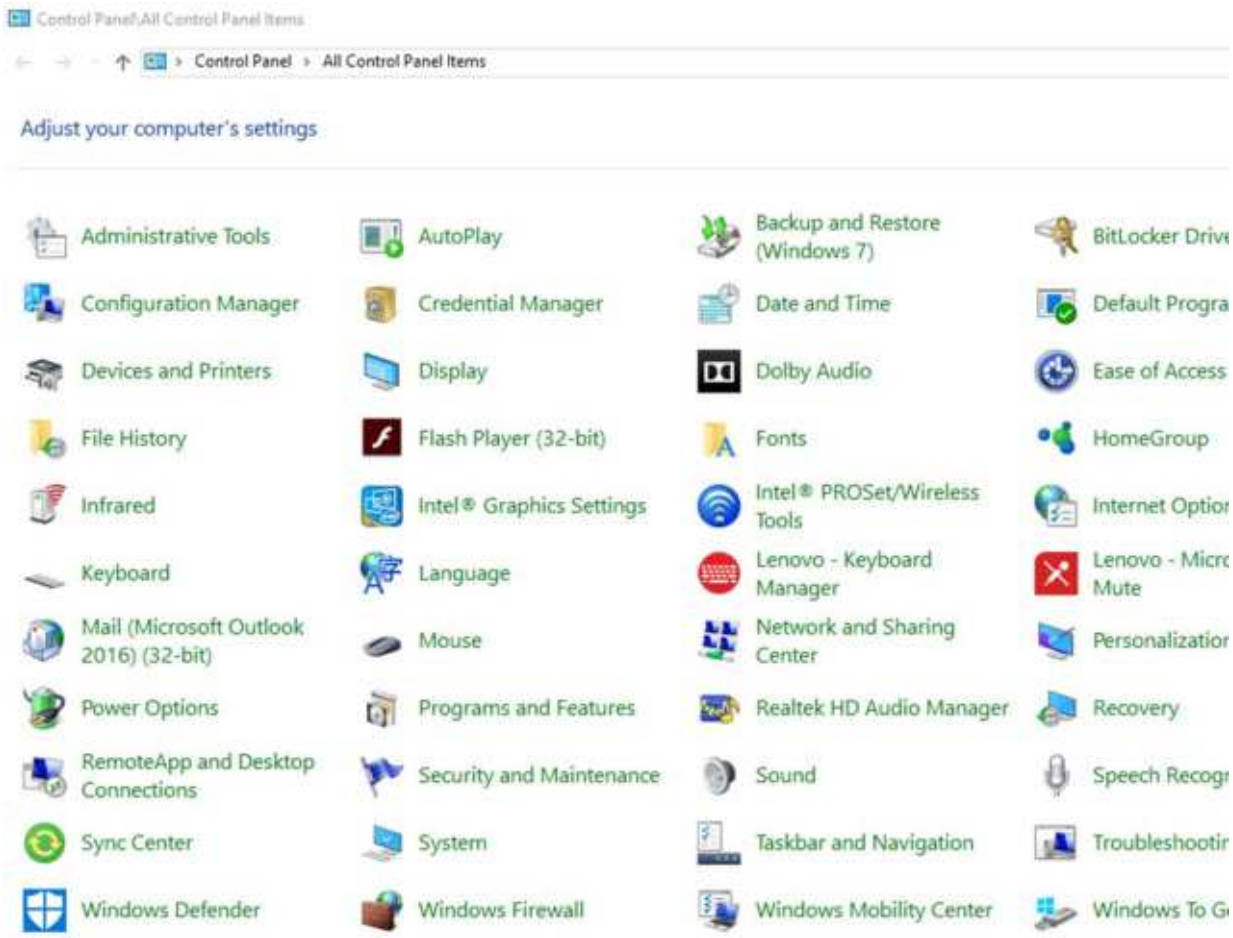



**Figure 94: Network Status and Tasks**

3. Select **Change adapter settings** from the menu on the left.

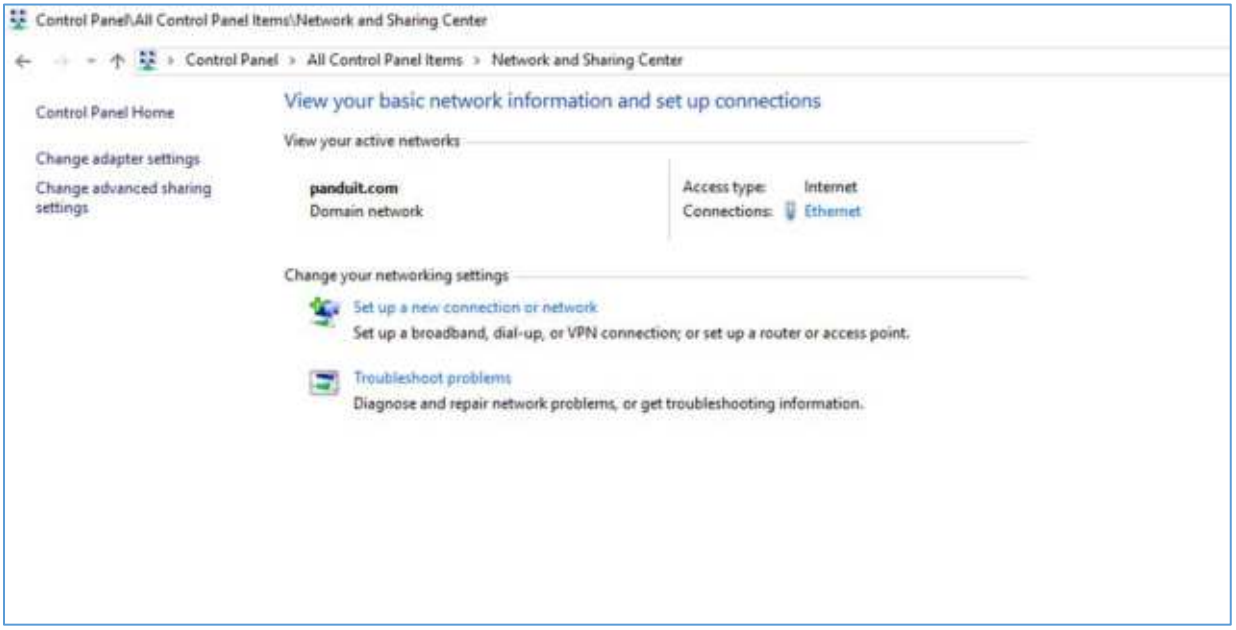



**Figure 95: Change Adapter Settings**

4. Right-click **Ethernet** and select **Properties**.




**Figure 96: Properties**

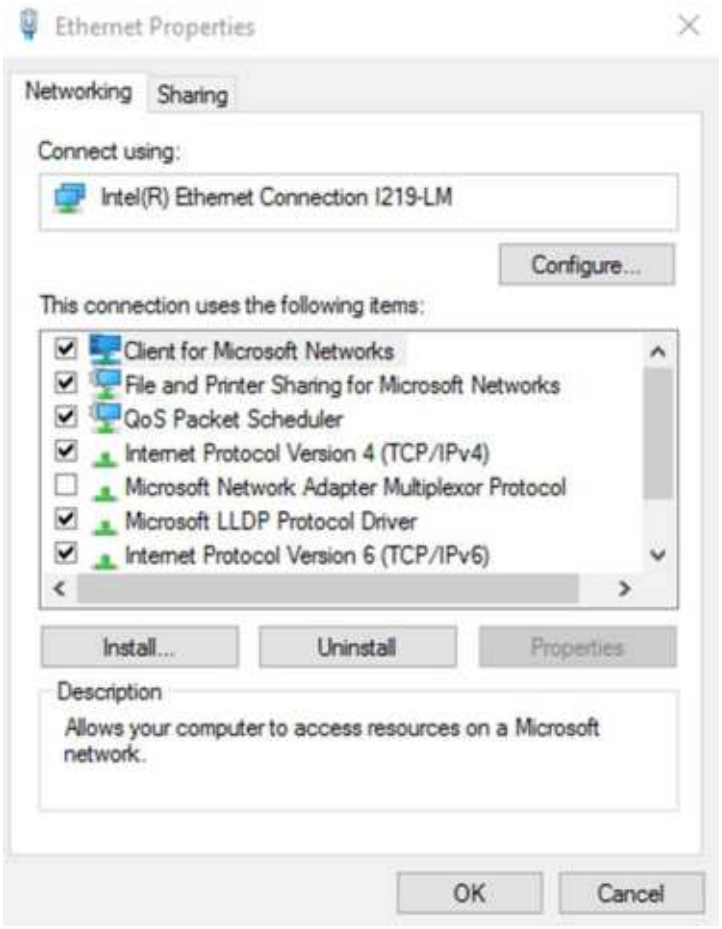



**Figure 97: Ethernet Properties**

5. Select **Internet Protocol (TCP/IP) Version 4** (you may need to scroll down). Then click the **Properties** button.




**Figure 98: Internet Protocol Version 4**

6. Select the **Use the following IP address** radio button. The **Use the following DNS server addresses** radio button then selects automatically.

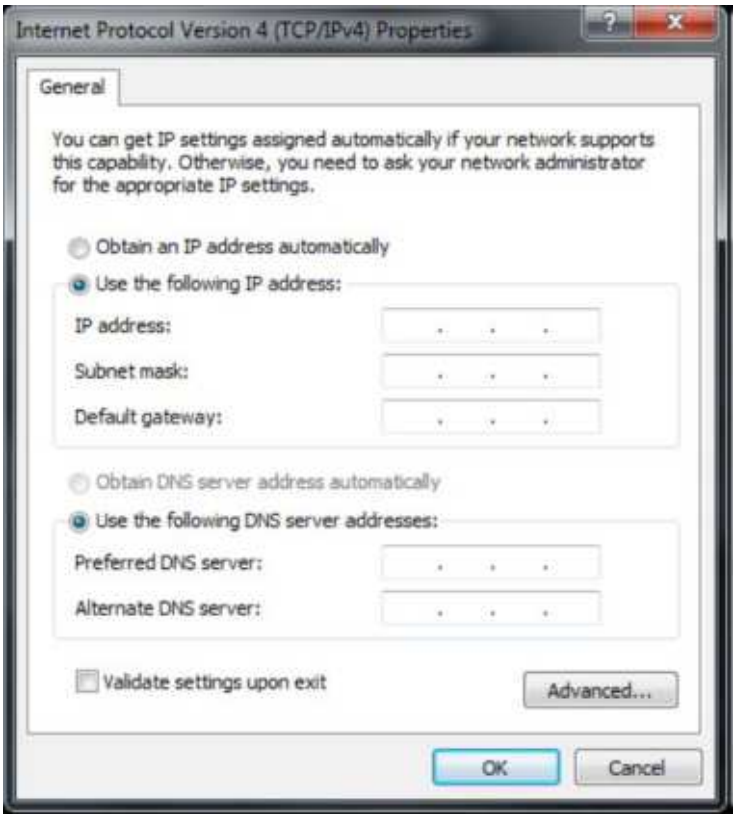



**Figure 99: DNS Server**

Enter the following details into the appropriate boxes:

- IP address: 192.168.0.10
- Subnet mask: 255.255.255.0
- Default gateway: 192.168.01
- Preferred SNS server: 192.168.0.1

7. Click **OK** to accept the entries.
8. Connect the PDU network connection directly to the PC's Ethernet card using a patch cable.
9. Power the PDU unit.
10. Open a web browser on the PC.
11. Enter the address bar **http://192.168.0.1** into your browser.

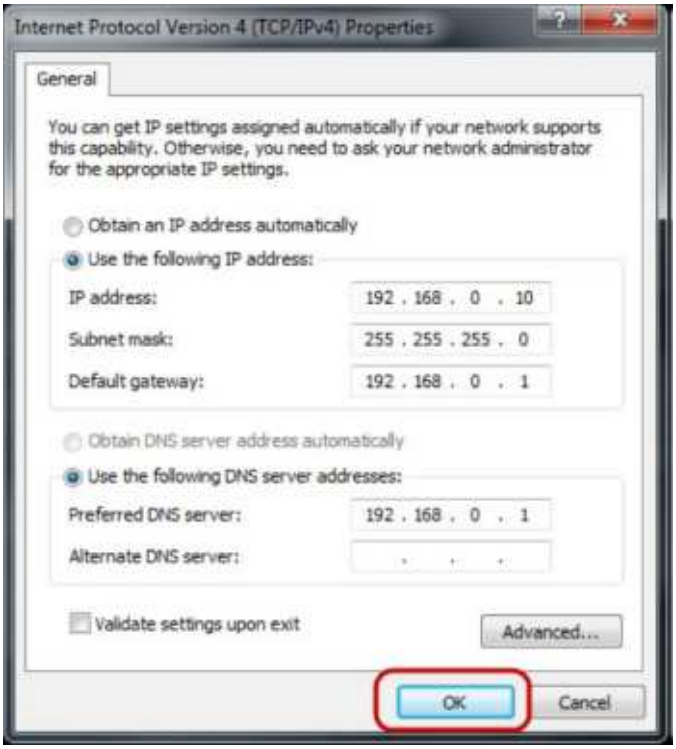



**Figure 100: Confirmation**

12. Press **OK**.