PANDUIT®
infrastructure for a connected world

PANDUIT™
POWER SOLUTIONS

G5 Intelligent PDU User Manual v4.5

Table of Contents

Section 1 – System Overview 9
PDU Controller 9
Connecting the PDU via Ethernet Port 9
Connecting the PDU to a Computer Serial Port 10
Section 2 – Web Graphical User Interface (GUI) Configuration 11
Internet Protocol (IP) Addressing 11
Connecting to the PDU 11
Web Configuration 11
Introduction to the Web GUI 15
Screen Resize Due to Multiple PDU Configuration 17
Menu Dropdowns 18
Introduction to the Dashboard 18
Network Settings 19
System Management Information 21
Setting Time and Date on the PDU 24
Outlet Power Management 27
Outlet Power Sequence Setup 28
Setting Metering Thresholds 30
Email Setup 42
Event Notifications 46
Data Log 48
Web Interface Access 49
Setting Up the System for RADIUS Authentication 51
Configuring the system with LDAP Server Settings 52
Section 3 – Simple Network Management Protocol (SNMP) 57
SNMP Management Configuration 57
Configuring Users for SNMP V1/V2c 59

Configuring Users for SNMP v3 61
Configuring SNMP Traps 63
Section 4 – Local Display 66
Onboard Display and Network Controller 66
Control Buttons 67
Network Controller Menu Structure 68
Main Menu Selections 68
Setup Menu 69
Sensors Menu 82
Section 5 – Daisy Chain Configuration 83
Daisy-Chain Overview 83
Daisy-Chain Setup 83
RNA (Redundant Network Access) Functionality 83
RNA Setup 84
Power Share 86
Section 6 – Electronic Security Handle 89
Configuring Cabinet Access Control 91
Adding a User for Local Rack Access 93
Configuring Rack Access Settings. 94
Configuring Handle Settings. 96
Configuring Keypad Settings 97
Remote Controlling the Handle. 97
Controlling the Beacon. 99
The Status LED 101
Setting Status LED State 102
Handle and Compatible Card Types 102
Section 7 – Panduit G5 Accessories 103
Hardware Overview 103
Configuring Temperature Scale 105

Configuring Environmental Sensors 105
Security 107
Non-volatile Storage 107
Authentication Data 107
Network Transport Security 107
Network Configuration Data 107
External Authorization Mechanisms 108
Other Features 108
Warranty and Regulatory Information 109
Warranty Information 109
Regulatory Information 109
Panduit Support and Other Resources 110
Accessing Panduit Support 110
Acronyms and Abbreviations 112
Appendix A: Sensor Configuration 109
Door Switch Sensor 109
Dry Contact Input Sensor (side panel switch) 109
Temperature & Humidity Sensors 110
Configuring Environmental Sensors 111
Appendix B: Firmware Upgrade Options 113
G5 Upgrade Tool (GUT) 113
Web Interface Method 113
USB Method 114
FTPs Method 114
Appendix C: Bulk Management of PDUs 116
G5 Upgrade Tool (GUT) 116
Appendix D: System Reset or Password Recovery 119
Appendix E: PDU Alarms 120
Trap Codes assigned to Alarms List 122

Appendix F: Panduit Network Controller Replace or Rotate 180° 129
Appendix G: Direct connect to the PDU by Changing Your PC's IP Address..... 131
Appendix H: Command Line Interface (CLI)..... 137
CLI Commands..... 140
Network Commands 142
User Commands..... 144
Device Commands 144
Power Commands 146
Appendix I: RADIUS Server Configuration 148
Appendix J: Panduit G5 Accessories 150
Appendix K: Compliance Model Number Details..... 151
Appendix L: JSON API Web Service..... 152

Table of Figures

Figure 1: Ethernet Port for Network Connection 9
Figure 2: Status LED & Serial In Port Identified 10
Figure 3: Changing Your Password 12
Figure 4: After Login 12
Figure 5: Change User Password 13
Figure 6: Change Password 13
Figure 7: Login Page 15
Figure 8: Landing Page/Dashboard 15
Figure 9 - Resized Dashboard Screen 17
Figure 10: Power Summary Page 18
Figure 11: Outlet Monitoring Page 19
Figure 12: Environmental Monitoring Page 19
Figure 13: Security Monitoring Page 19
Figure 14: System Management 21
Figure 15: System Management Configuration 22
Figure 16: Rack Location Configuration 23
Figure 17: Power Panel & Core Location 24
Figure 18: NTP Configuration 25
Figure 19: Daylight Saving Time Configuration 26
Figure 20: Control & Manage PDU 28
Figure 21: Outlet Control Enabled 29
Figure 22: Edit Outlets 29
Figure 23: One-Delay Time 30
Figure 24: Saved Sequence 30
Figure 25: Power Threshold 31
Figure 26: Energy Threshold 33
Figure 27: Phase Current Alarm 34
Figure 28: Phase Voltage Alarm 36
Figure 29: Load Segment Breaker 38
Figure 30: Device Detection Threshold Information 40
Figure 31: Outlet Information 41
Figure 32: Email Setup 43
Figure 33: SMTP Account Settings 44
Figure 34: Email Recipients 45
Figure 35: Event Notifications 46
Figure 36: Data Log 48
Figure 37: Data Log Configuration 49

Figure 38: User Settings 51
Figure 39: RADIUS Configuration 52
Figure 40: LDAP Configuration 54
Figure 41: Enable Role Privileges 55
Figure 42: Test LDAP Configuration 56
Figure 43: SNMP Management 57
Figure 44: SNMP General 58
Figure 45: SNMP Port 59
Figure 46: Setup SNMP Port and Trap Port 59
Figure 47: Define SNMP V1/V2c User 60
Figure 48: Edit V1/2c Manager 60
Figure 49: SNMP V3 Manager 61
Figure 50: SNMP V3 Edit 62
Figure 51: SNMPv2 Configuration Information 63
Figure 52: SNMPv3 Trap Server Information. 64
Figure 53: Network Controller 66
Figure 54: Network Controller Menu Structure 68
Figure 55: Main Menu Selections 69
Figure 56: Setup Menu 69
Figure 57: Network Submenu 70
Figure 58: Device Submenu 71
Figure 59: Screen Submenu 72
Figure 60: Language Submenu 73
Figure 61: USB Submenu 74
Figure 62: Units Submenu 75
Figure 63: Alarms Menu 76
Figure 64: Power Menu 77
Figure 65: Device Submenu 78
Figure 66: Phase Submenu 79
Figure 67: Breaker Submenu 80
Figure 68: Outlet Submenu 81
Figure 69: Sensors 82
Figure 70: Connection Diagram RNA Daisy Chain 84
Figure 71: Connection Diagram Power Share & Daisy Chain 87
Figure 72: SmartZone Security Handles 89
Figure 73: Connection Diagram for SmartZone Security Handle 90
Figure 74: Rack Access Control Web GUI 92
Figure 75: Rack Access Control Actions Web GUI 92

Figure 76: Local Rack Access Web GUI 94
Figure 77: Rack Access Settings Web GUI 95
Figure 78: Handle Settings Web GUI 96
Figure 79: Remote Control 98
Figure 80: Beacon 99
Figure 81: Beacon Settings Web GUI 100
Figure 82: Status LED Settings Web GUI 102
Figure 83: Sensor Ports for Vertical PDU 104
Figure 84: Sensor Ports for Horizontal PDU 105
Figure 85: User Settings 105
Figure 86: Celsius Setting 105
Figure 87: Fahrenheit Setting 105
Figure 88: Door Switch Sensor Configuration 109
Figure 89: Dry Contact Cable 110
Figure 90: Temperature and Humidity Sensors 111
Figure 91: Sensor Ports on controller 112
Figure 92: Upload Firmware 113
Figure 93: G5 Upgrade Tool Interface 116
Figure 94: System Management Screen Web GUI 117
Figure 95: G5 Upgrade Tool Interface 117
Figure 96: Example CSV File 118
Figure 97: G5 Upgrade Tool Interface 118
Figure 98: Screws on Network Controller 129
Figure 99: Ribbon Cable for the Network Controller 130
Figure 100: Control Panel 131
Figure 101: Network Status and Tasks 132
Figure 102: Change Adapter Settings 133
Figure 103: Properties 133
Figure 104: Ethernet Properties 134
Figure 105: Internet Protocol Version 4 135
Figure 106: IP Settings for Direct Connection 136
Figure 107: Connect MA017 to the PDU In/Serial port 138
Figure 108: Serial Cable Pinout 139

Section 1 – System Overview

PDU Controller

All Panduit G5 Intelligent PDUs feature a Rotatable or Hot Swappable Intelligent Network Controller (iNC). This centralized piece of intelligent hardware receives an IP address, contains a Graphical Web Interface and is addressable over the network.

Connecting the PDU via Ethernet Port

Connecting the PDU to a LAN provides communication through an Internet or Intranet connection enabling monitoring and control over the intelligent power distribution unit.

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

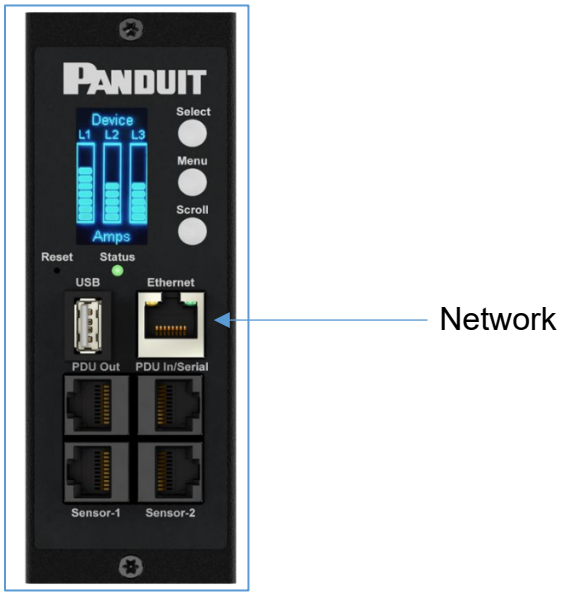


Figure 1: Ethernet Port for Network Connection

From the factory the PDU defaults to DHCP and HTTP**S** connection. If you are connected to a network with a DHCP server, the PDU automatically receives an IP address and will display it on the OLED screen. If there is no DHCP server after several minutes, the PDU defaults to IP address is 192.168.0.1, which will be displayed on the PDU OLED screen. If the network cable is unplugged and plugged back in, the PDU will restart the DHCP server search process.

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 (see Figure 2).

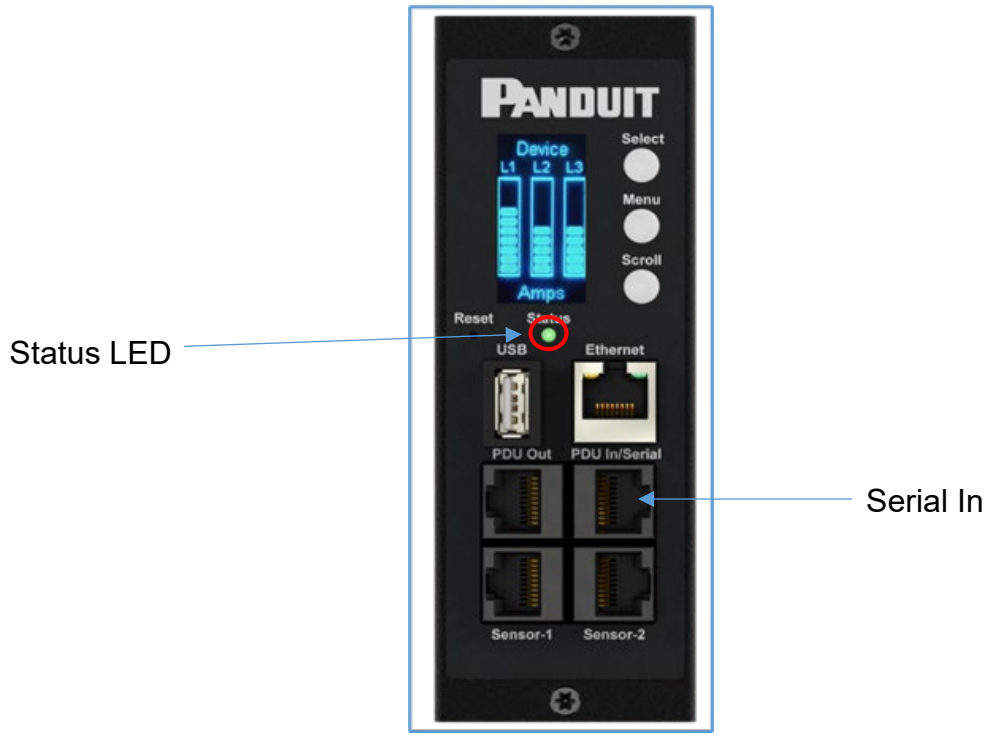


Figure 2: Status LED & Serial In Port Identified

Additional details in Appendix G.

Section 2 – Web Graphical User Interface (GUI) Configuration

Internet Protocol (IP) Addressing

After the PDU receives an IP address, login to the Web interface to configure the PDU and assign a static IP address (if desired).

Connecting to the PDU

1. Ethernet port on the PDU indicates solid green light on the right and a flashing yellow light on the left. This indicates successful connectivity to the network.
2. 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.
3. In a standard web browser, enter the PDU IP address (“https://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 Google Chrome (mobile and desktop), Mozilla Firefox, Microsoft Edge and Apple Safari (mobile and desktop).

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.

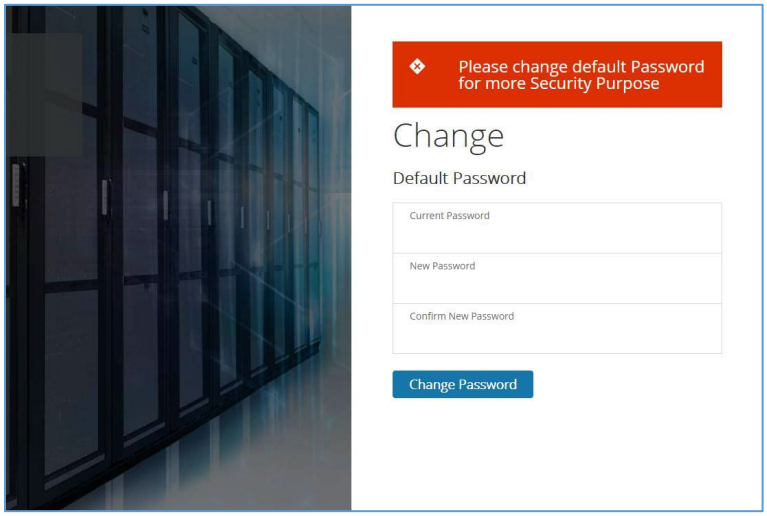


Figure 3: Changing Your Password

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.

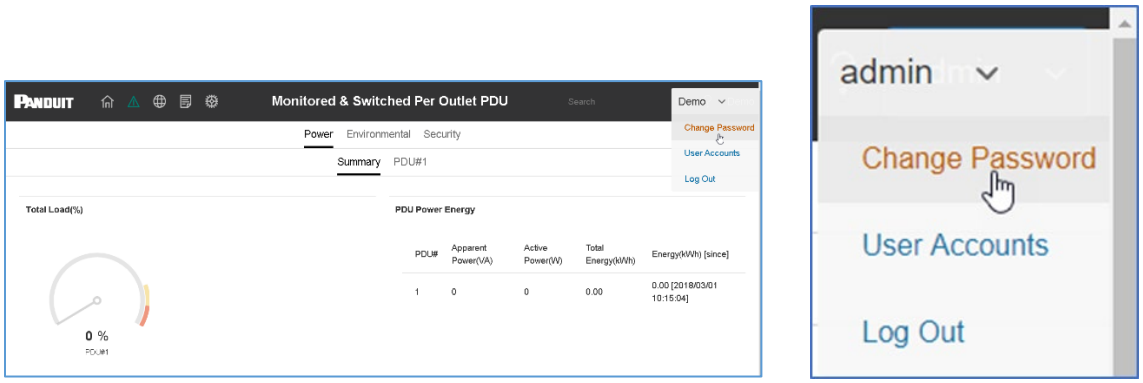
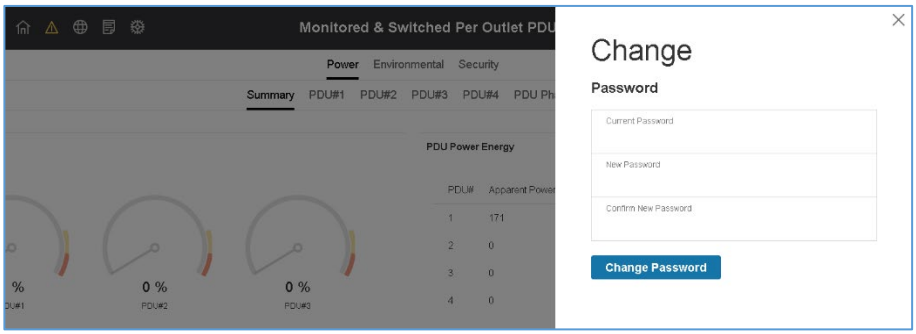


Figure 4: After Login

2. The Change User Password window opens.

Figure 5: 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.

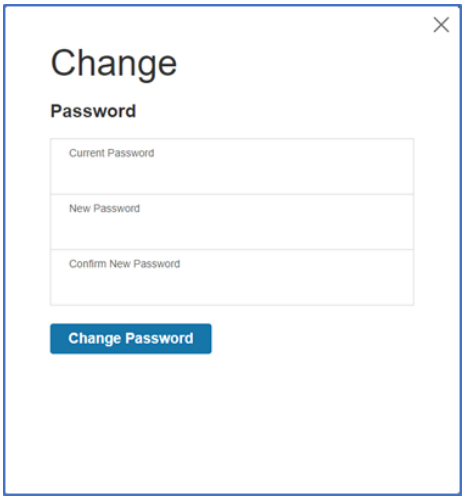
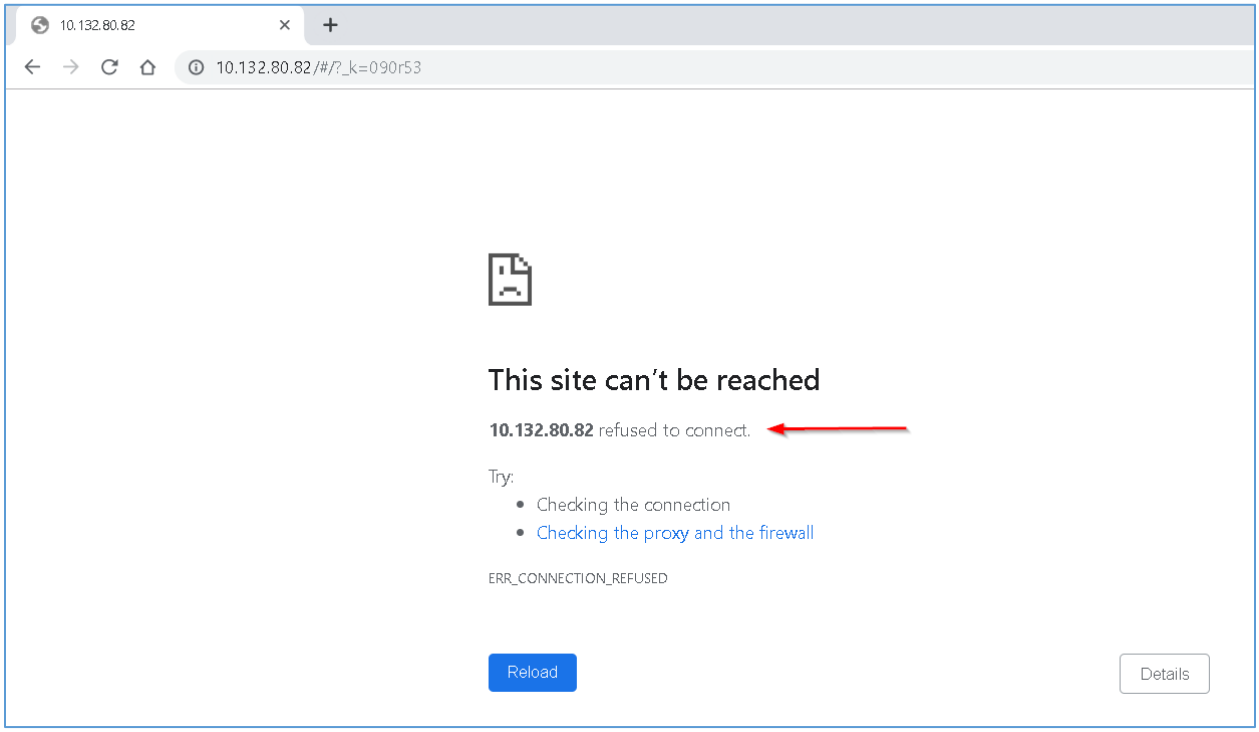


Figure 6: Change Password

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

Logging in to the Web Interface

- Open a supported web browser and enter the IP address of the PDU (HTTPS)
- If browser displays “refused to connect” please *double check* that you are using the “https://” protocol not “http://”



- If username and password have NOT been configured, use the default username: ***admin*** and password: ***12345678***. For security purposes, a change of password is required upon initial login.
- If admin credentials are lost use Appendix D to factory reset the PDU.

Introduction to the Web GUI

Login Page Note: https:// must be used (for initial login)

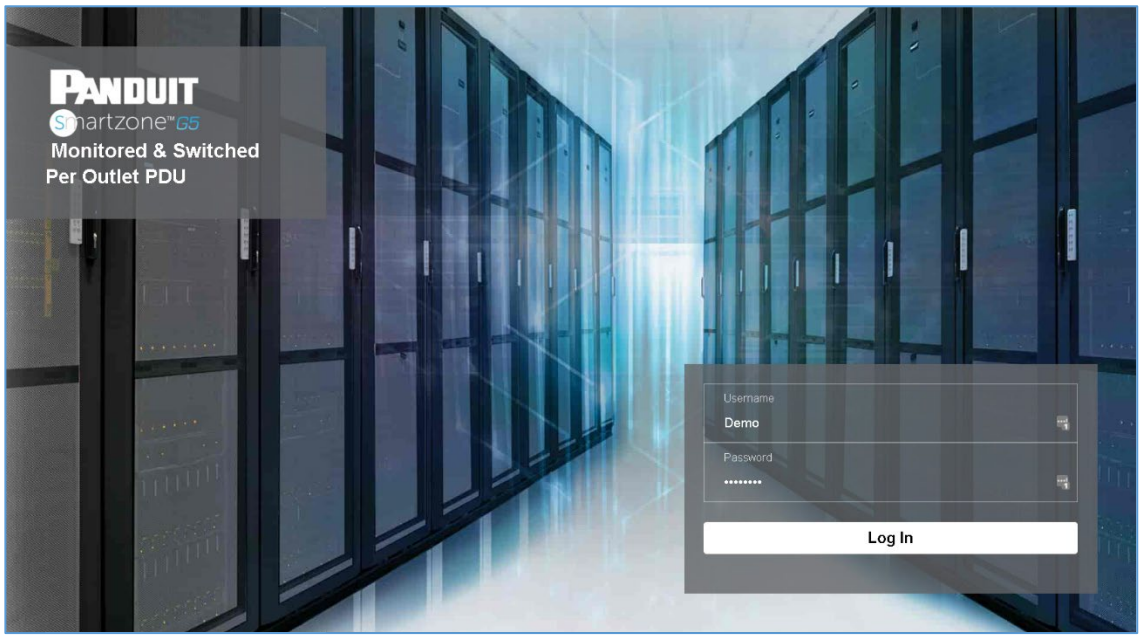


Figure 7: Login Page

Landing Page/Dashboard

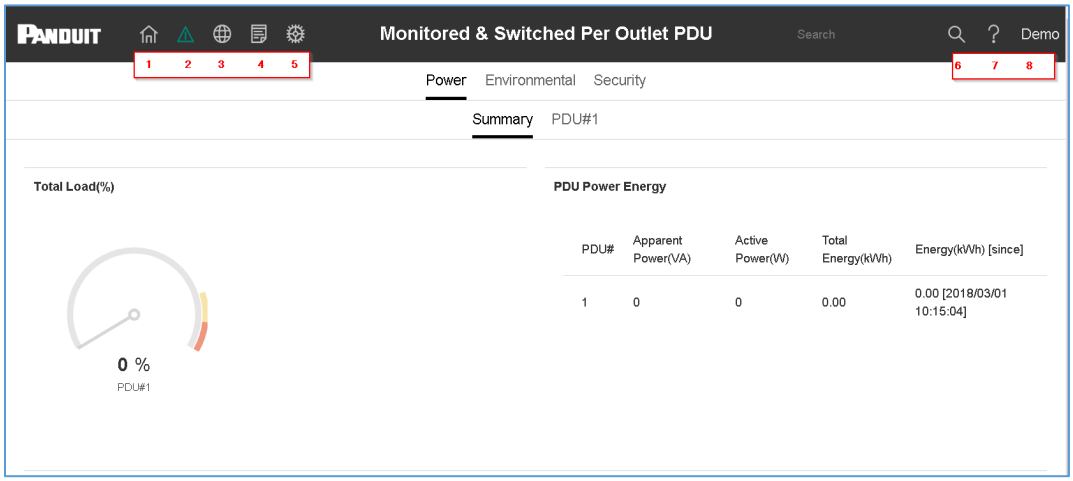


Figure 8: Landing Page/Dashboard

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. • 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

Number	Icon	Description
		click user guide and license to ask for help.
8	admin	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.

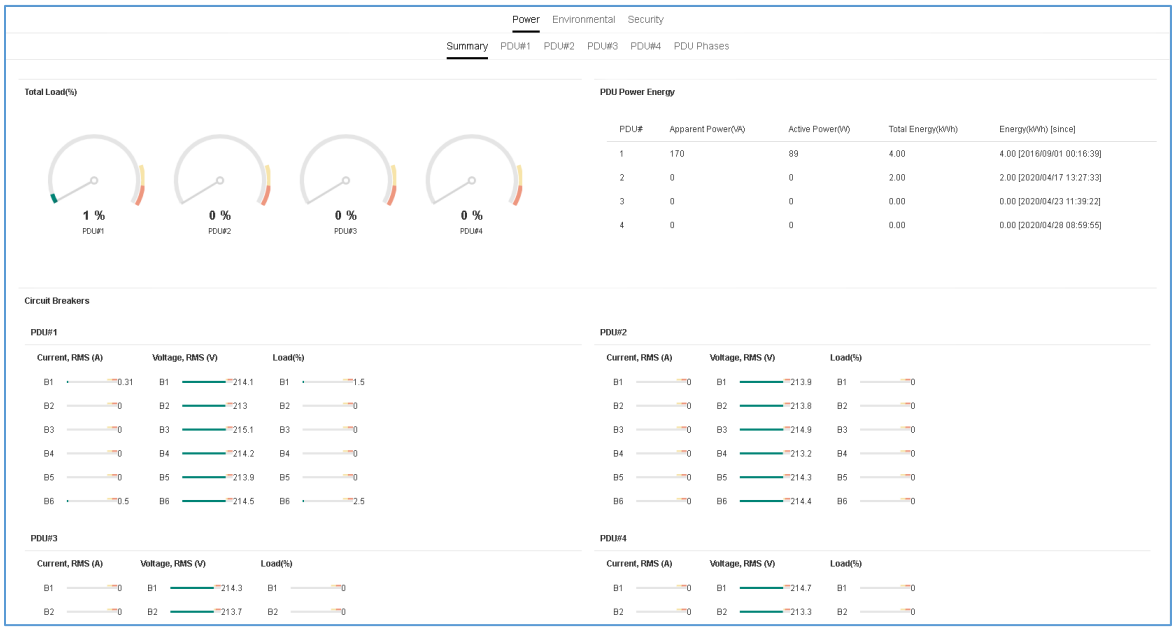


Figure 9 - Resized Dashboard Screen

Menu Dropdowns

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

Introduction to the Dashboard

Power Summary Page

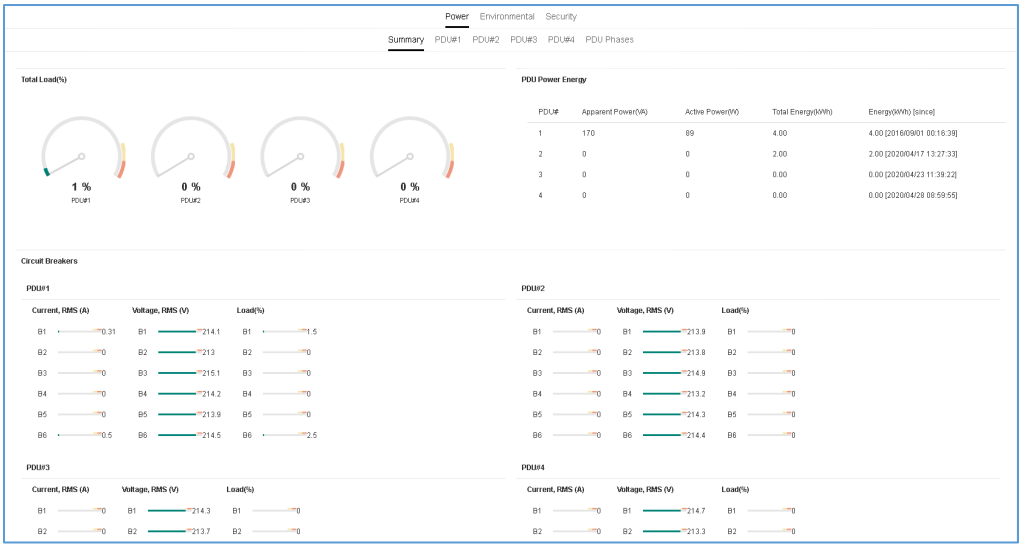


Figure 10: Power Summary Page

Outlet Monitoring Page



Figure 11: Outlet Monitoring Page

Environmental Monitoring Page

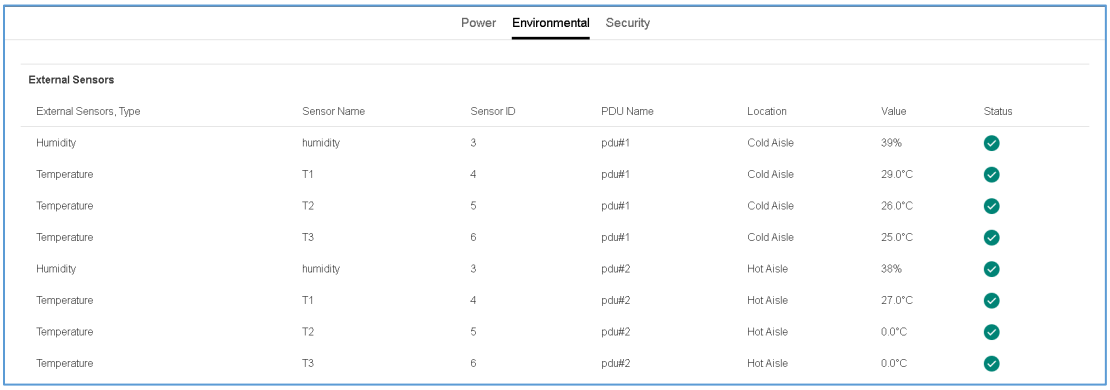


Figure 12: Environmental Monitoring Page

Security Monitoring Page

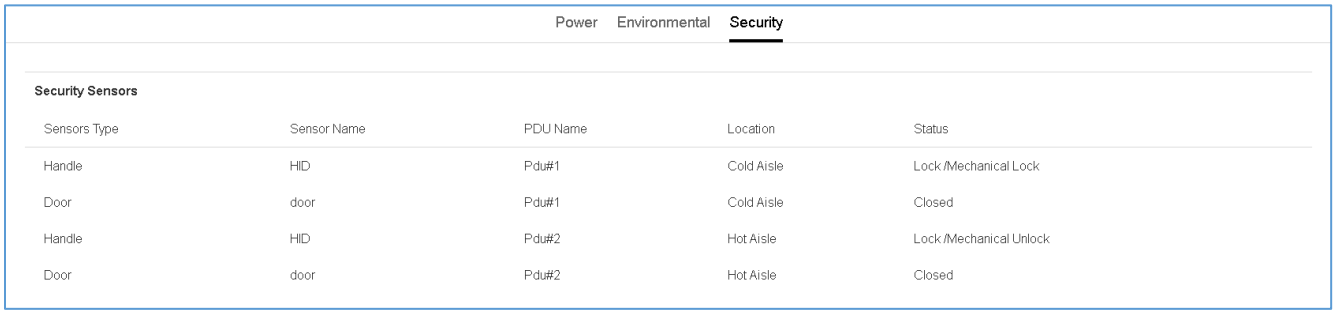
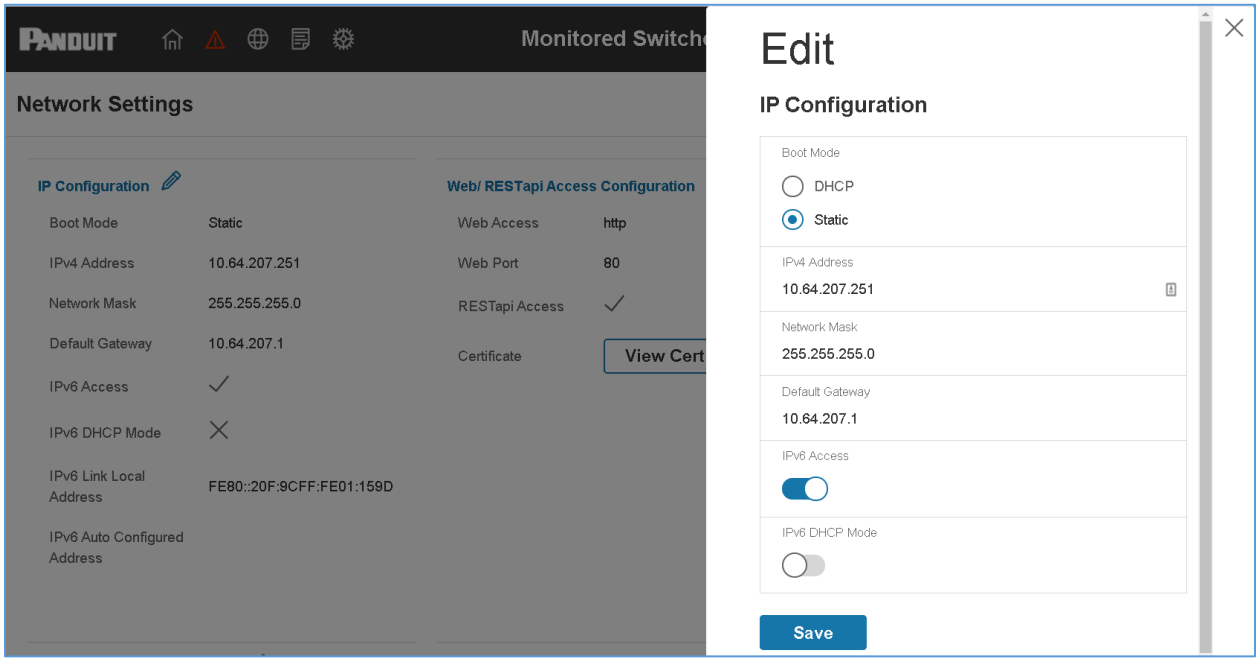


Figure 13: Security Monitoring Page

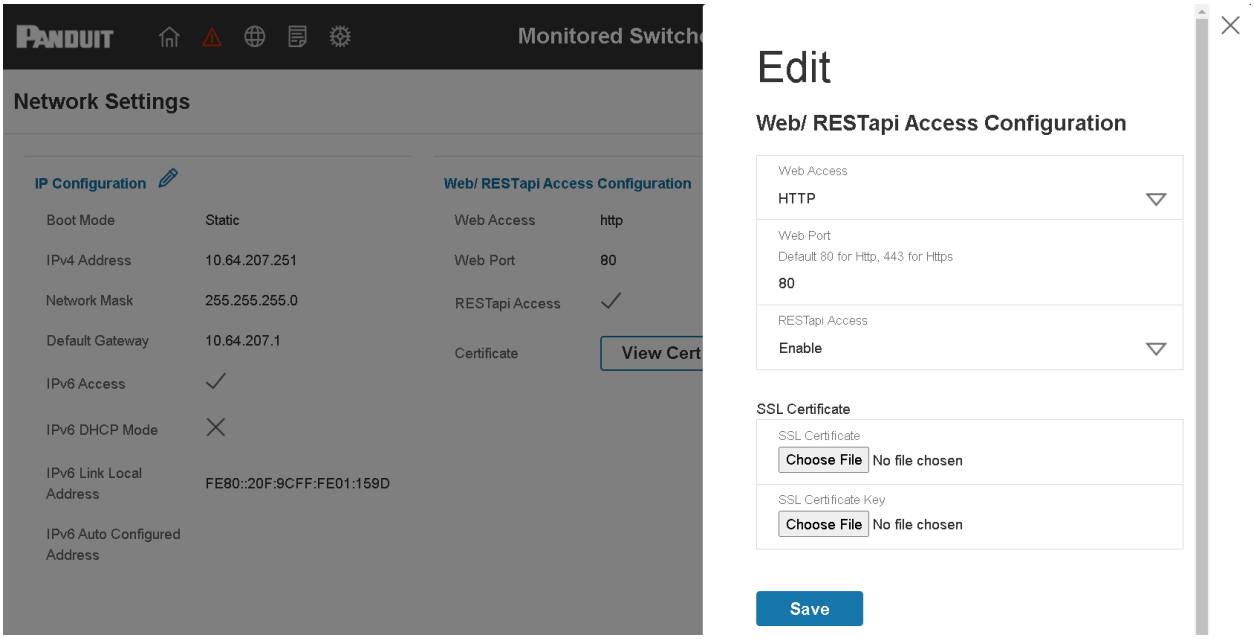
Network Settings

The Network Settings allow management of IP Configuration, Web RESTapi Access Configuration, SSH/FTPs Configuration, Network Time Protocol (NTP), Date/Time Settings and Daylight-Savings Time.

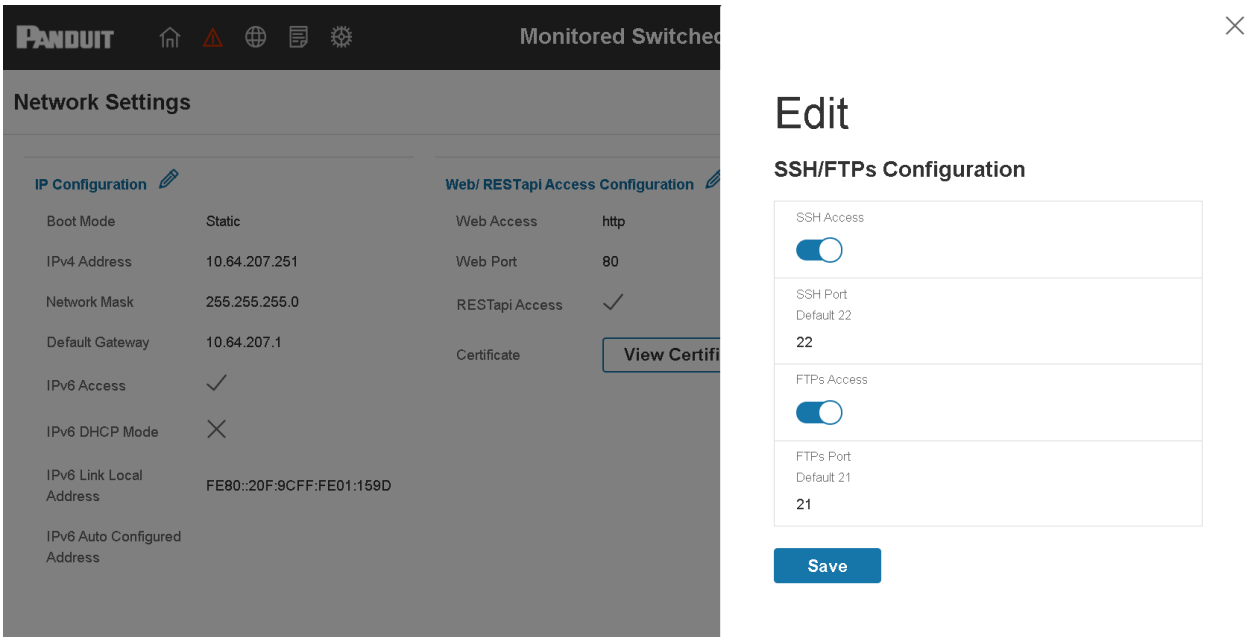
IP Configuration:



Web RESTapi Access Configuration can be used to set HTTP, HTTPS or Disable the onboard Web GUI.



SSH/FTP 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.

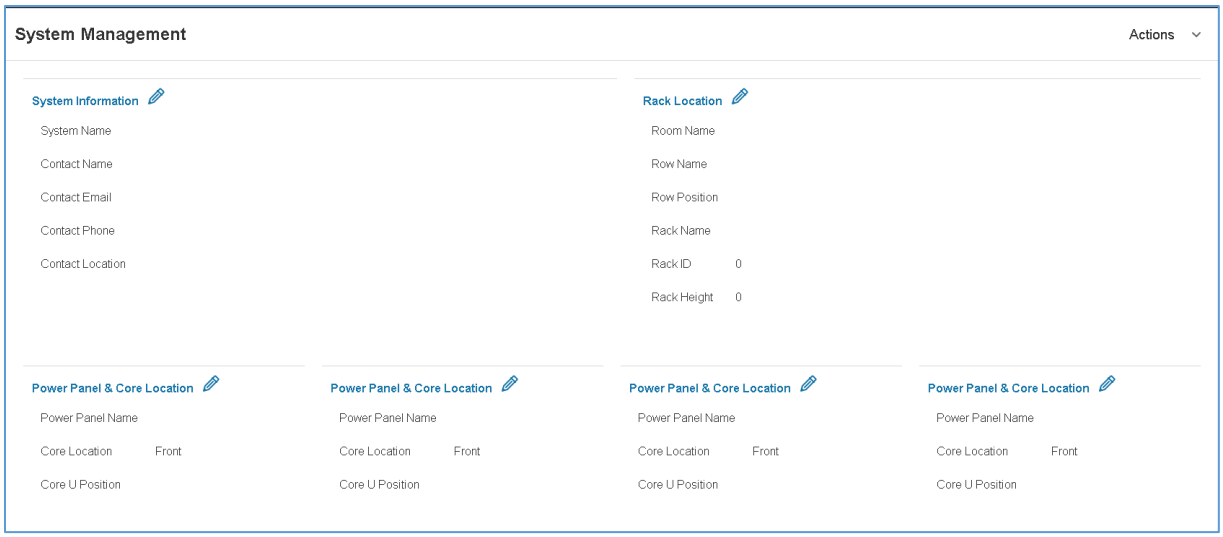


Figure 14: System Management

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.**

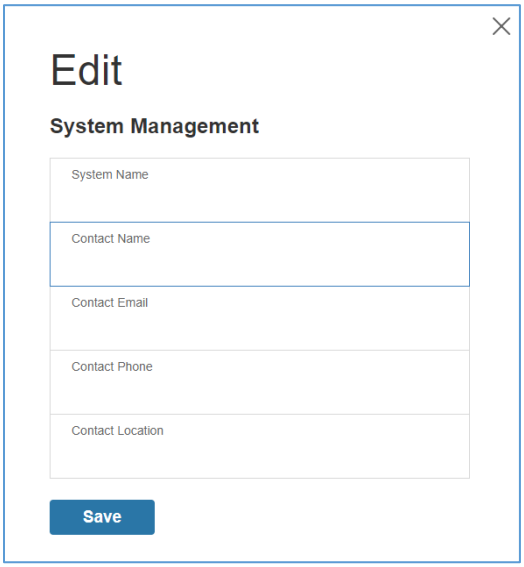


Figure 15: System Management Configuration

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**.
    a. Note: If editing ‘system management’ – all fields are required to be filled to save the information.

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.**

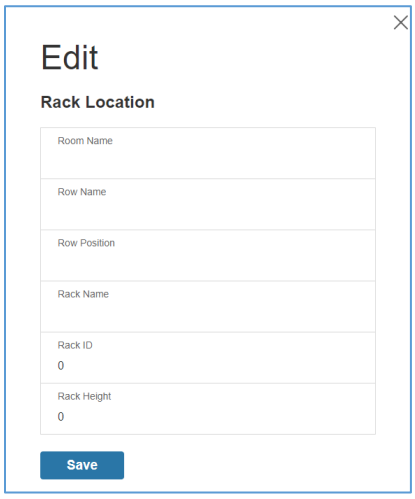


Figure 16: Rack Location Configuration

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.

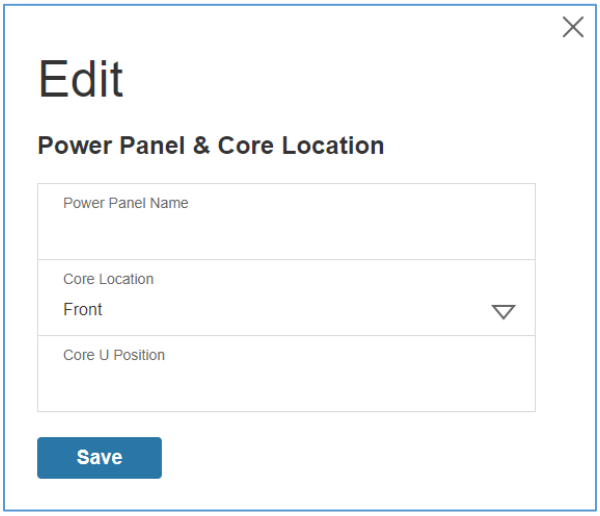


Figure 17: Power Panel & Core Location

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**.

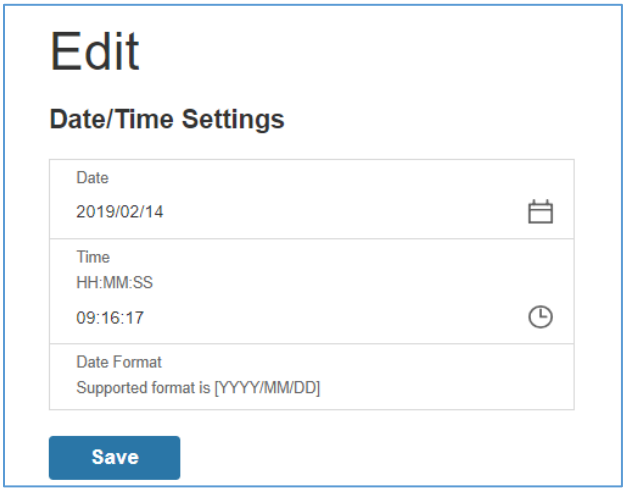
Note: If editing 'Power Panel & Core Location' – all fields are required to be filled to save the information.

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).

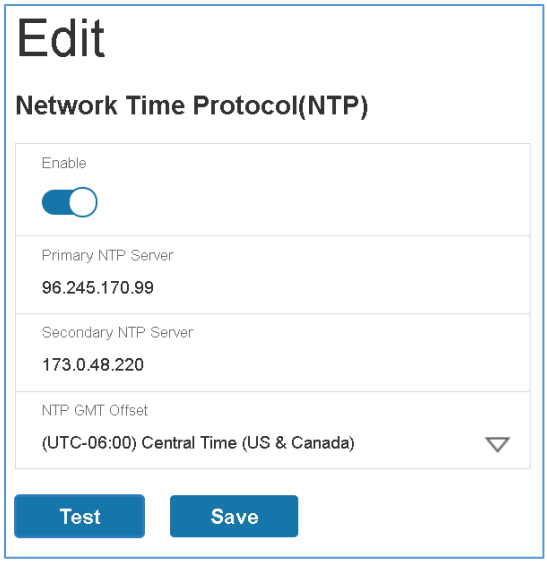


Figure 18: NTP Configuration

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**.

Note: NTP Server must be online to test and save the settings.

Setting Daylight Saving Time

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

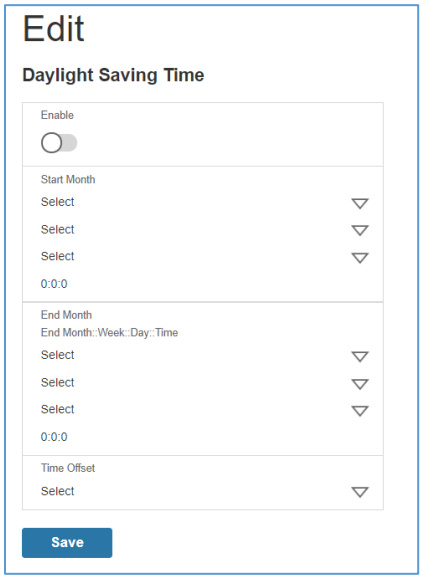


Figure 19: Daylight Saving Time Configuration

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.

Outlet Power Management

Naming an Outlet

For Panduit PDUs with outlet level control or monitoring, you can customize each outlet and view all circuit breaker to outlet associations through the Web 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 PDUs 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 PDU 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 PDUs

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.**

Outlet Power Sequence Setup

The outlets can be programmed to have a pre-determined on delay or off delay. (E.g. On Delay can be used to implement power on sequencing to avoid surge spikes or circuit breaker overload associated with IT equipment all being turned on at the same time.)

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

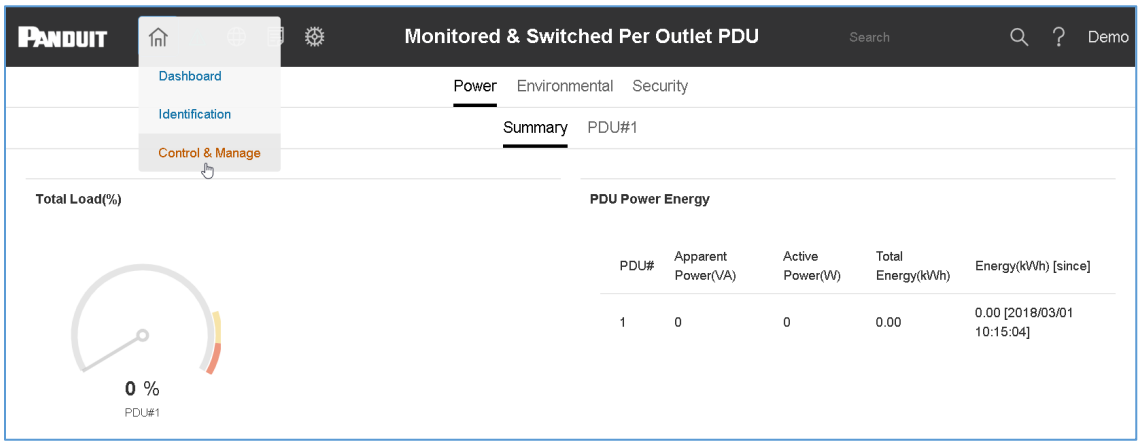


Figure 20: Control & Manage PDU

2. Select Outlet Control Enabled.

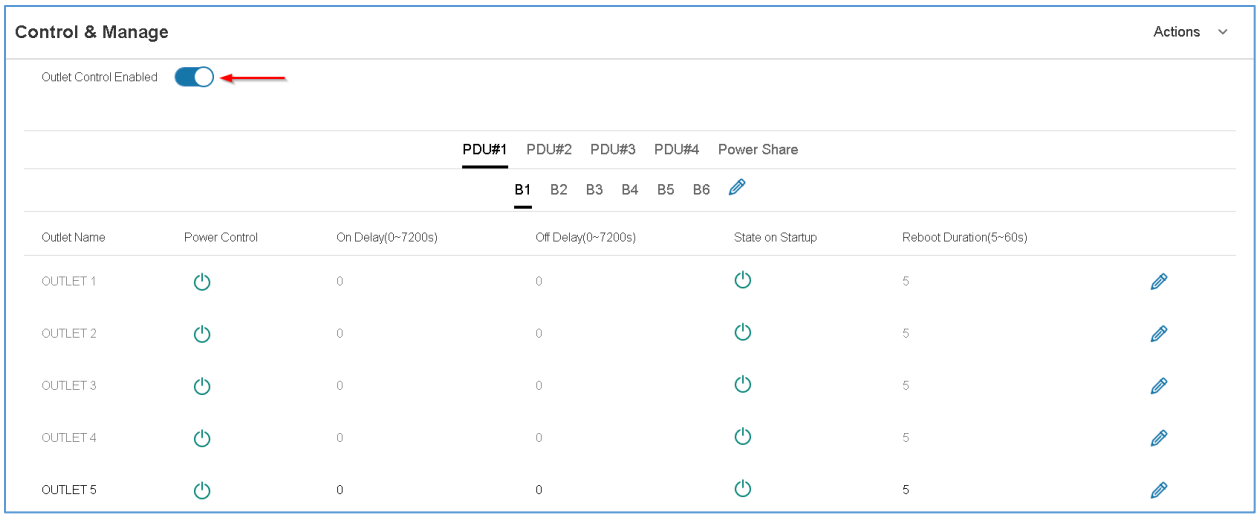


Figure 21: Outlet Control Enabled

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

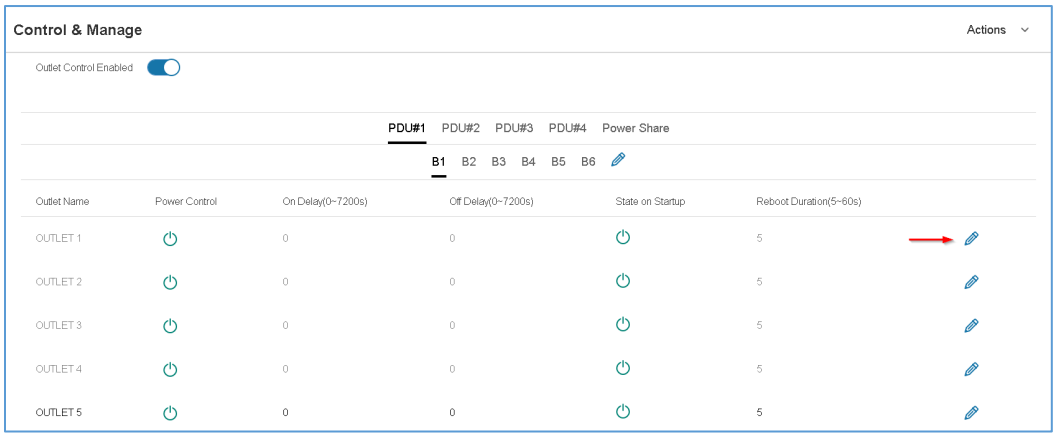


Figure 22: Edit Outlets

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

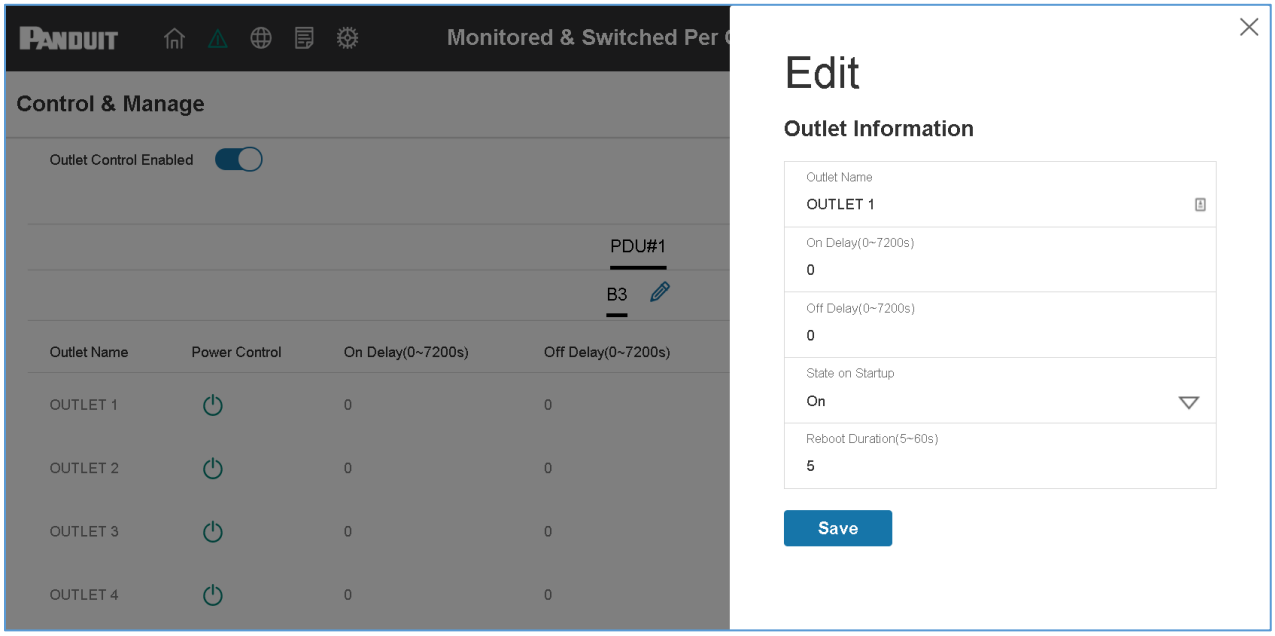


Figure 23: One-Delay Time

5. Your Outlet Power Sequence has been set.

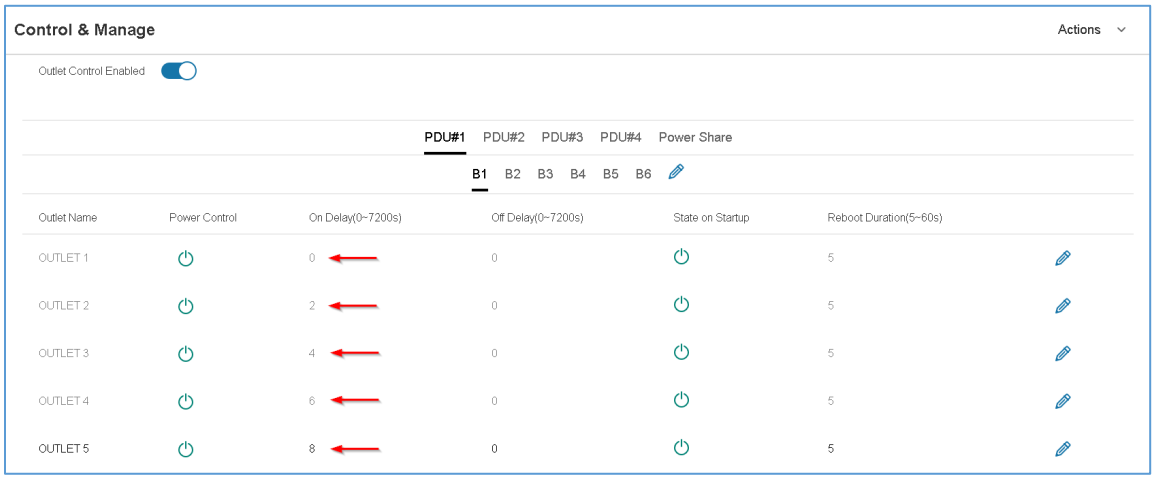


Figure 24: Saved Sequence

Setting Metering Thresholds

Power Threshold

The PANDUIT PDU 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.

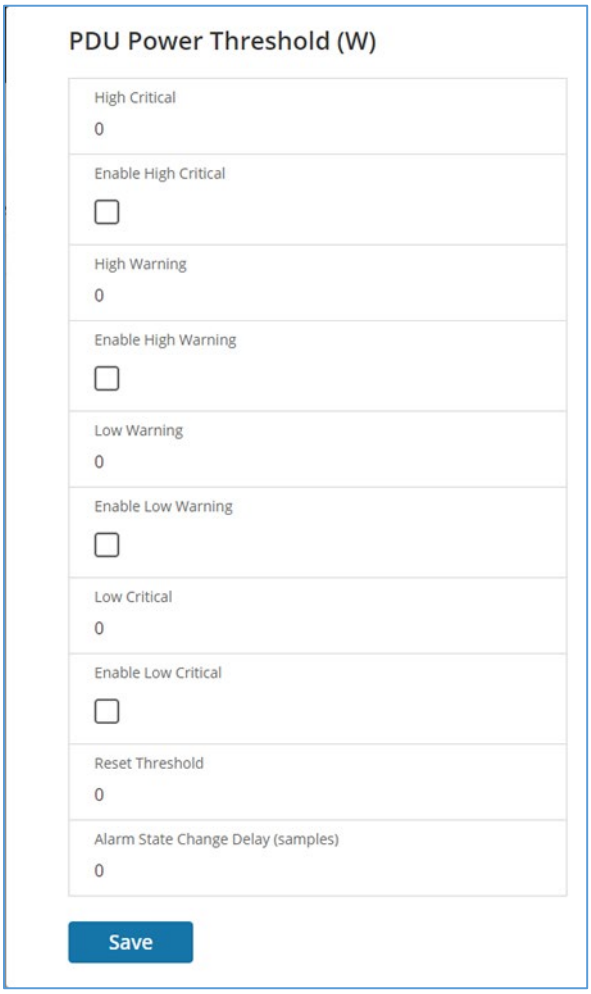


Figure 25: Power Threshold

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 PANDUIT PDU 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.

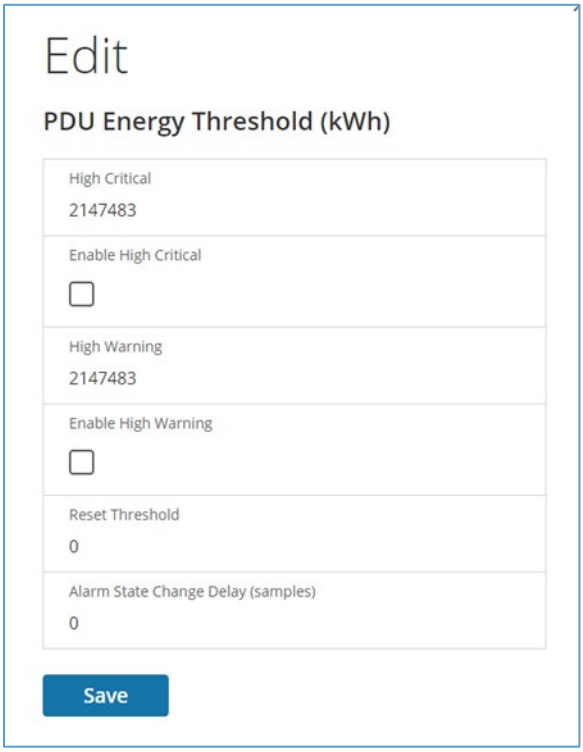


Figure 26: Energy Threshold

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 PANDUIT PDU 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.

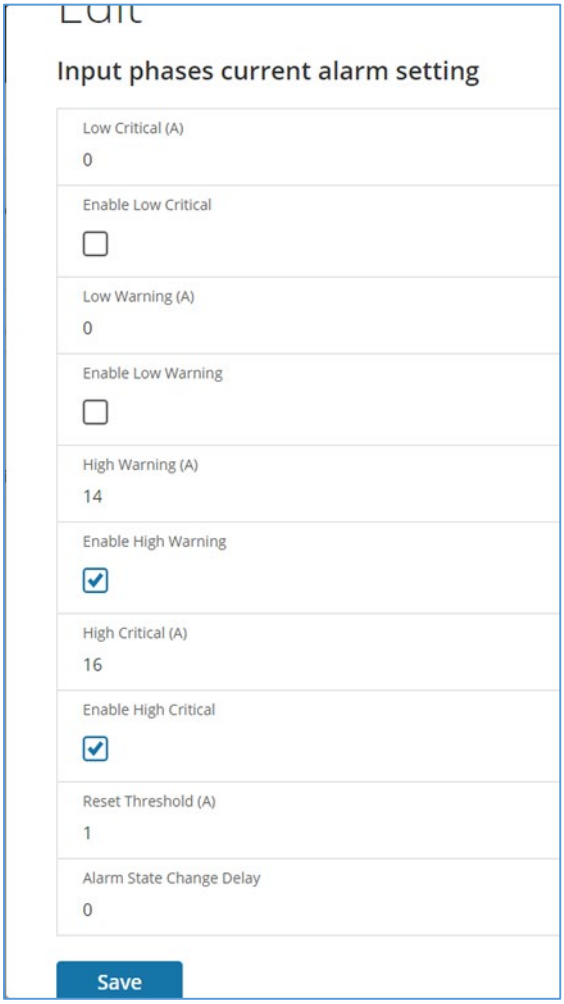


Figure 27: Phase Current Alarm

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 PANDUIT PDU 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.

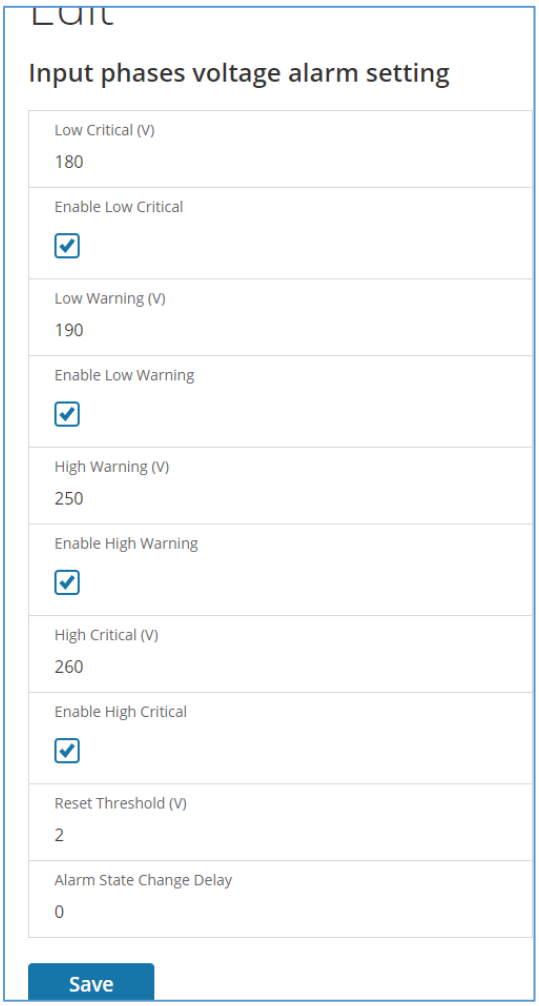


Figure 28: Phase Voltage Alarm

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 PANDUIT PDU 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.

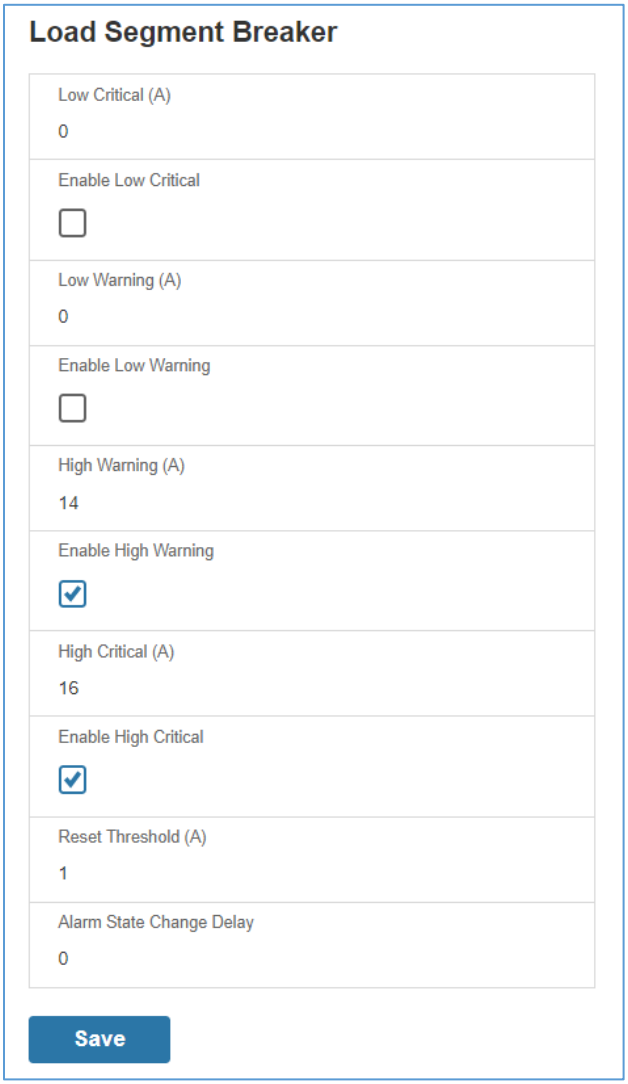


Figure 29: Load Segment Breaker

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**.

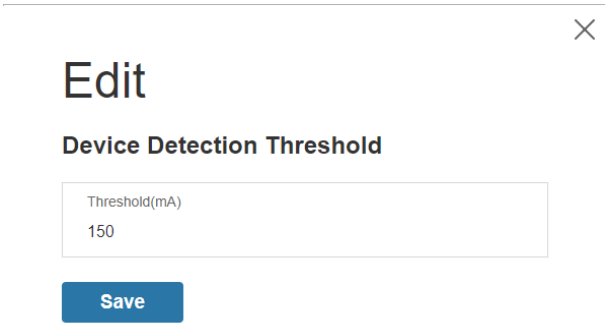


Figure 30: Device Detection Threshold Information

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

Outlet Alarm Threshold

The PANDUIT PDU 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.

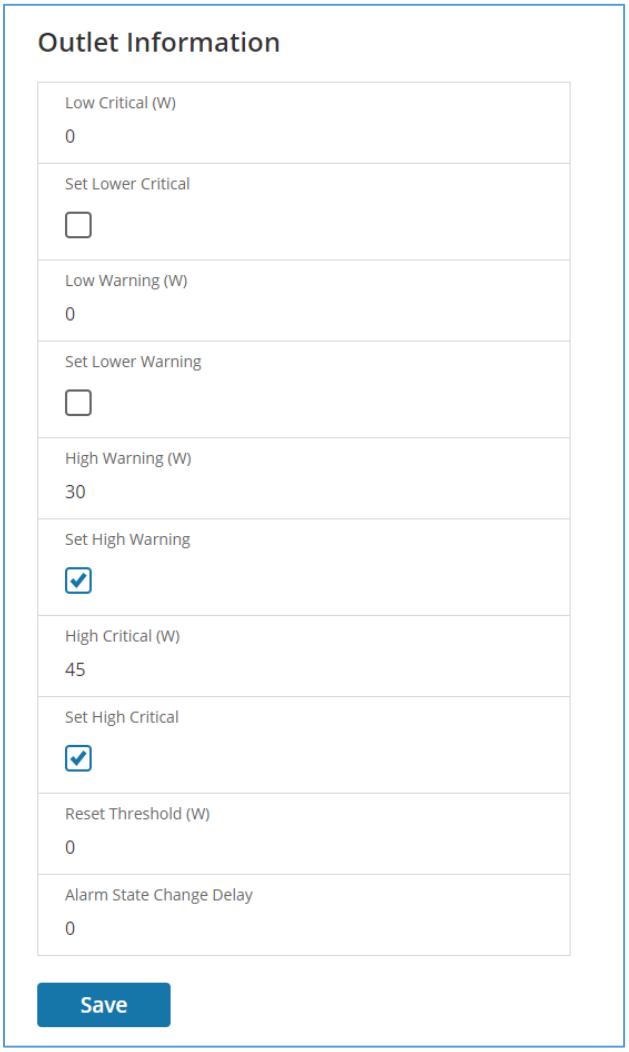


Figure 31: Outlet Information

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 Panduit PDU can be configured to send Emails to specific users when an event occurs. To do this, the information about the SMTP (Simple Mail Transfer Protocol) server needs to be configured.

Note: SMTP does not support SSL.

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

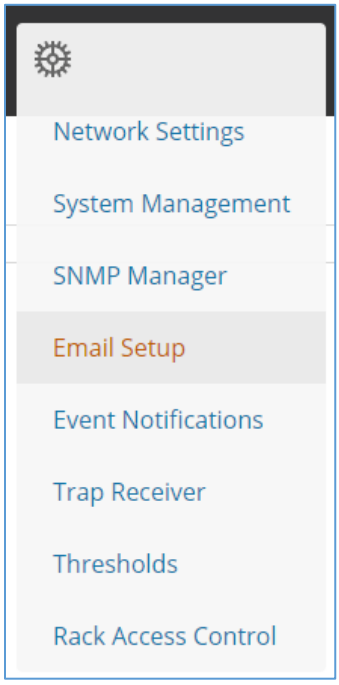


Figure 32: Email Setup

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

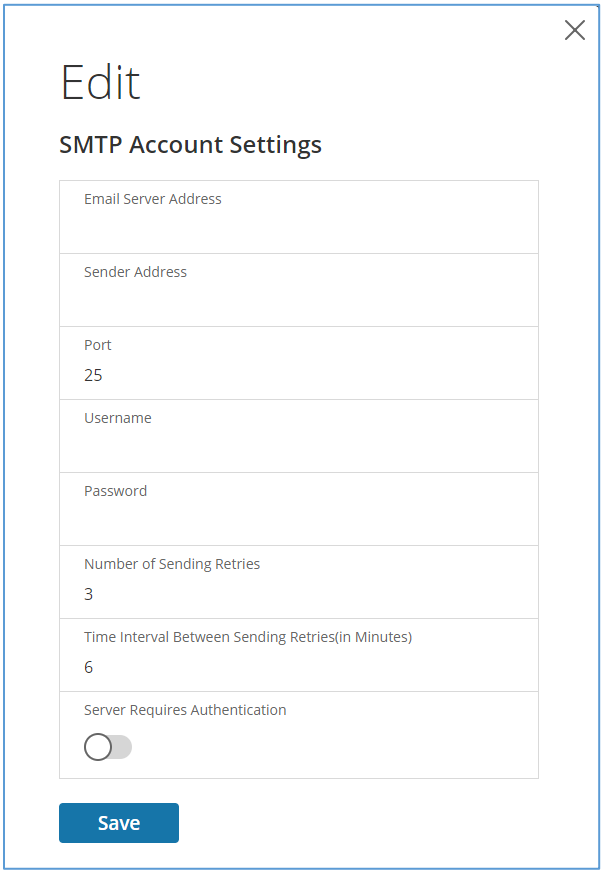


Figure 33: SMTP Account Settings

- Set the **Email Server Address**. This is the IP address of the SMTP that is going to accept the messages.
- Set the **Sender Address.** This is the email address that the email is sent from. You could use a unique email address on each PDU or the same email address across all PDUs.
- Configure the **Port** number. The port number is the communication endpoint on the server. The default is 25. Other common SMTP ports are 587 and 465
- If the SMTP server requires authentication, enter the **username** and **password.** These will be determined by the configuration on the SMTP server. If the SMTP does not require authentication, a **username** and **password** will need to be entered, but they will not be used.
- Set **Number of Sending Retries.** This will be the number of times the

PDU will attempt to resend a message if the message fails. The default setting is 3.

- Set **Time Interval Between Sending Retires (In Minutes).** This is the time, in minutes, the PDU will wait before retrying to send a failed message. The default setting is 6 minutes.
- Choose whether **Server Requires Password Authentication** is needed or not. If the SMTP server requires a username and password, this option needs to be selected.

3. Press **Save** when done.

Next, fill out the Email Recipients list.

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

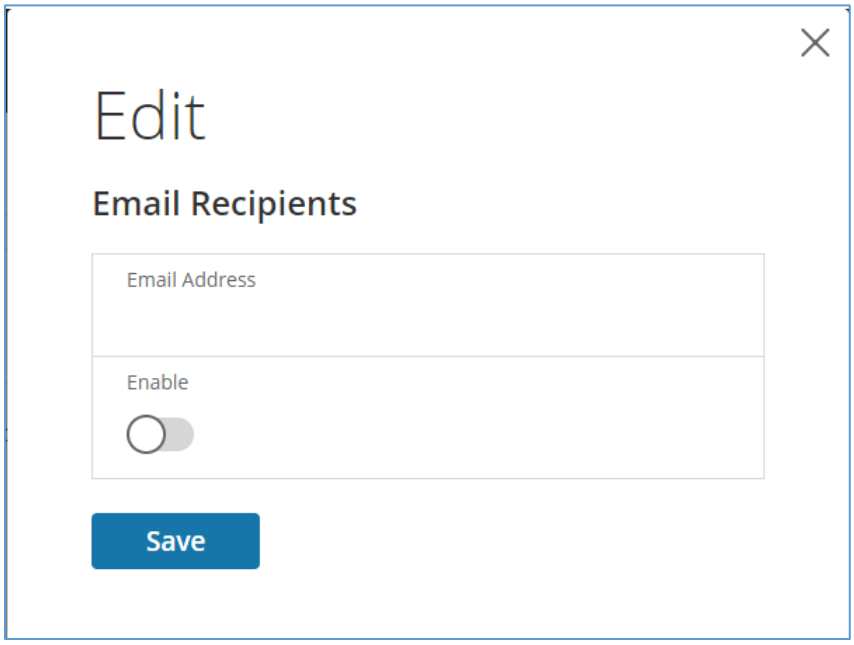


Figure 34: Email Recipients

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

Note: A maximum of 5 users can be entered to receive email alerts.

Event Notifications

The Panduit G5 iPDU can be configured to provide event notifications.

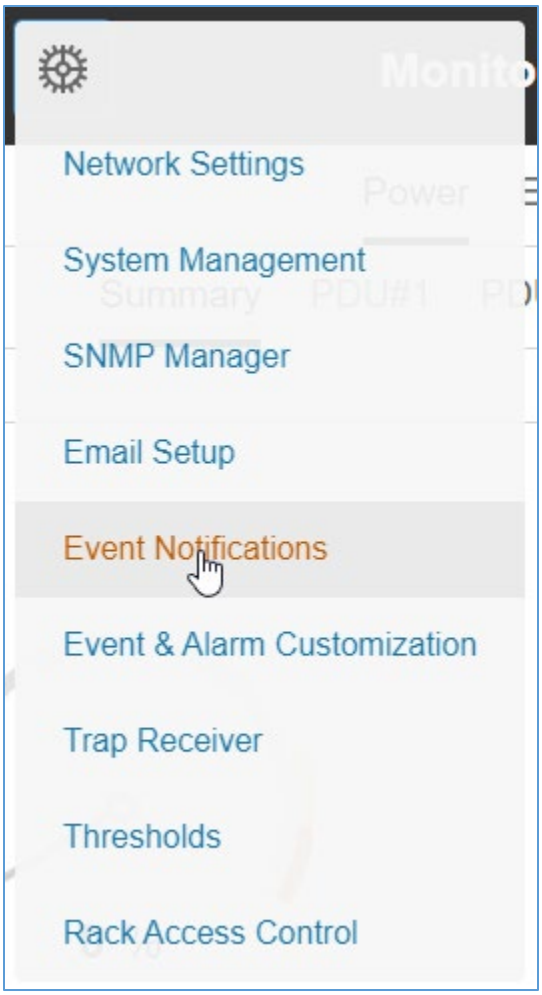


Figure 35: Event Notifications

Note: Not every Event Notification applies or is supported by every PDU type even though the toggle switch in the Web GUI may seem like the feature is supported. In that instance the user is advised to ignore that toggle switch.

Below is a table of PDU types and the Event Notifications that particular PDU type supports.

Event Notifications	Monitored Input (MI Series)	Monitored Input > 6 Breakers (MI Series)	Monitored Switched (MS Series)	Monitored Switched > 6 Breakers (MS Series)	Monitored Per Outlet (MPO Series)	Monitored and Switched Per Outlet (MSPO Series)
Circuit Breaker Status Changed	X	X	✓	X	✓	✓
Breaker Voltage	X	X	✓	X	✓	✓
Breaker/Group Current	✓	X	✓	X	✓	✓
User Activity	✓	✓	✓	✓	✓	✓
Smart Rack Access	✓	✓	✓	✓	✓	✓
Outlet Power Control Status Changed	X	X	✓	✓	X	✓
User Status Changed	✓	✓	✓	✓	✓	✓
Critical Alarm	✓	✓	✓	✓	✓	✓
Warning Alarm	✓	✓	✓	✓	✓	✓
Password/Settings Changed	✓	✓	✓	✓	✓	✓
Network Card Reset/Start	✓	✓	✓	✓	✓	✓
External Sensor Status Changed	✓	✓	✓	✓	✓	✓
PDU Configuration File Imported/Exported	✓	✓	✓	✓	✓	✓
User Role Status Changed	✓	✓	✓	✓	✓	✓
Firmware Updated	✓	✓	✓	✓	✓	✓
Communication Status Changed	✓	✓	✓	✓	✓	✓
Daisy Chain Status Changed	✓	✓	✓	✓	✓	✓
Enter Bootloader Mode	✓	✓	✓	✓	✓	✓
LDAP/Radius Error	✓	✓	✓	✓	✓	✓

Power Share Changed	✓	✓	✓	✓	✓	✓

Data Log

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**.

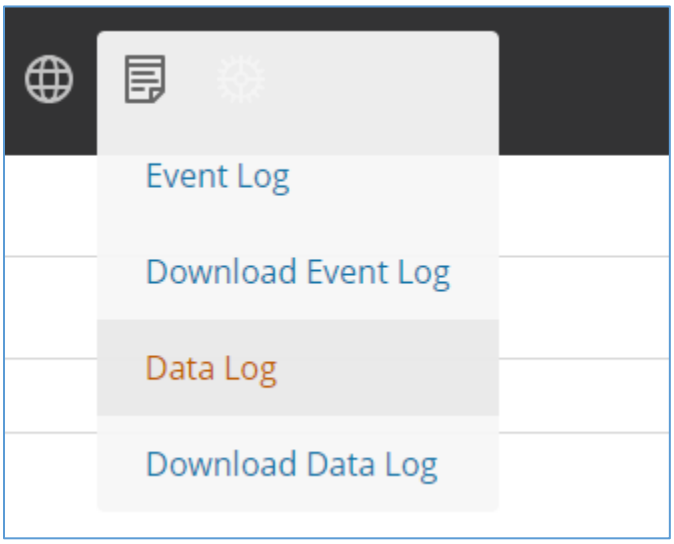


Figure 36: Data Log

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

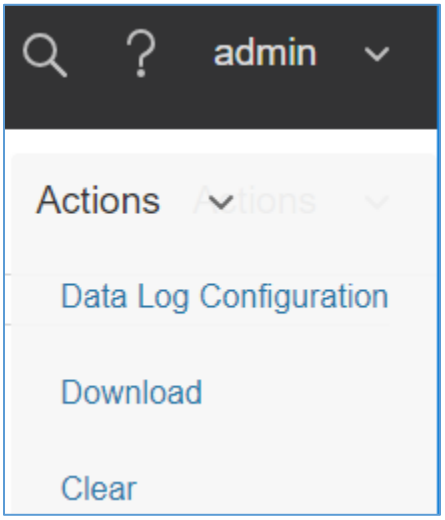


Figure 37: Data Log Configuration

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**.

Web Interface Access

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 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.

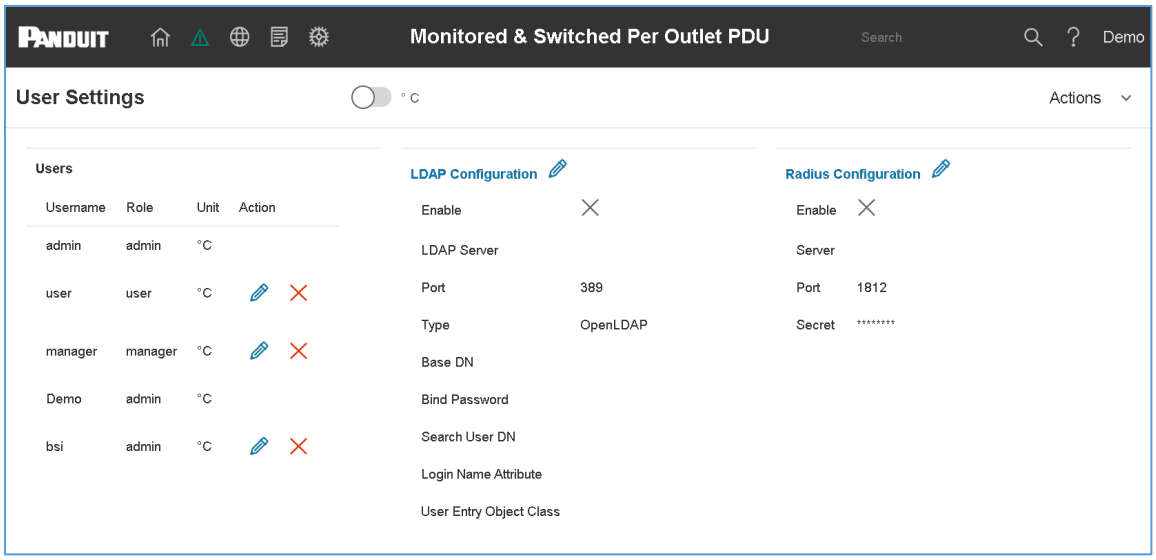


Figure 38: User Settings

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

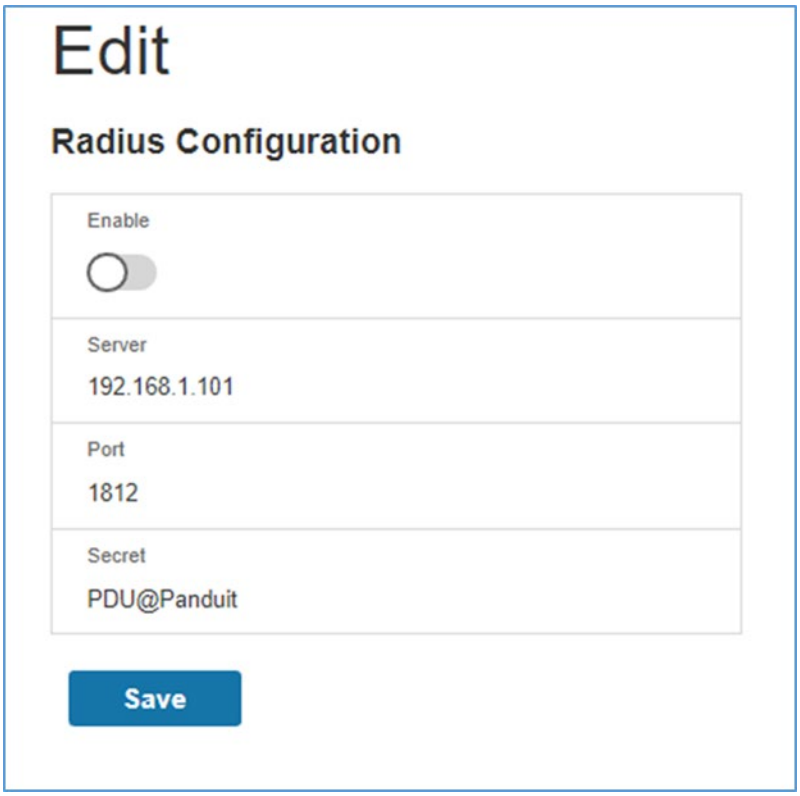


Figure 39: RADIUS Configuration

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.

> Note: By default, a RADIUS user will have the "user" Role if one is not specified. The administrator of the RADIUS server may configure a Panduit vendor (19536) dictionary, with a "User-Role" integer attribute set to User (1) or Admin (2). When this User-Role attribute is the first attribute for the user, that user will have the admin Role after logging in. For complete details, see Appendix H: Radius Server Configuration

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.

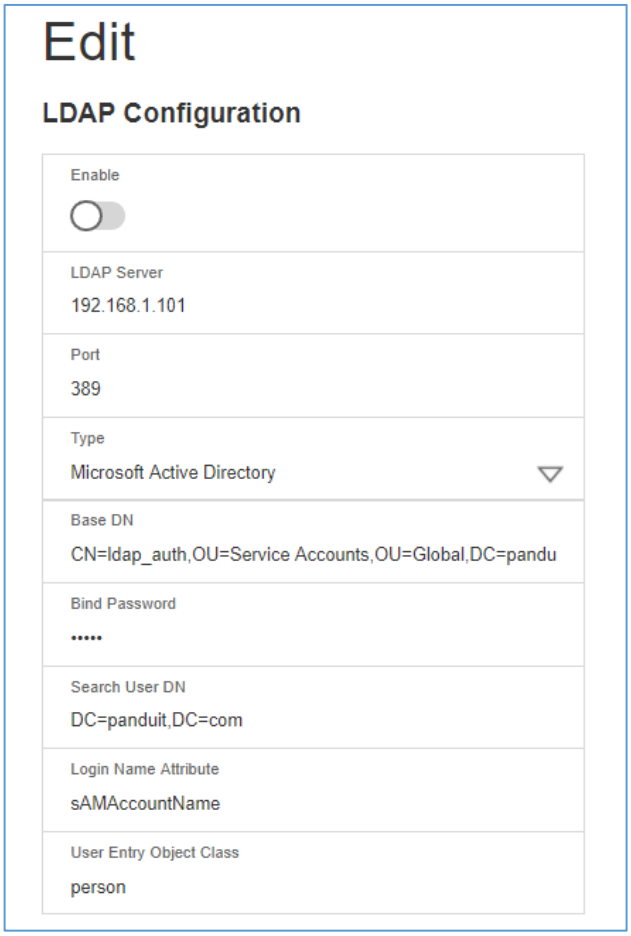


Figure 40: LDAP Configuration

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*

Note: There are no limits to the amounts of admins that the PDU imposes. However, there may be limits by the LDAP server.

2. Within the PANDUIT 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).

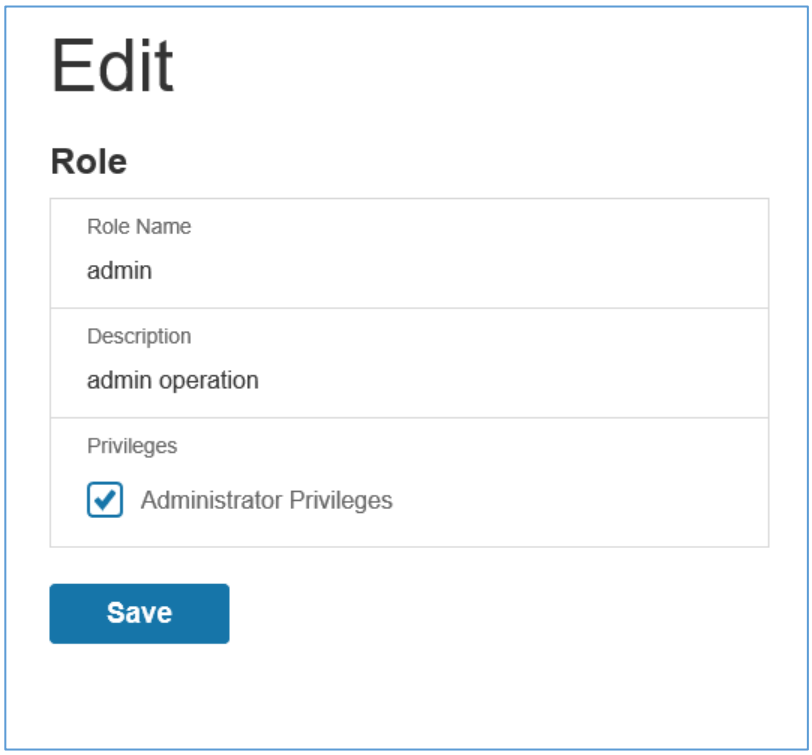


Figure 41: Enable Role Privileges

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.

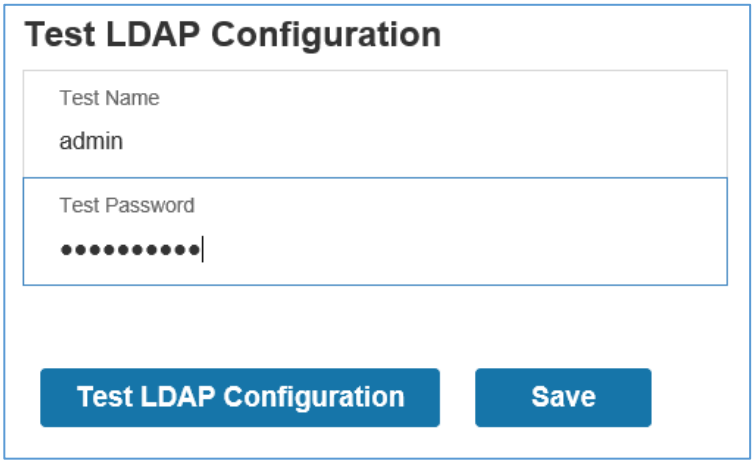


Figure 42: Test LDAP Configuration

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

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.

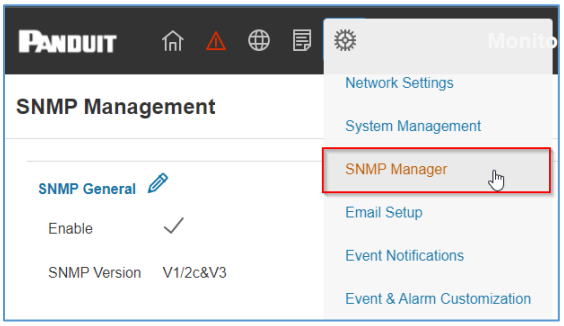


Figure 43: SNMP Management

3. The SNMP General includes SNMP Access and Version.

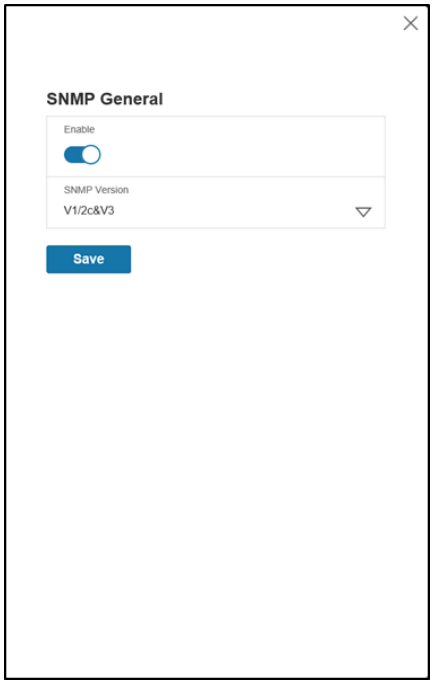


Figure 44: SNMP General

Setup SNMP Port

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

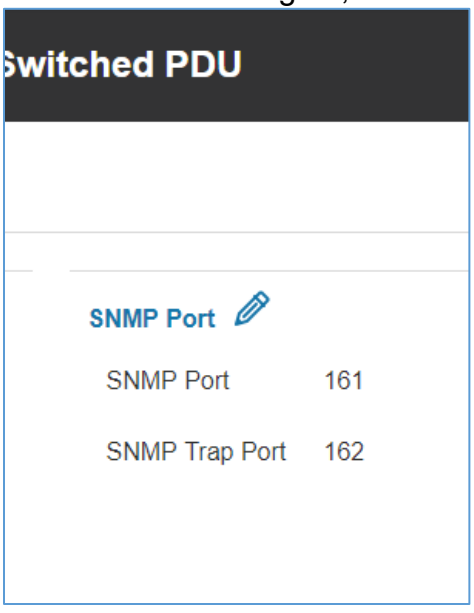


Figure 45: SNMP Port

3. Set up SNMP Port and SNMP Trap Port.

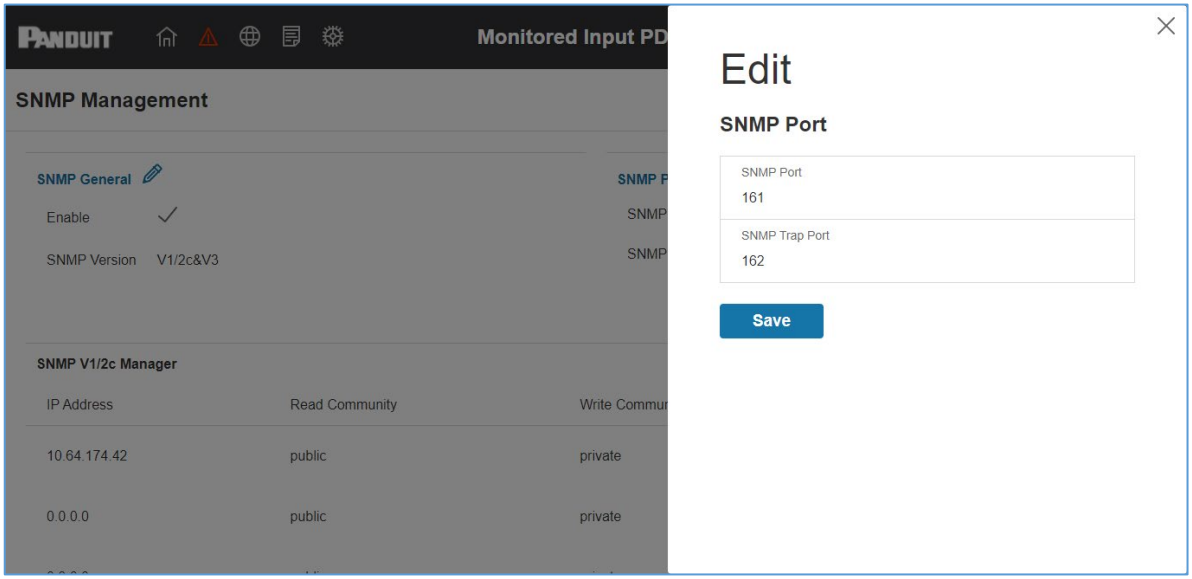


Figure 46: Setup SNMP Port and Trap Port

Configuring Users for SNMP V1/V2c

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 47: Define SNMP V1/V2c User

4. The Edit panel pop up displays.

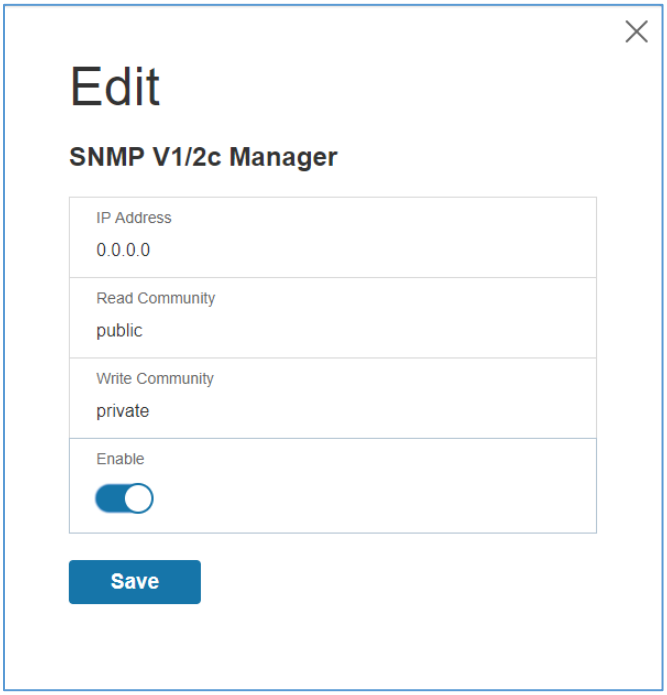


Figure 48: Edit V1/2c Manager

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

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.

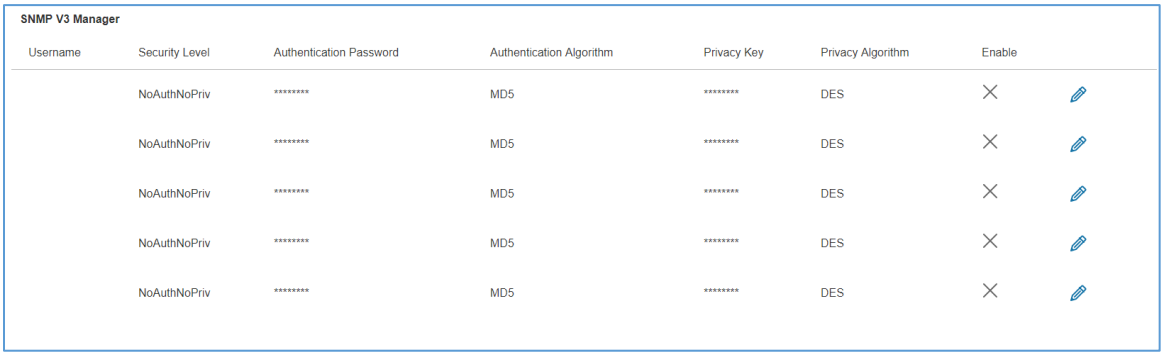


Figure 49: SNMP V3 Manager

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

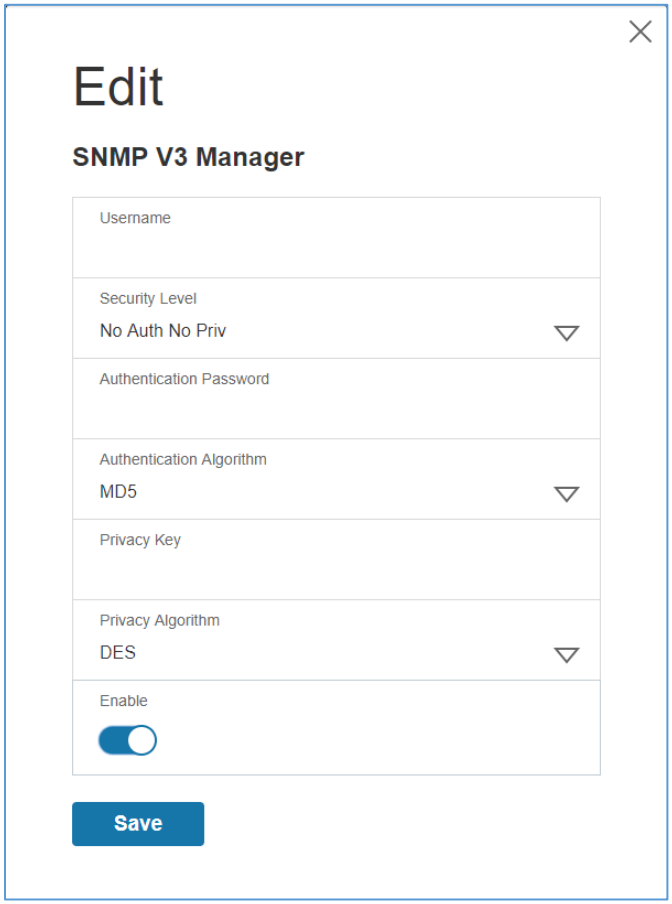


Figure 50: SNMP V3 Edit

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 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.

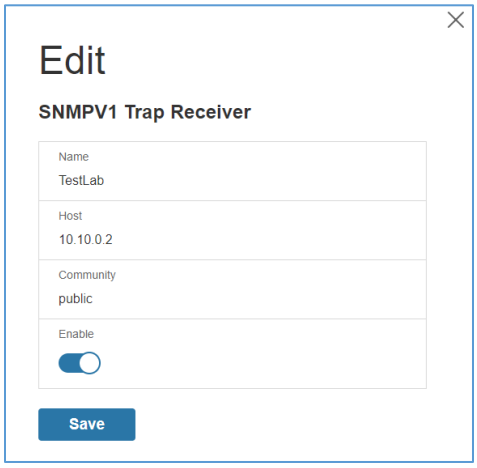


Figure 51: SNMPv2 Configuration Information

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.

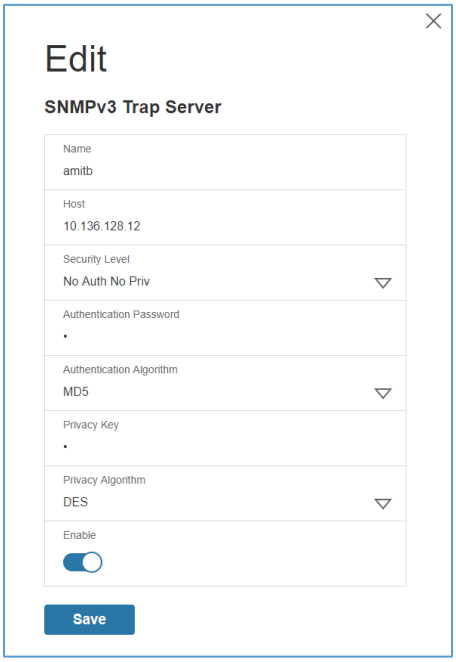


Figure 52: SNMPv3 Trap Server Information.

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 – Local Display

Onboard Display and Network Controller

The Onboard Display provides information about the PDU and connected devices. The PDU has a three-button, graphical Network Controller panel (see Figure 22). Use the buttons to change the screen display and retrieve specific data.



Figure 53: Network Controller

The Network Controller Display has three modes:

1. **Menu mode** (Network Controller 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 Network Controller 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. **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.

Status LED

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

Network Controller Menu Structure

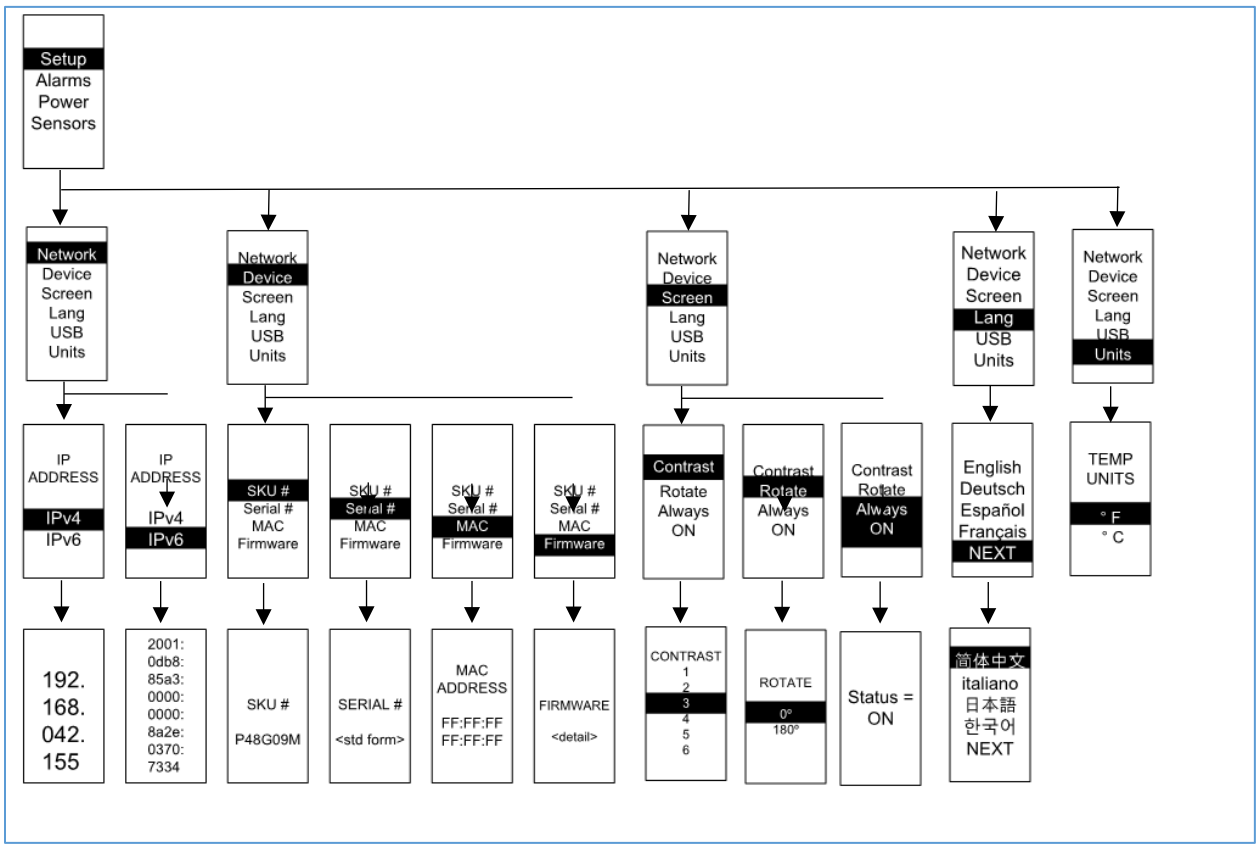


Figure 54: Network Controller Menu Structure

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.

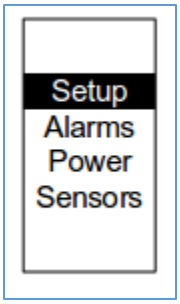


Figure 55: Main Menu Selections

Setup Menu

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

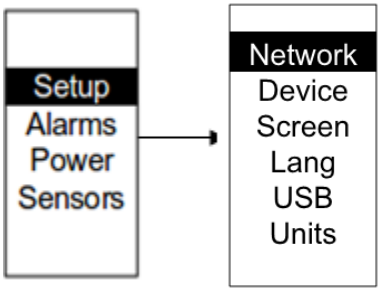


Figure 56: Setup Menu

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.

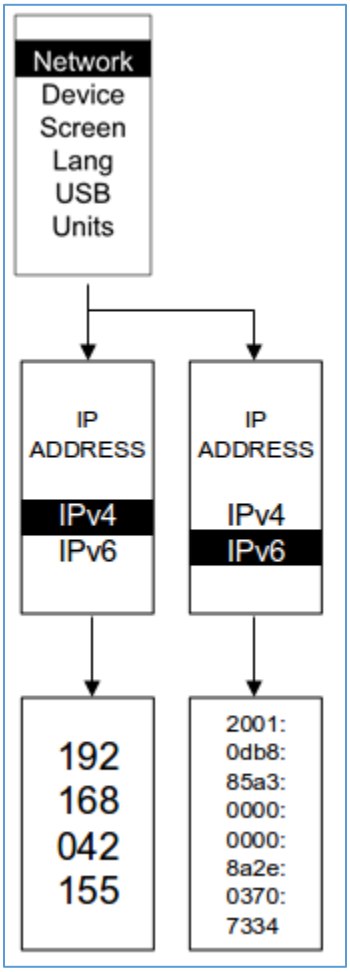


Figure 57: Network Submenu

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.

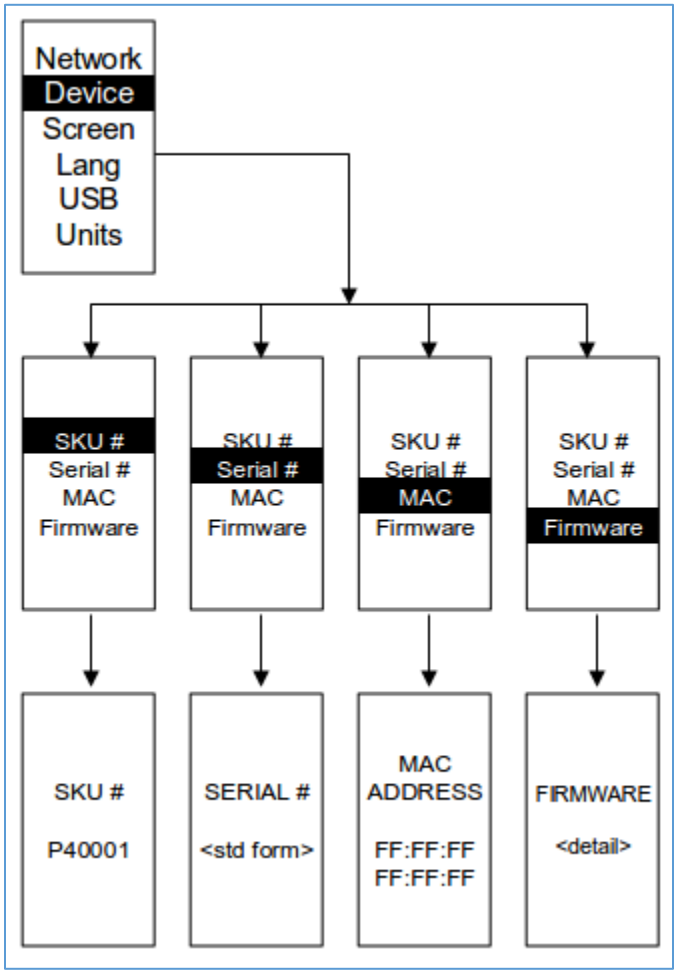


Figure 58: Device Submenu

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.

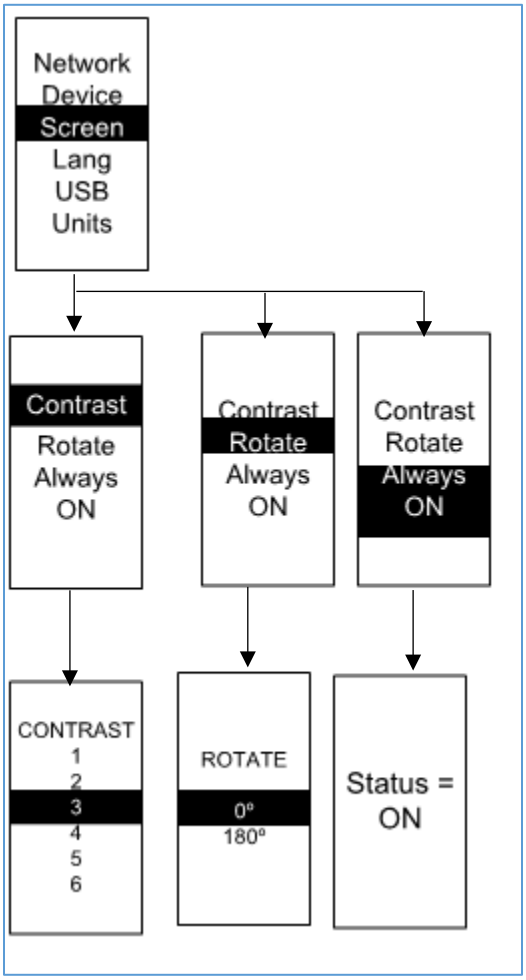


Figure 59: Screen Submenu

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 60: 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 reboot into the USB operation and Configuration Mode.

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

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 reboot and re-enter USB mode.

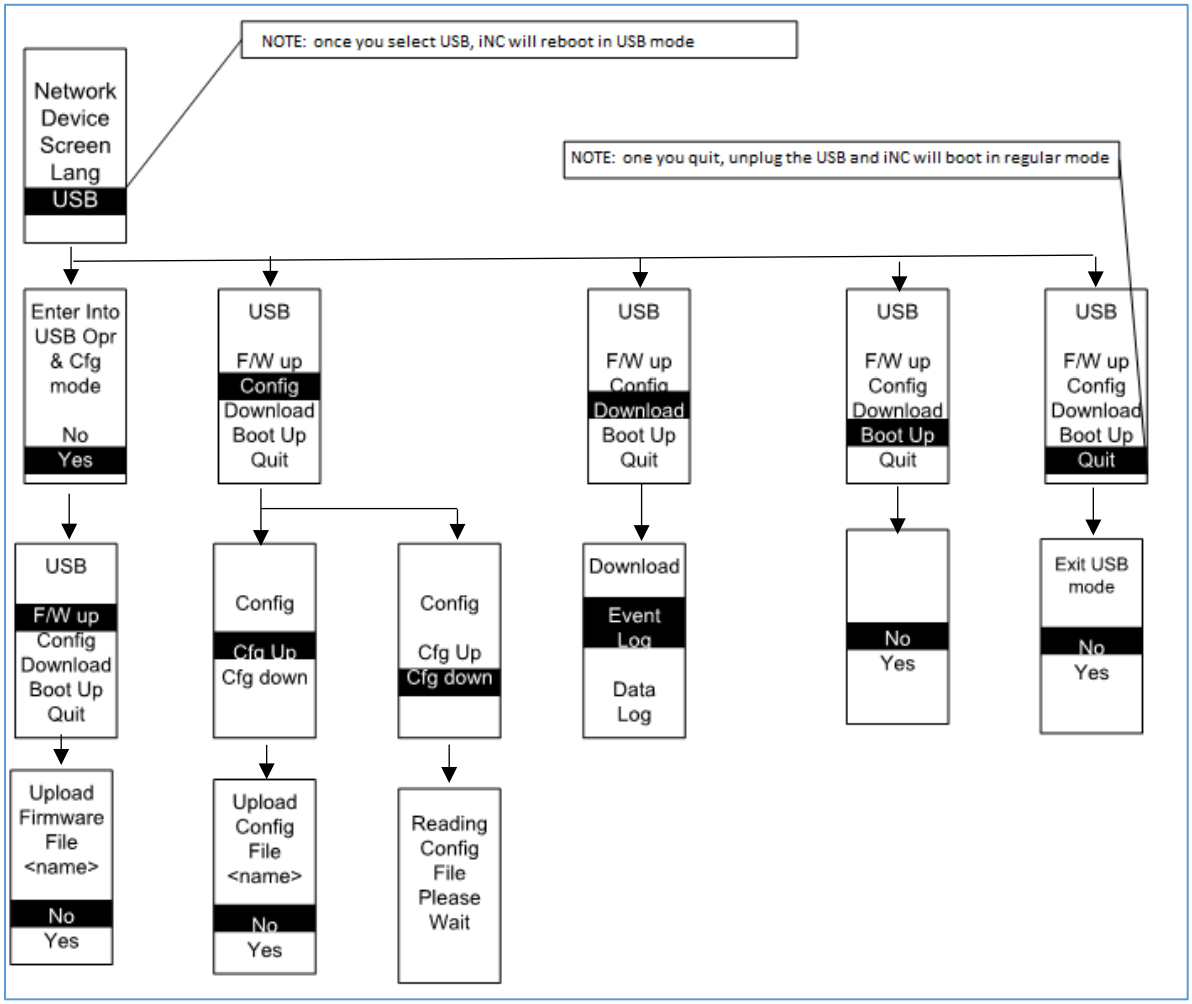


Figure 61: USB Submenu

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.

Note: This can only be done locally at the PDU.

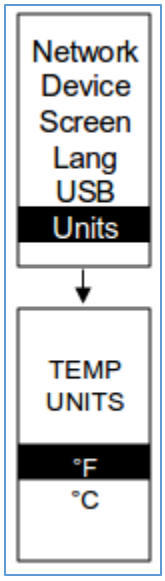


Figure 62: Units Submenu

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.

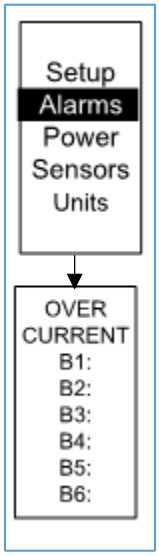


Figure 63: Alarms Menu

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.

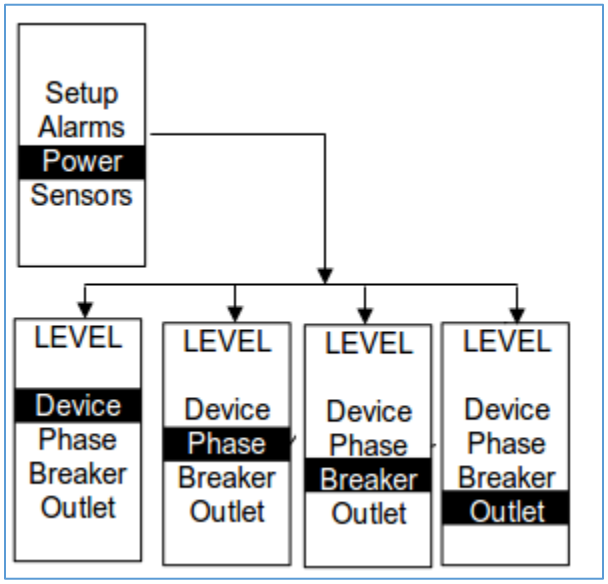


Figure 64: Power Menu

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.

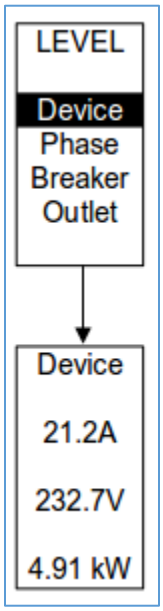


Figure 65: Device Submenu

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.

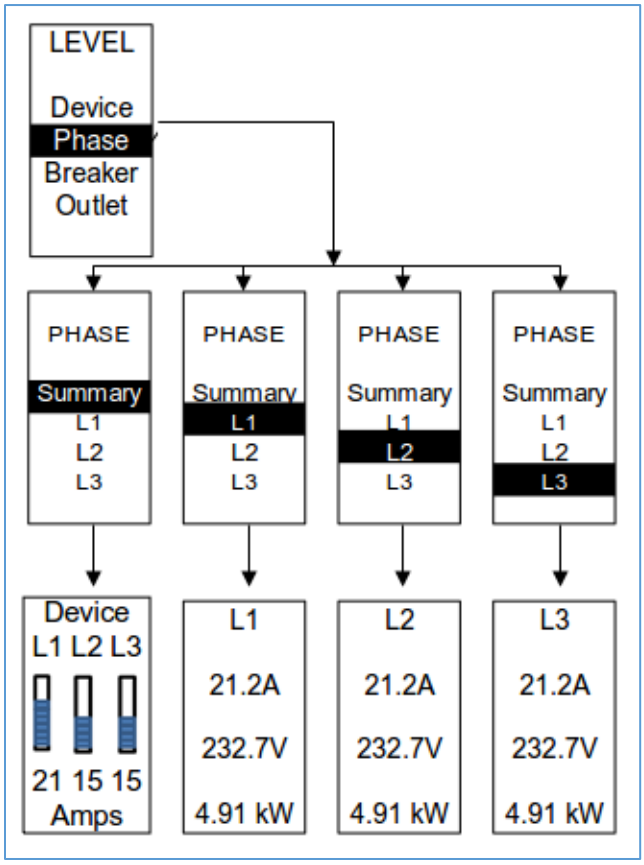


Figure 66: Phase Submenu

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.

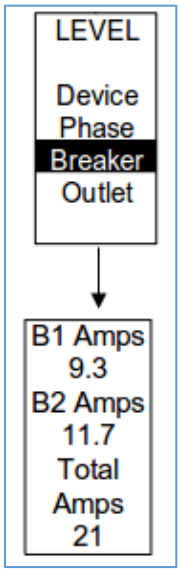


Figure 67: Breaker Submenu

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.

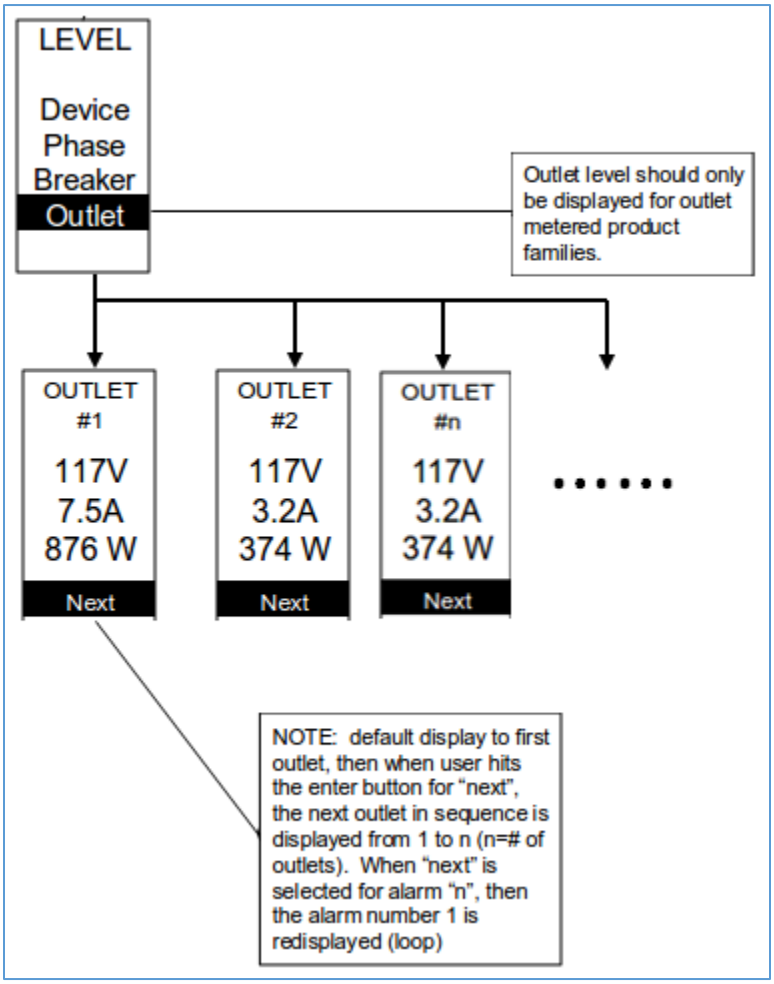


Figure 68: Outlet Submenu

Note: Custom outlet names noted in the Web GUI do not make changes to the local display. This is done to make it easier to map to outlet numbers which can locally be seen on the outlets themselves.

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.

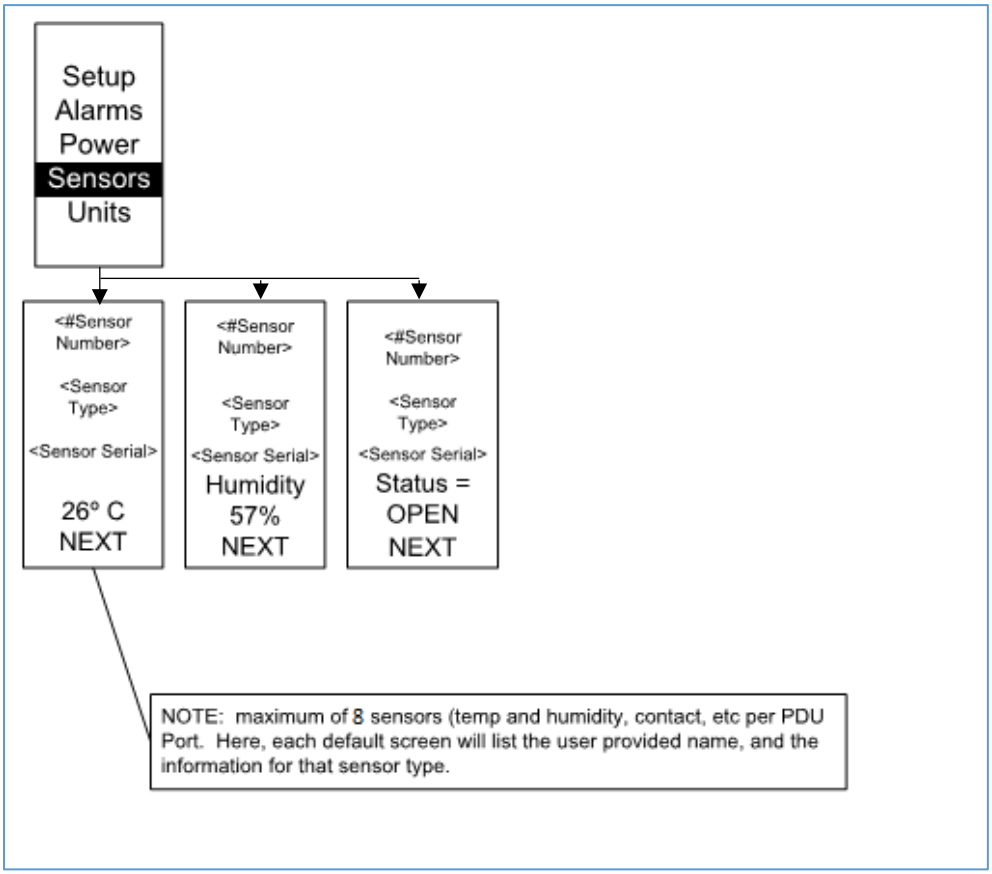


Figure 69: Sensors

NOTE: Maximum of 8 sensors are configured per PDU.

Section 5 – Daisy Chain Configuration

Daisy-Chain Overview

In daisy chain mode, up to (4) PDUs of the same SKU number, and on the same Firmware version, can be connected via one IP address. This allows users to gather information and data on all daisy-chained PDUs from the main 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 a 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.

Note: When replacing a Daisy Chained PDU or Accessory, please 'RESTART' the Primary (main) PDU1 controller to re-synchronize the daisy chained PDUs sequence. This action will not disrupt operations (or outlet states) and can be completed remotely via Web GUI, SNMP or CLI or physically by pressing and holding the reset button on the primary controller for 10 seconds (but not more than 15 seconds).

Daisy-Chain Setup

1. After the initial PDU is configured (parent), 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. A maximum of (2) PDU can be used in the RNA convention. See the below figure for a connection diagram when deploying RNA.

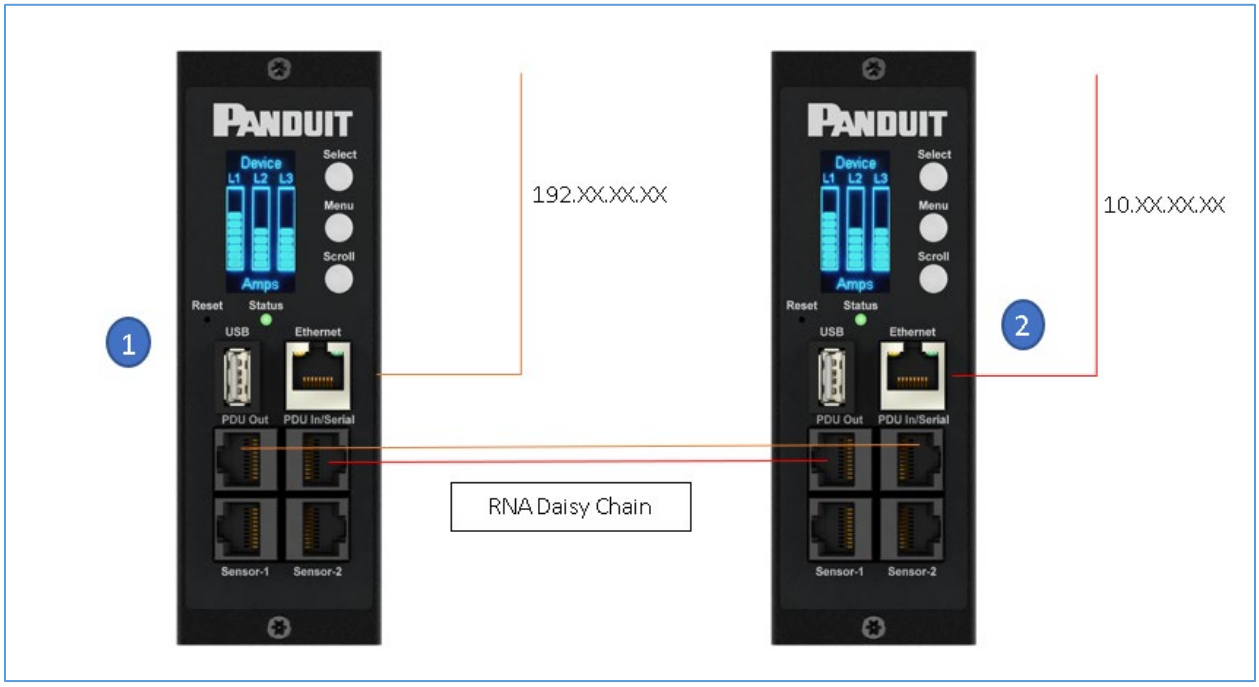


Figure 70: Connection Diagram RNA Daisy Chain

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 (see Figure 69)

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.

Power Share

Power Share is designed to allow for continual sensor monitoring and electronic rack access if one of the 2 power feeds is lost. This feature is available for vertical (0U) PDUs only. However, due to limited available power from the Panduit iPDU Controller, power share was designed and tested under the following conditions:

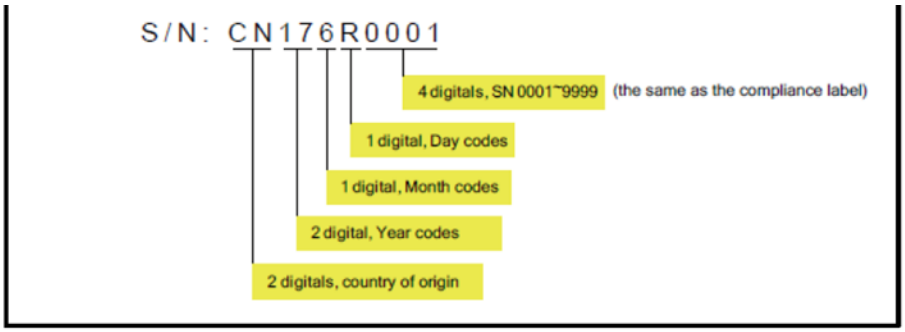
ACF05 or AC06 Electronic Security Handle, ACF10 (T+D), ACF11 (3T+D).

Care must be taken to not overload the system with accessories as this may cause instability or power share to become unavailable. Additionally, power share is only supported by Firmware version 3.x or higher on PDUs with a serial number:

COO: China S/N: > (greater than) CN213N6480
PDU's manufactured in China after March 22nd, 2021

COO: India S/N: > (greater than) IN21536039
PDU's manufactured in India after May 3rd, 2021

For complete details on the Serial number please use the Following Guide:



1st Character Year Codes

Year	2006	2007	2008	2009	2010	2011	2012	So on
Code	06	07	08	09	10	11	12	

2nd Character Month codes

Month	January	February	March	April	May	June	July	August	September	October	November	December
Code	1	2	3	4	5	6	7	8	9	A	B	C

3rd Character Day Code

Day	1st	2nd	3rd	4th	5th	6th	7th	8th	9th	10th	11th	12th	13th	14th	15th	16th
Code	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	G

Day	17th	18th	19th	20th	21st	22nd	23rd	24th	25th	26th	27th	28th	29th	30th	31st
Code	H	J	K	L	M	N	P	Q	R	S	T	U	V	W	X

The iPDU controller has a maximum output power capacity of 800mA @ 5V = 4 watts. Based on this, DO NOT deploy the Automatic Light Bar (PN: ACD01) when deploying solutions leveraging Power Share.

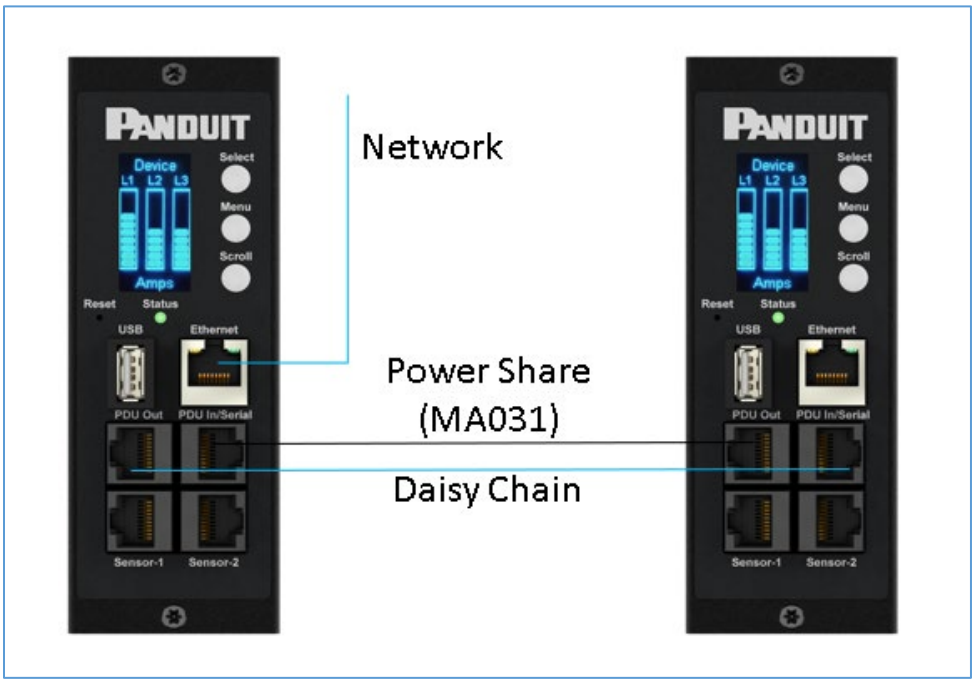
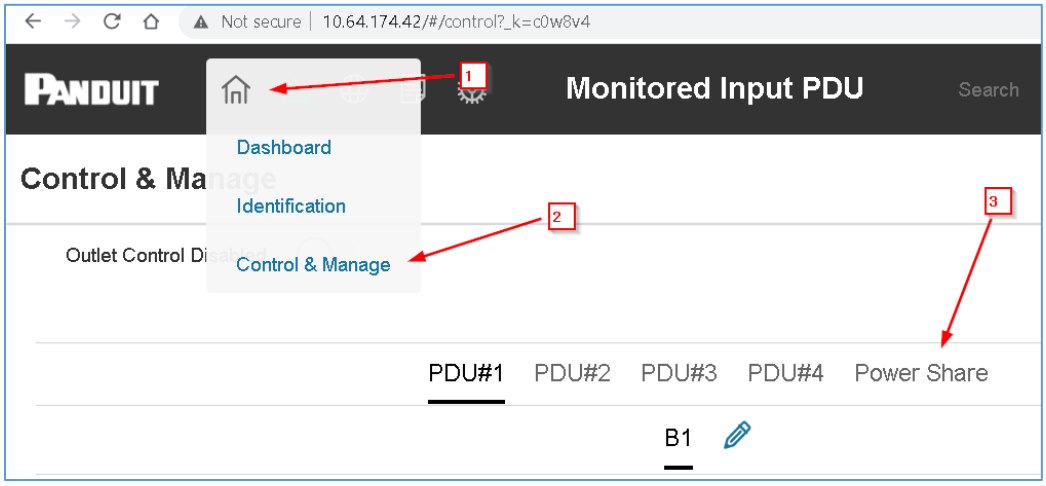


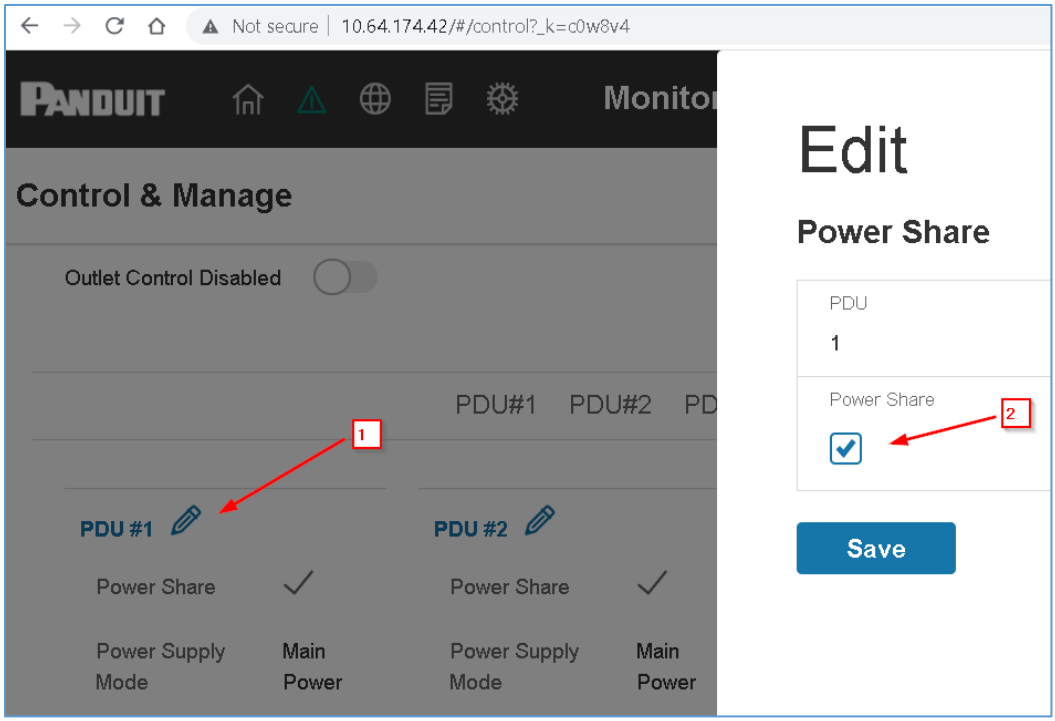
Figure 71: Connection Diagram Power Share & Daisy Chain

To confirm that your controller has Power Share from the Web GUI

Home → Control & Manage → Power Share



Enable power share under the edit menu.



Section 6 – Electronic Security Handle

The Panduit Intelligent PDUs allow users to electronically secure and control access to cabinets. G5 PDU Firmware v3.3.1 (or higher is required). For the latest firmware please visit: panduit.com → Support → Download Center → PDUs

Note: For security, verify that the handle is seated prior to engaging locking mechanism. If handle locks prior to handle being properly seated, unlock handle, seat properly, then lock again. Only users with admin privileges are allowed to make configuration level changes to the PDU (including Rack Access Security).



Figure 72: Electronic Security Handles

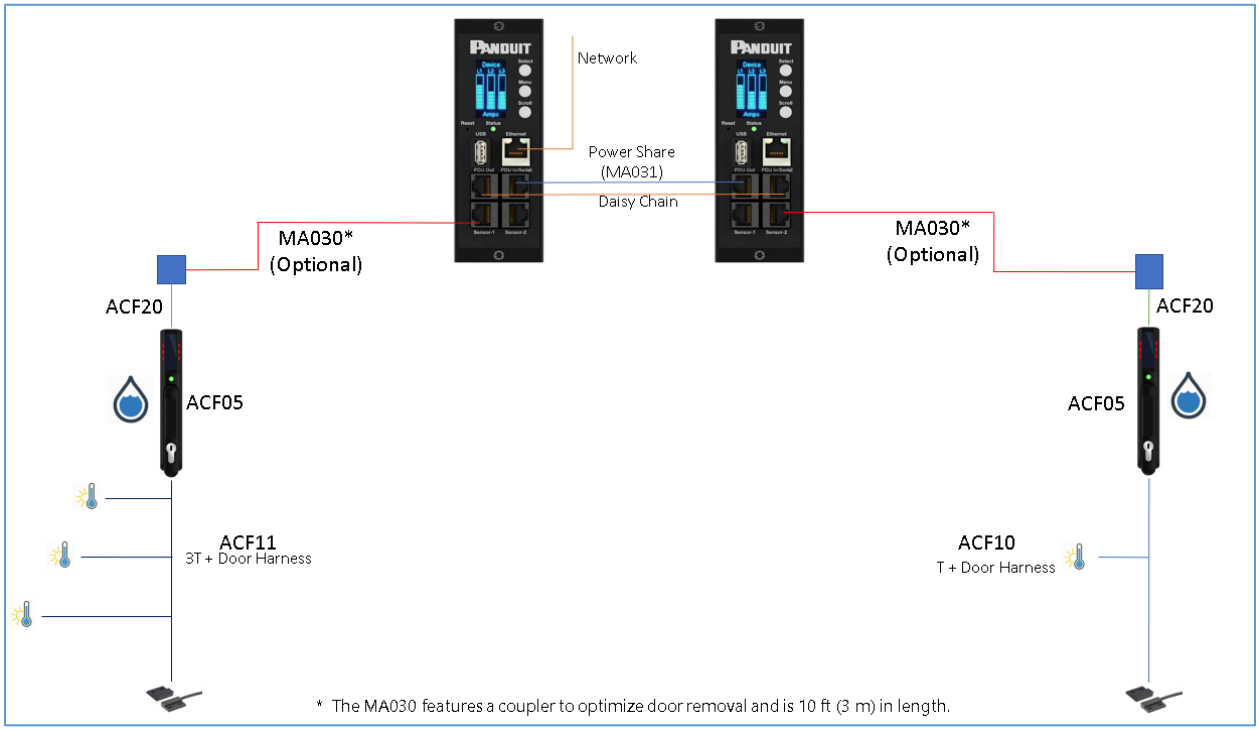


Figure 73: Connection Diagram for Electronic Security Handle

Note: Specialized sensors were developed for attaching directly to the Electronic Security Handle optimizing cable routing.

Use the below table to help count total sensors being deployed.

Part Number	*Number onboard Sensors*	*Device connects to*
ACF05	*2*	*Panduit G5 PDU*
ACF06	*2*	*Panduit G5 PDU*
ACF11	*4*	*Panduit G5 Handle*
ACF10	*2*	*Panduit G5 Handle*
ED001	*1*	*Panduit G5 PDU*
EE001	*1*	*Panduit G5 PDU*

ACA01	*1*	*Panduit G5 PDU*
ACC01	*1*	*Panduit G5 PDU*
EA001	*1*	*Panduit G5 PDU*
EB001	*2*	*Panduit G5 PDU*
EC001	*4*	*Panduit G5 PDU*

Note: A maximum of 8 sensors can be managed by the Panduit G5 PDU controller. A maximum of 2 handles can be managed by each individual Panduit G5 iPDU.

Configuring Cabinet 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, perform the following steps.

Note: The Hot Aisle or Cold Aisle is selected directly on the electronic handle through a DIP Switch. This is not a configuration item in the Web Interface.

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

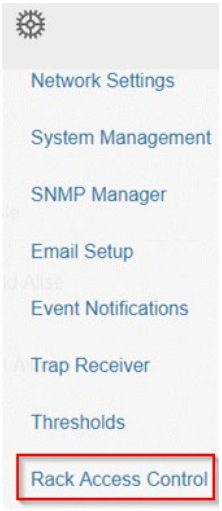


Figure 74: Rack Access Control Web GUI

3. The Actions Menu on the right side of the page will allow the user to Add Card, Rack Access Settings, Handle Settings, Keypad Settings, Remote Control, Beacon Settings, and Status LED Settings.

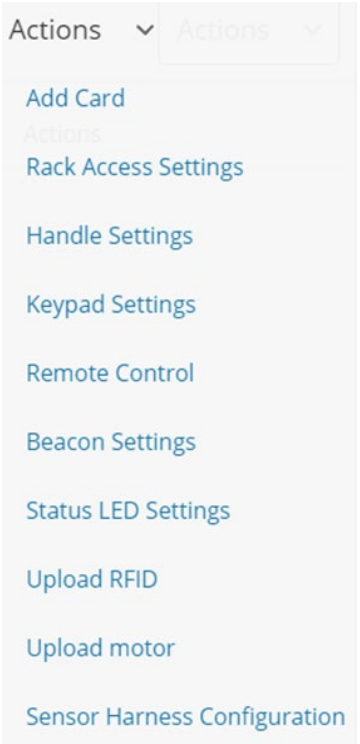


Figure 75: Rack Access Control Actions Web GUI

Adding a User for Local Rack Access

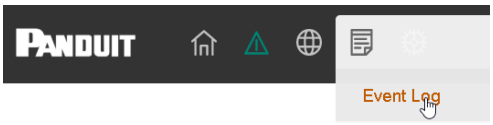
Every user that needs access to the cabinet needs to have their access card added into the PDU. Each card (or user) must have a username and either a card ID or keypad PIN code.

> **Note**: A maximum of 200 cards can be programmed per cabinet. When a user is added to 1 side of the cabinet, the system automatically allows them access to the other side (if applicable).

Determining Card ID

To determine the card ID, follow these steps:

1. Place the card near the reader (top of the handle).
2. Go to the event logs on the PDU →



3. Look for the most recent message about an unauthorized card swipe.

   Example:

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

4. The number in the message is the card ID.

Adding a Local access user

1. To add a new card (or user), select **Add Card** from the **Actions** menu.

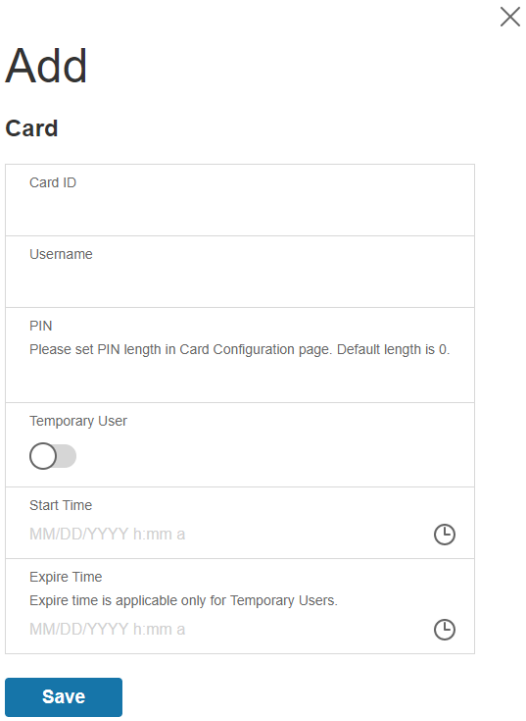


Figure 76: Local Rack Access Web GUI

2. Enter a username to identify the user.
3. If the system is configured for RFID Only or Dual Auth, enter the determined card ID.

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

4. If the system is configured for Keypad Only or Dual Auth, enter the pin.

   Note: users must be assigned unique PIN codes in 'Keypad Only' mode.

5. If you want to have the card access expire:
   a. Select Temporary User
   b. Add a Start and Expire time
6. Click **Save**.

Configuring Rack Access Settings.

The Rack Access Setting are common to the entire system. These include Aisle Control, AutoLock Time, Door Open Time, and Max Door Open Time.

2. To update the rack access settings, select **Rack Access Settings** from the Actions menu.

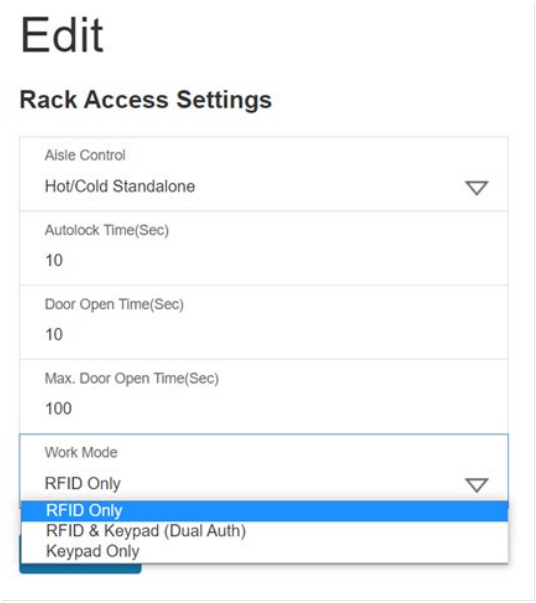


Figure 77: Rack Access Settings Web GUI

3. Select from two options in the **Aisle Control.**
    a. **Hot/Cold Combined –** Operating hot or cold causes both handles to open.
    b. **Hot/Cold Standalone –** Operates hot or cold independently
4. The **AutoLock Time** is the number of seconds after the handle will automatically lock.
5. The **Door Open Time** is the number of seconds after the handle alerts door open
6. The **Max. Door Open Time** is the number of seconds before a critical alarm announces, door opens.
7. **Work Mode** will tell the type of handle connected. For example, RFID only means the handle has a card reader and no keypad.
    a. Card (RFID) Only: Gain access to cabinet through swiping an authorized card.

    b. Keypad Only: Gain access to the cabinet through depressing an authorized secret pin into the keypad:

c. Dual Authentication (Card (RFID) + Keypad): First swipe an authorized card then within 5 seconds enter an authorized secret PIN into the keypad.

Configuring Handle Settings.

Handle settings and information relate to a specific handle. These include the Access Control Unit (ACU) name.

1. To update the handle settings, select **Handle Settings** from the **Actions** menu.

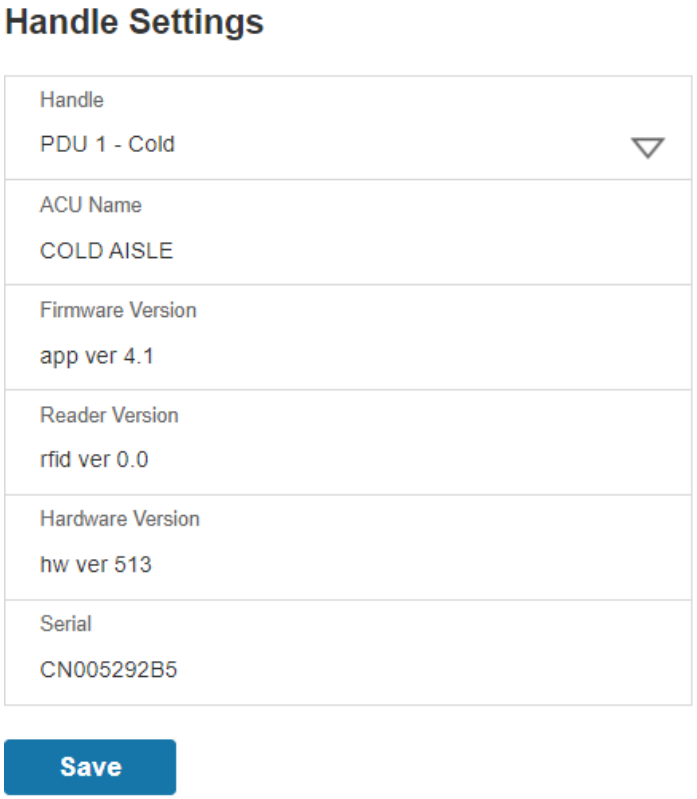


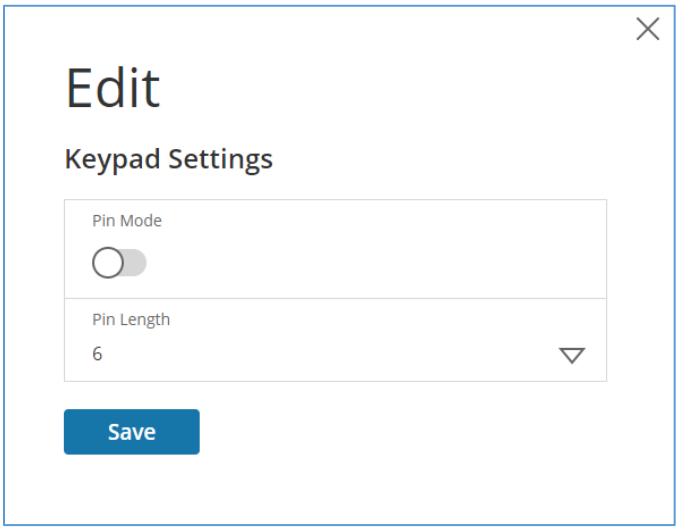
Figure 78: Handle Settings Web GUI

2. Select the handle to edit or get information about.
   a. Select the handle you are interested in, Under the PDU section.
3. Enter in the **ACU Name**. The ACU name is a name to help distinguish the different handles. This field is alphanumeric and accepts special characters.
4. The **Firmware Version, Hardware Version** and **Serial** are read-only attributes about the handle.

a. **Firmware Version** is the firmware version running on the handle.
b. **Hardware Version** is the version of hardware of the handle.
c. **Serial** is the serial number of the handle.

Configuring Keypad Settings

If a Electronic Security handle with Keypad is deployed; the user has the following options:



a. PIN Mode turned on hides the user PIN in the Web GUI.
b. All users must adhere to the same PIN length.
c. Users must select unique PIN codes in ‘Keypad Only’ mode.

Remote Controlling the Handle.

The remote control will allow you to remotely open and close a handle.

1. To remotely control a handle, select **Remote Control** from the Actions menu.

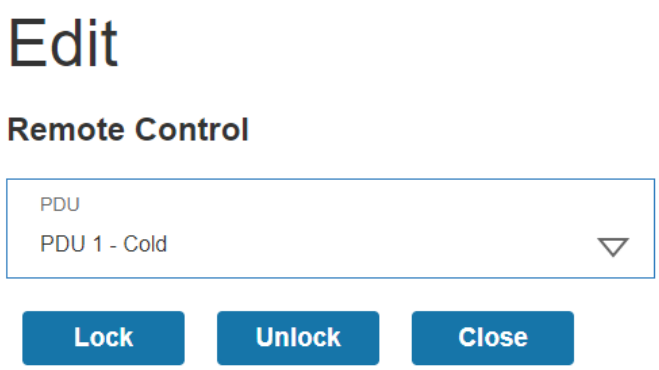


Figure 79: Remote Control

2. Select the handle to control:
    a. Under the PDU section, Select the handle
3. Select the action you wish to perform.
    a. **Lock** remotely locks the handle
    b. **Unlock** remotely unlocks the handle.
4. When finished, click **Close**.

Controlling the Beacon.

The beacon is a visual indicator to give you status of the cabinet at a glance. The beacon will flash yellow when the cabinet is in a minor alarm or flash red when the cabinet has a critical alarm. You can also use the beacon's locate function to flash the beacon a certain color to easily locate the cabinet. The default state of the beacon LED is on solid green.



Figure 80: Beacon

Beacon LED Table:

Function	State	Color	Purpose
Locate	Blinking	Blue, Green, Yellow, Red, White, Magenta	Identifies rack location. (customizable)
Critical Alarm	Blinking	Red	Any critical alarm in the system. (not customizable)
Warning Alarm	Blinking	Yellow	Any warning alarm in the system (not customizable)
Normal State	Solid	Blue, Green, Yellow, Red, White, Magenta	Visual indicator on the handle. (customizable)

1. To control a handle beacon, select **Beacon Settings Control** from the **Actions** menu.

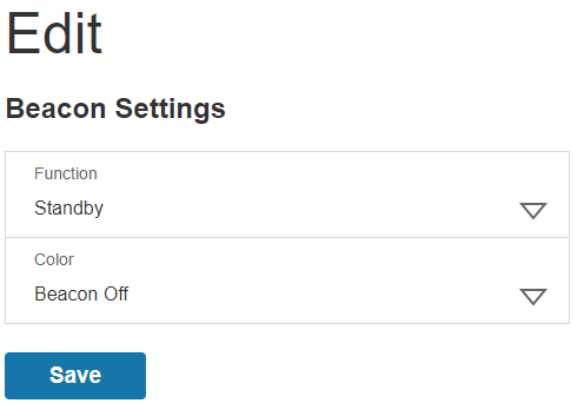
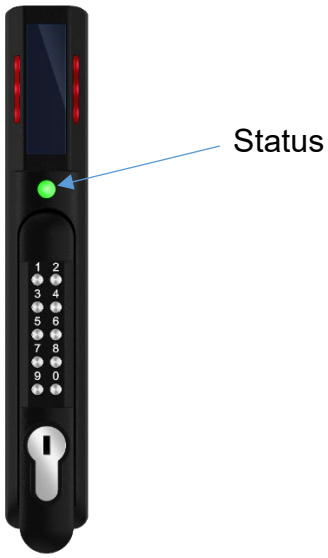


Figure 81: Beacon Settings Web GUI

2. Select the function of the beacon:
    a. **Standby –**beacon color no alarms
    b. **Locate** –flash beacon
3. Select color for **Standby** or **Locate**.
4. Select **Save**.

The Status LED

The Electronic Security Handle is equipped with a status LED to give a visual indication of the handle and security status. A summary of all the status LED states can be seen in the follow table. The default state of the status LED is on solid green.



Status LED Table in Order of Priority:

Status LED Color	Description
Standby – Solid (or off)	Customer selectable color in standby state. (customizable)
Red - Blinking	Blinks three times signaling authentication error (not customizable)
Green - Blinking	Lock Open (not customizable)
Magenta – Blinking	Key used to unlock or Mechanical handle lifted away from base (not customizable)
Yellow – Blinking	Handle open past Door Open Time (not customizable)
Red - Solid	Lock open for longer than Autolock Time. (look for obstruction) (not customizable)
Red - Solid	Door open for longer than Door Open Time (door sensor) (not customizable)

Setting Status LED State

1. To set the standby state of the status LED state, select **Status LED Settings** from the **Actions** menu.

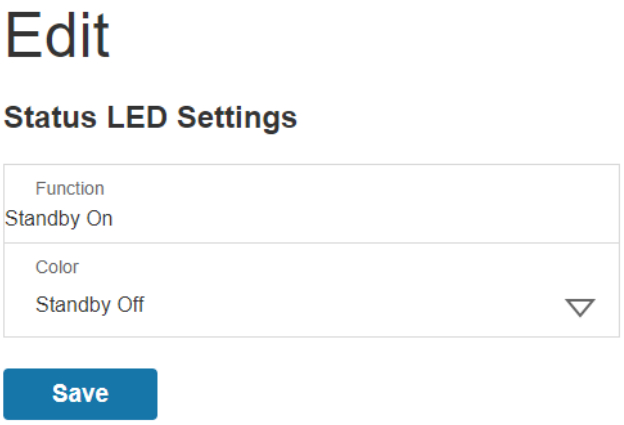


Figure 82: Status LED Settings Web GUI

2. Select the color of Status LED when the handle is in standby state.
3. Select **Save.**

Handle and Compatible Card Types

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

	MIFARE® Classic 1k	*MIFARE Plus® 2k*	*MIFARE® DESFire® 4k*	*HID® iCLASS*	*HID® 125kHz Prox*	*EM 125kHz Prox*	*Output*
ACF05 *ACF06*	*UID*	*UID*	*UID*	-	*CSN*	*CSN*	*Wiegand*

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

Section 7 – Panduit G5 Accessories

Hardware Overview

The Panduit G5 accessories are specially designed to interoperate Panduit G5 iPDU controller. Connecting unapproved sensors to the G5 iPDU controller or connecting Panduit G5 Sensors to 3rd party controllers may result in damage.

Monitoring critical attributes (such as temperature, humidity, leak detection, and intrusion) are all vital aspects of maintaining an efficient-working data center or IT room atmosphere.

Note: A maximum of 8 sensors can be managed by the Panduit G5 PDU controller. Sensors may be installed with PDUs powered on.

The following table lists available sensors as well as sensor count:

Sensor	Description	Sensor Count
Temperature Sensor (EA001)	Monitors the temperature in the rack.	1
Temperature + Humidity Sensor (EB001)	Monitors the temperature and relative humidity in the rack.	2
Three Temperature + Humidity Sensor (EC001)	Monitors the temperature in three areas using three separate probes and the relative humidity using one probe.	4
Door Sensor (ACA01)	Monitors intrusion when a door on which the sensor is installed has been opened greater than 10 mm.	1
Water - Rope Sensor (ED001)	Monitors leak detection of liquid with a resistivity of less than 2 megaohms (including distilled water).	1
Water – Spot Sensor (EE001)	Monitors leak detection of liquid with a resistivity of less than 2 megaohms (including distilled water) in the monitored area.	1

Sensor	Description	Sensor Count
Sensor Port Hub (EF001)	Passive hub allowing for three additional sensors to be connected.	N/A
Leak Detection Sensor Extension (EG001)	Extends the Rope type leak detector by an additional 6m. A total of four extensions can be added to the leak detection sensor for a total length of 30m.	N/A
Panduit G5 Dry Contact Sensor (ACC01)	Input to the G5 iPDU and designed to monitor a change in contact state.	1

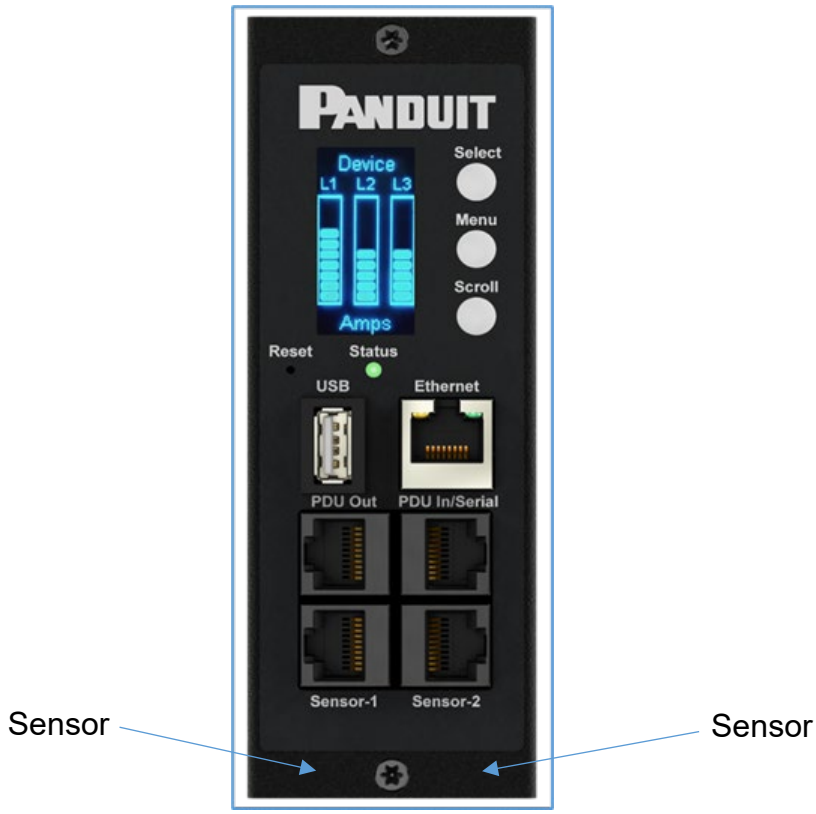


Figure 83: Sensor Ports for Vertical PDU



Figure 84: Sensor Ports for Horizontal PDU

Configuring Temperature Scale

To configure the temperature scale (Celsius or Fahrenheit) of the temperature sensors:

1. Go to User Accounts.

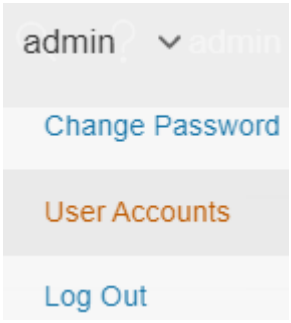
d. 

Figure 85: User Settings

2. The button at the top of the screen can be used to select Celsius or Fahrenheit.

e. 

Figure 86: Celsius Setting

f. 

Figure 87: Fahrenheit Setting

Configuring Environmental Sensors

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

3. Open the **Settings**.
4. View the Threshold section on the Settings page. Select **Threshold** to configure sensors.
5. Go to External Sensors.
6. Select **Edit** button to configure the desired sensors.
7. In the **Edit** dialog box, type value of up critical, up warning, low warning, and low critical.

   Select **Save** to exit the sensor setup.

Security

This product contains software that stores user entered data. All data entered by the user is stored in non-volatile storage on the system running the software.

Non-volatile Storage

- The G5 iNC Controller uses non-volatile storage on the G5 PDU to store all configuration information.

Authentication Data

- Usernames are stored in non-volatile memory and are available to ‘administrator’ role users, for the purpose of managing access to the system.
- Passwords used for managing the software are stored in non-volatile storage.
- SNMP v1/v2c community strings are stored in non-volatile storage.
- SNMP v3 usernames and passwords are stored in non-volatile storage.

Network Transport Security

- The product comes with a default SSH RSA 1024-bit private host key.
- The product comes with a default RSA 2048-bit private key and certificate.
- The user may upload a custom HTTPS certificate and private key.
    - The HTTPS certificate should use a SHA-256 signature.
    - The private key should be RSA 2048-bit.
    - Other private key types may work, but performance may be negatively impacted if greater private key sizes are used: RSA 3072-bit, RSA 4096-bit.
- The product uses TLS 1.2 to communicate with HTTPS web browser clients.
- The product provides a SSH server with these algorithms to communicate with SSH clients:
    - Key exchange algorithms: diffie-hellman-group14-sha1
    - Host key algorithms: ssh-rsa
    - Encryption algorithms: aes256-ctr
    - MAC algorithms: hmac-sha1

Network Configuration Data

- Network Configuration, including Static IP addresses and addresses obtained by DHCP are exposed on an “Identification” page and on a Network Configuration page, to aid in network management of the product.

- The product implements an internal authentication mechanism, authorization events generate “Event Logs” containing the IP address and username of successful logins, and the IP address of failed logins for valid usernames.

External Authorization Mechanisms

- LDAP & Radius – username & password are stored in non-volatile storage.
- LDAP is not encrypted over the network.
- The remote LDAP server authenticity (fingerprint) is not validated.
- The Radius protocol is designed to only transmit hashed and obfuscated passwords over the network.

Other Features

- The product includes a real-time clock and a capacitor that maintains time for a short amount of time when no power is applied. When combined with NTP, accurate timestamps on logs are provided.

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)

Panduit Support and Other Resources

Majority of your support needs can be met by visiting Panduit.com and navigating to the respective product page. If you require additional assistance; we are here to help.

Accessing Panduit Support

North America

Customer Service

- Price & Availability
- Expedites

800-777-3300 or cs@panduit.com

PDU Technical Support:

- PDU Selection
- Competitor Cross references
- Product Documentation

Email: TechSupport@panduit.com

Europe / Middle East

Customer Service

- Price & Availability
- Expedites

0044-(0)208-6017219 or EMEA-CustomerServices@panduit.com

PDU Technical Support:

- PDU Selection
- Competitor Cross references
- Product Documentation

Email: TechSupportEMEA@panduit.com

https://www.panduit.com/en/support/contact-us.html

Global PDU System Support:

- Firmware Updates
- Bulk Configuration

DCIM Software Support
Email: systemsupport@panduit.com
Phone: 1-866-721-5302

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

IP

Internet Protocol

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

Appendix A: 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.

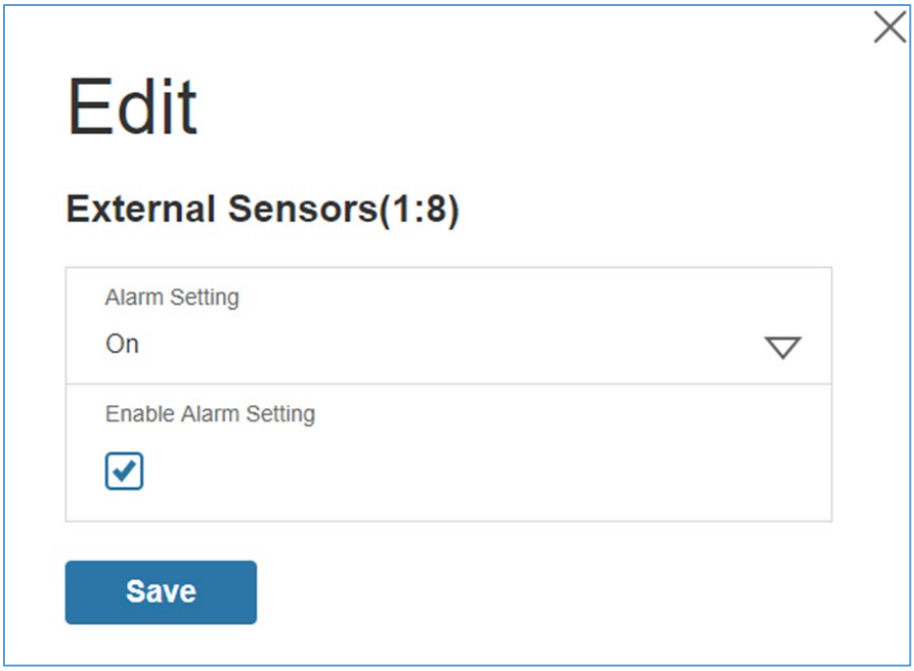


Figure 88: Door Switch Sensor Configuration

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

Dry Contact Input Sensor (side panel switch)

The dry contact sensor can be configured to alert when the when the contact is opened, alert when the contact is closed, or the alerts can be disabled.

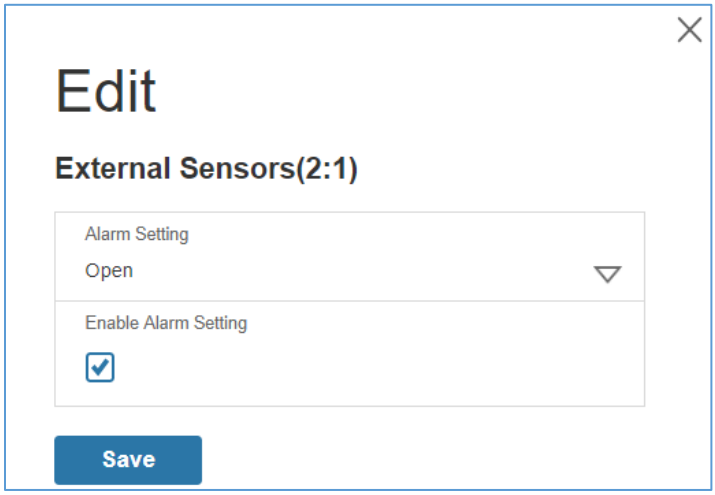


Figure 89: Dry Contact Cable

Note: The dry contact cable is only designed to connect to a Panduit PDU. 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 PDU. 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.

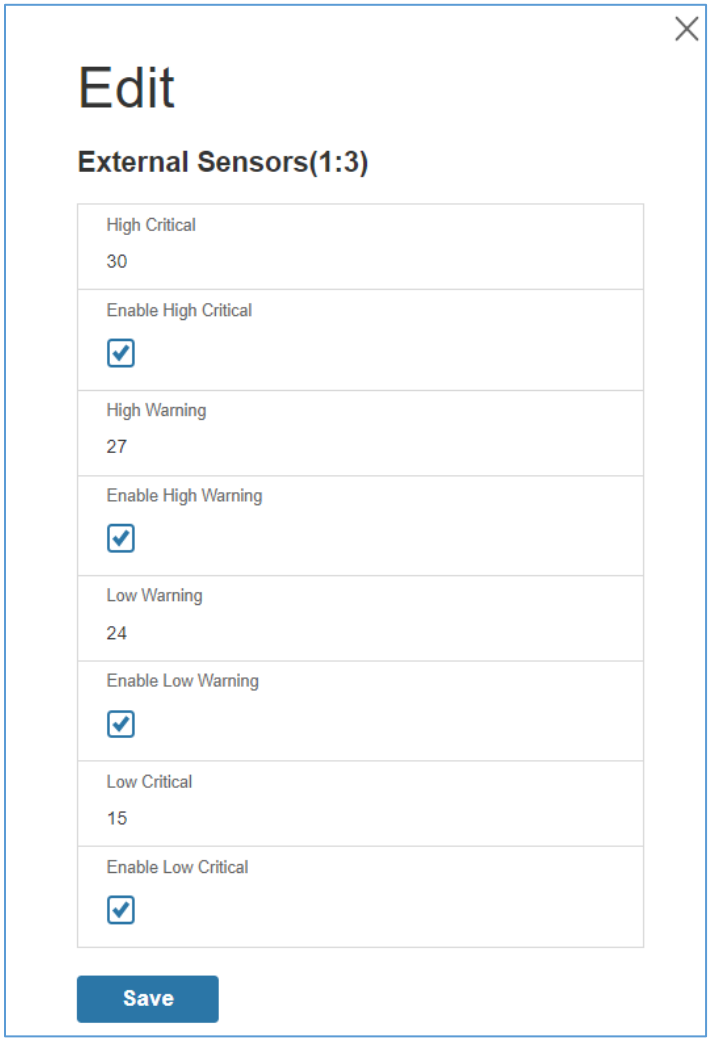


Figure 90: Temperature and Humidity Sensors

Configuring Environmental Sensors

Each Panduit G5 Intelligent PDU features an onboard controller capable of managing a maximum of 8 sensors.

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

8. Open the **Settings**.
9. View the Threshold section on the Settings page. Select **Threshold** to configure sensors.
10. Go to External Sensors.

11. Select **Edit** button to configure the desired sensors.
12. In the **Edit** dialog box, type value of up critical, up warning, low warning, and low critical.
13. Select **Save** to exit the sensor setup. Repeat this process for additional sensors.

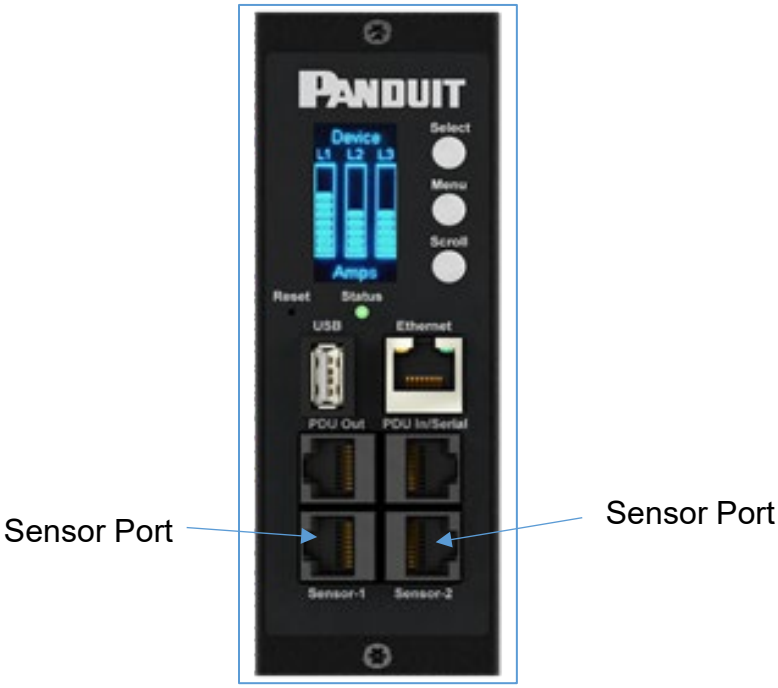


Figure 91: Sensor Ports on controller

Appendix B: Firmware Upgrade Options

It's important to remain up to date on your PDU firmware as bugs are resolved and performance improves with every release.

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. Updating the firmware does not affect the configuration or outlet state of the intelligent PDU.

Note: If you load incompatible firmware, no damage will occur and PDU will maintain the original firmware.

G5 Upgrade Tool (GUT)

The 'G5 Upgrade Tool' has been created to streamline the firmware upgrade process for either individual or bulk management of PDUs. See Appendix C for details.

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 Settings > System Management > Actions > Update Firmware.
4. In the Firmware Update dialog box, browse to (**Panduit.FW)** firmware file.

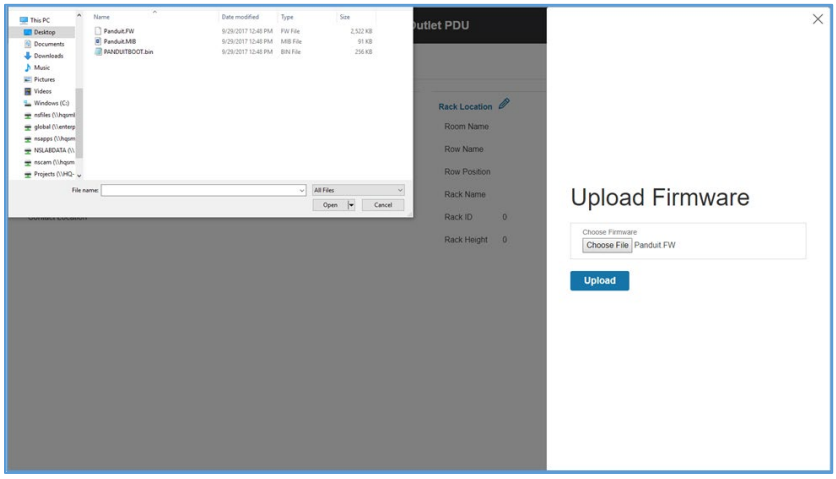


Figure 92: Upload Firmware

NOTE: the firmware file name must be retained AS IS.

5. Select Upload. The system will update the newest firmware to the Intelligent Network Controller.
6. When the upload is finished, the system will reboot automatically.

USB Method

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

1. Save the Firmware file ('*.FW') to a USB drive.
2. Insert the USB drive into the USB port of the 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**.

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 *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.

Appendix C: Bulk Management of PDUs

A dedicated G5 Upgrade Tool (GUT) is included with every firmware release. This utility enables a user to bulk manage PDUs. This utility features Firmware Upgrading, Configuration Replication (common parameters) and management of uncommon parameters (.csv) file. Requires Windows OS.

G5 Upgrade Tool (GUT)

1. Firmware Upgrade

    a. Insert IP address or IP address range in the Scan Network Tab

    b. Insert admin credentials

    c. Click 'Start Upgrade'

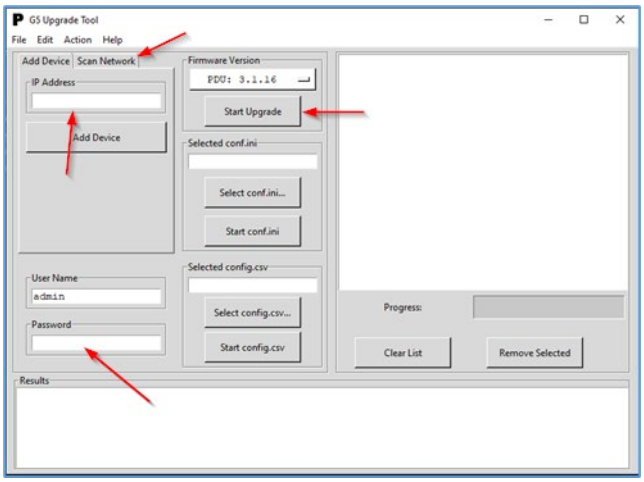


Figure 93: G5 Upgrade Tool Interface

Note: Simplify firmware upgrade from 2.x to 3.x using this utility down to a single click.

2. Configuration Replication of Common Parameters

    a. Pre-set the common parameters (e.g. thresholds, rack access control, etc..) via the Web GUI and download configuration (conf.ini) from the System Management menu.

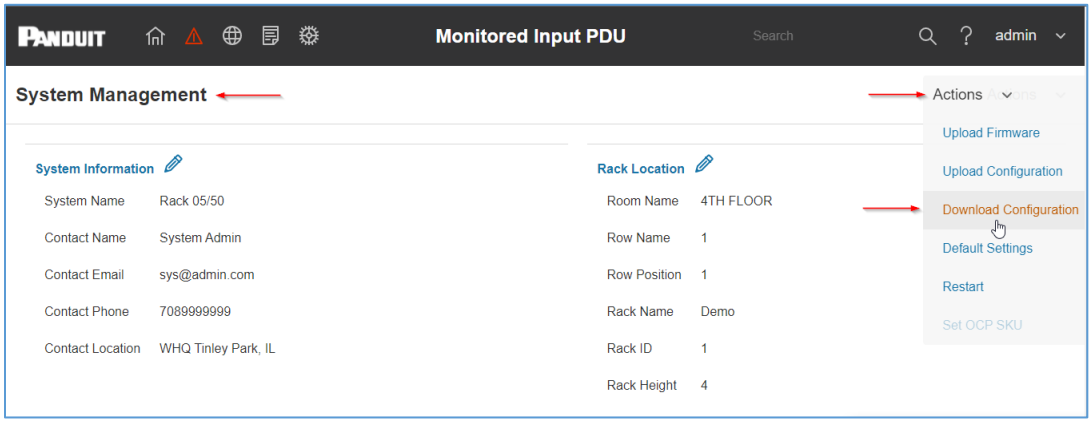


Figure 94: System Management Screen Web GUI

b. Insert IP Address or Range of the target PDU(s)

c. Insert admin credentials

d. Load the confi.ini file to the G5 Upgrade Utility and click Start Conf.ini

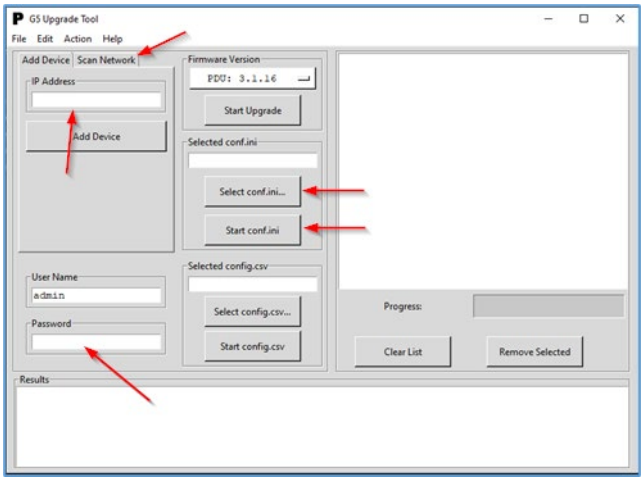


Figure 95: G5 Upgrade Tool Interface

3. Configuration Replication of Un-Common Parameters

   a. Insert IP Address or Range of the target PDU(s)

   b. Insert admin credentials

   c. Edit and Save the .csv file.

Panduit Detailed Monitoring Device Configuration					
1					
Cabinet Number				10.64.174.42	10.64.207.251
CABINET TYPE				Server Cab TypeA	Server Cab TypeA
Network	IP Configuration	Boot Mode	DHCP | Static		
Network	IP Configuration	IPv4 Address	string		
Network	IP Configuration	Network Mask	String		
Network	IP Configuration	Default Gateway	string		
Network	Web Access Configu	RESTapi Access	Checked - Yes | No	Checked - Yes	Checked - Yes
Network	NTP	Enable	Checked - Yes | No	Checked - Yes	Checked - Yes
Network	NTP	Primary Server	string	96.245.170.99	96.245.170.99
Network	NTP	Secondary Server	string	173.0.48.220	173.0.48.220
Network	NTP	Region	int	1202	1202
System Management	System Information	System Name	string50	PDU SZ Security Han	PDU Legacy Handle
System Management	System Information	Contact Name	string50	User 1	User 2
System Management	System Information	Contact Email	string50	user1@panduit.com	user1@panduit.com
System Management	System Information	Contact Phone	string50	7799999999	7089999999
System Management	System Information	Contact Location	string50	WHQ Tinley Park, IL	WHQ Tinley Park, IL
System Management	Rack Location	Room Name	string50	4TH FLOOR	4TH FLOOR
System Management	Rack Location	Row Name	string50	1	1
System Management	Rack Location	Row Position	string50	1	2
System Management	Rack Location	Rack Name	string50	Demo	Demo

Figure 96: Example CSV File

d. Load the Config.csv file to the G5 Upgrade Utility and click Start Config.csv

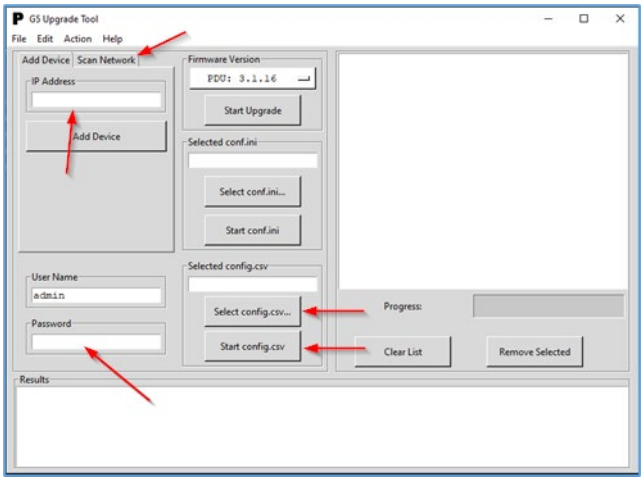


Figure 97: G5 Upgrade Tool Interface

Appendix D: System Reset or Password Recovery

Use Reset Button on Controller

Press and hold the Reset Button for 8 seconds to recover from an Intelligent Network Controller communication failure. This will cause a reset of the iNC controller, all configuration(s) will be retained.

To Default the controller to factory settings, press and hold the Reset Button for at least 20 seconds. This will cause a reset of the iNC controller erasing all existing configurations, including username(s) and password(s). It does not change the Energy (kWh) value and does not affect the outlet state.

Appendix E: PDU Alarms

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

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

User Administration	User Administration Password changed User Administration Password settings changed User Administration User added User Administration User deleted User Administration User modified
Smart Rack Access	Smart Rack Access Door Open Smart Rack Access Door Closed Smart Rack Access User Card Swiped 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.

Trap codes assigned enhanced security alarms:

Trap Class	Trap Code	Trap Description
Warning	1100	Door Open for longer than configured door time out
Critical	1101	Door Open for longer than configured max door open time
Informational	1102	Door unlocked with authorized pin code
	1103	Door accessed with unauthorized pin code.
	1104	Door locked because opposite aisle locked.
	1105	Door opened because opposite aisle unlocked.
	1106	Temporary user expired and was removed.
	1108	User added
	1109	User modified
	1110	User deleted.

Trap codes assigned for Phase Power alarms:

Trap Class	Trap Code	Trap Description
Critical	1121-1123	Input Phase Measurement Active Power of PHASE (1-3) asserted above upper critical
	1124-1126	Input Phase Measurement Active Power of PHASE (1-3) asserted below lower critical
	1127-1129	Input Phase Measurement Apparent Power of PHASE (1-3) asserted above upper critical
Warning	1130-1132	Input Phase Measurement Apparent Power of PHASE (1-3) asserted below lower critical

	1133-1135	Input Phase Measurement Active Power of PHASE (1-3) asserted above upper warning
	1136-1138	Input Phase Measurement Active Power of PHASE (1-3) asserted below lower warning
	1139-1141	Input Phase Measurement Apparent Power of PHASE (1-3) asserted above upper warning
	1142-1144	Input Phase Measurement Apparent Power of PHASE (1-3) asserted below lower warning
Cleared	1145-1147	Input Phase Measurement Active Power of PHASE (1-3) deasserted above upper critical/below lower critical/above upper warning/below lower warning
	1148-1150	Input Phase Measurement Apparent Power of PHASE (1-3) deasserted above upper critical/below lower critical/above upper warning/below lower warning
	1151	Role Added by Admin User
	1152	Role Deleted by Admin User
	1153	Role Modified by Admin User

Appendix F: Panduit Network Controller Replace or Rotate 180°

1. Use a T10 Torx screwdriver on the screws as shown in Figure 98. The screws are held in with retaining washers.

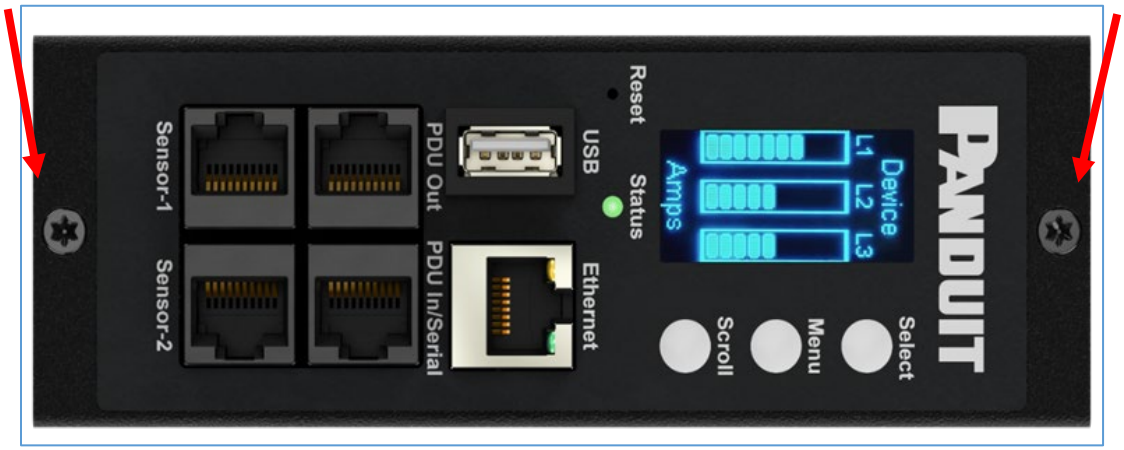


Figure 98: Screws on Network Controller

   a. Controller may be rotated to accommodate overhead or underfloor power. If rotating controller, **YOU MUST DISCONNECT** the ribbon cable to prevent damage to the ribbon cable. After rotating the controller, carefully reconnect the ribbon cable making sure to not pinch any of the ribbon cable.

2. If replacing controller, disconnect the existing ribbon cable from the existing controller. To reinstall, carefully connect the ribbon cable to the new controller making sure to not pinch any of the ribbon cable.

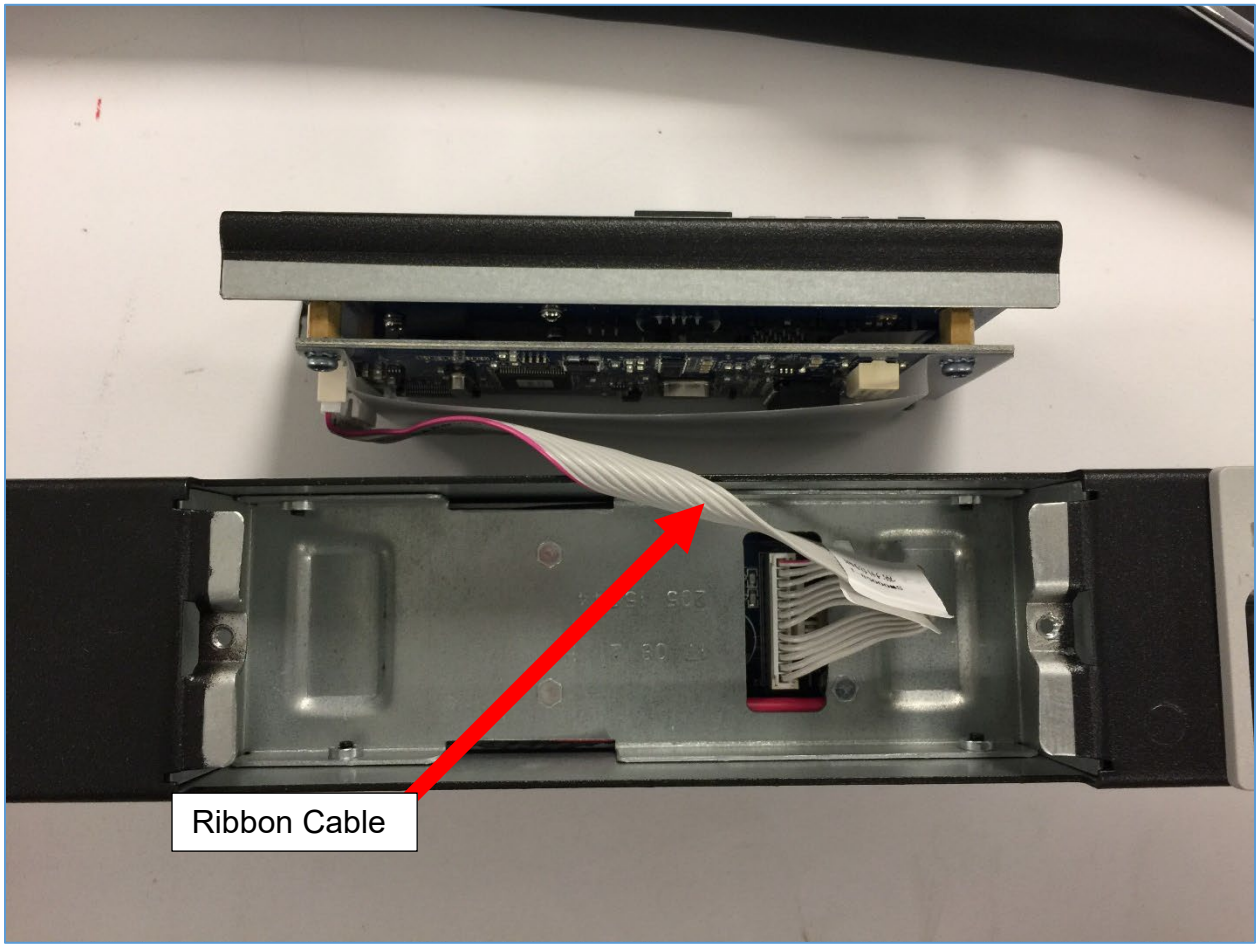


Figure 99: Ribbon Cable for the Network Controller

3. Replace and tighten the two (T10) screws on the Intelligent Network Controller to 2.2 – 3.1 lbf-in (0.25 – 0.35 N-M). Overtightening the screws may result in metal deformation.

Appendix G: Direct connect to the PDU by 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. Type **control** into Windows Search and select **Control Panel**.

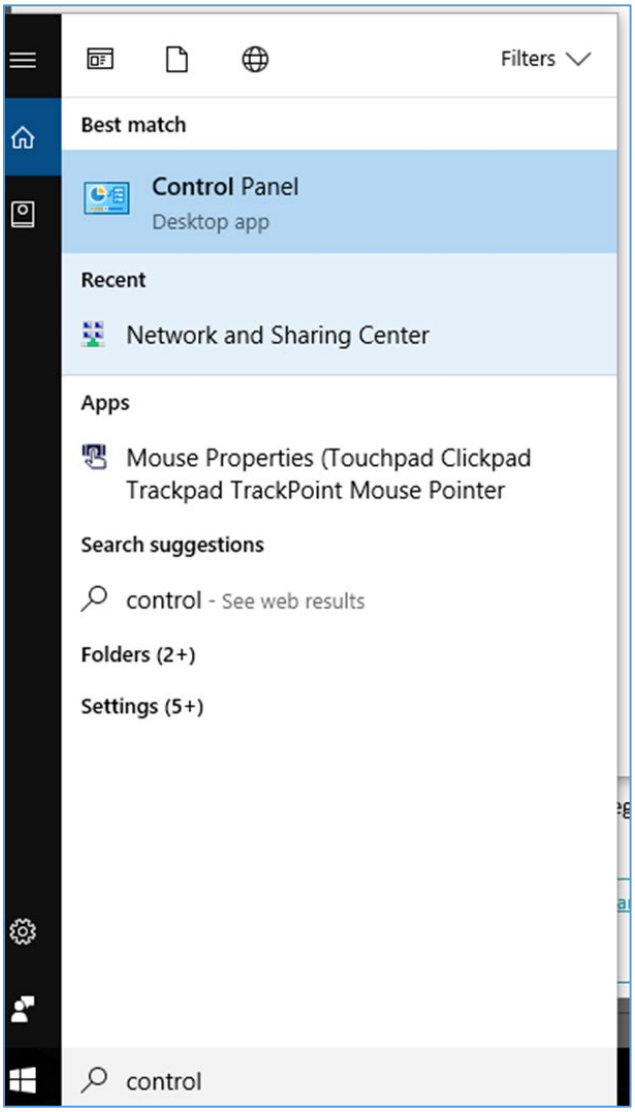


Figure 100: Control Panel

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

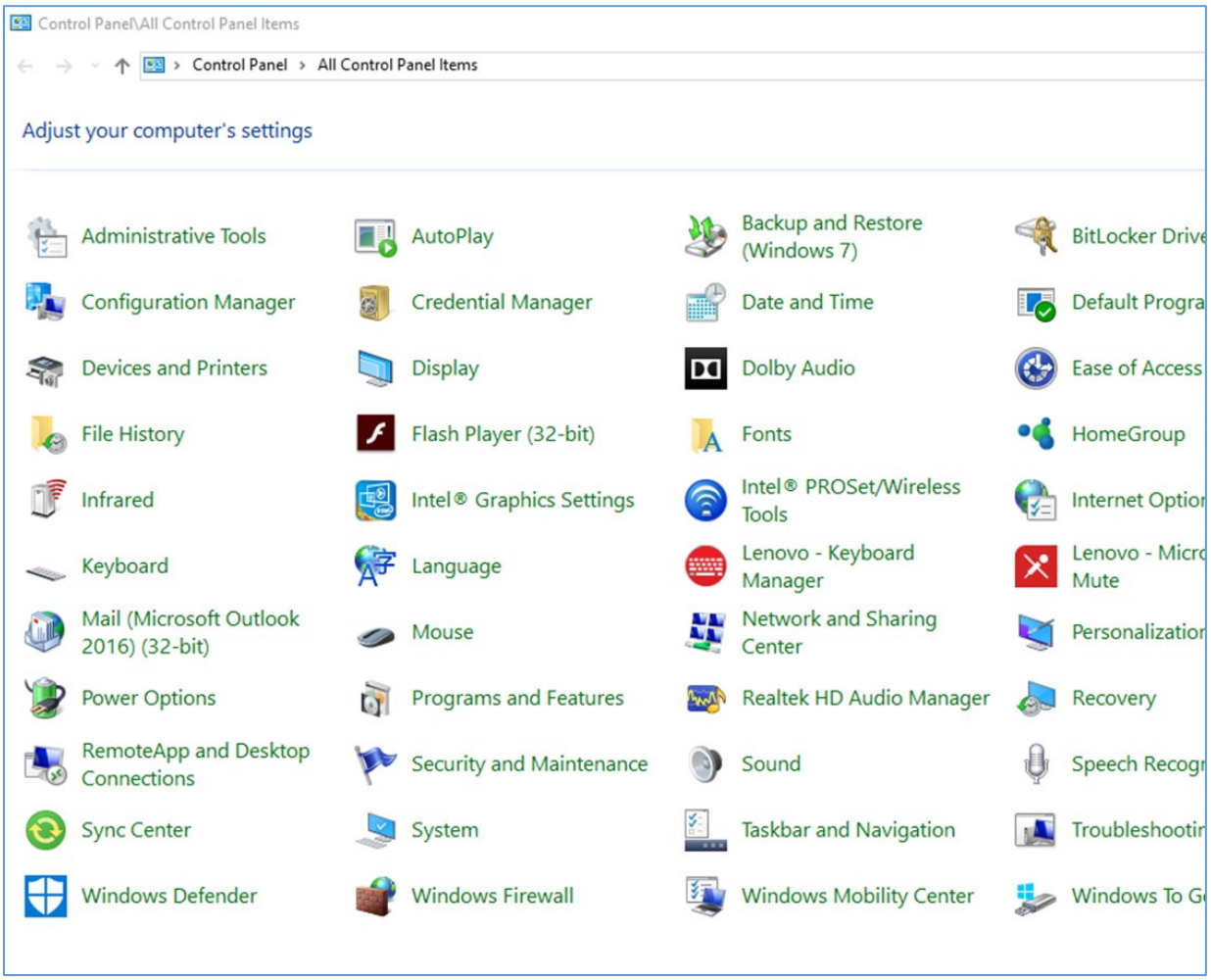


Figure 101: Network Status and Tasks

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

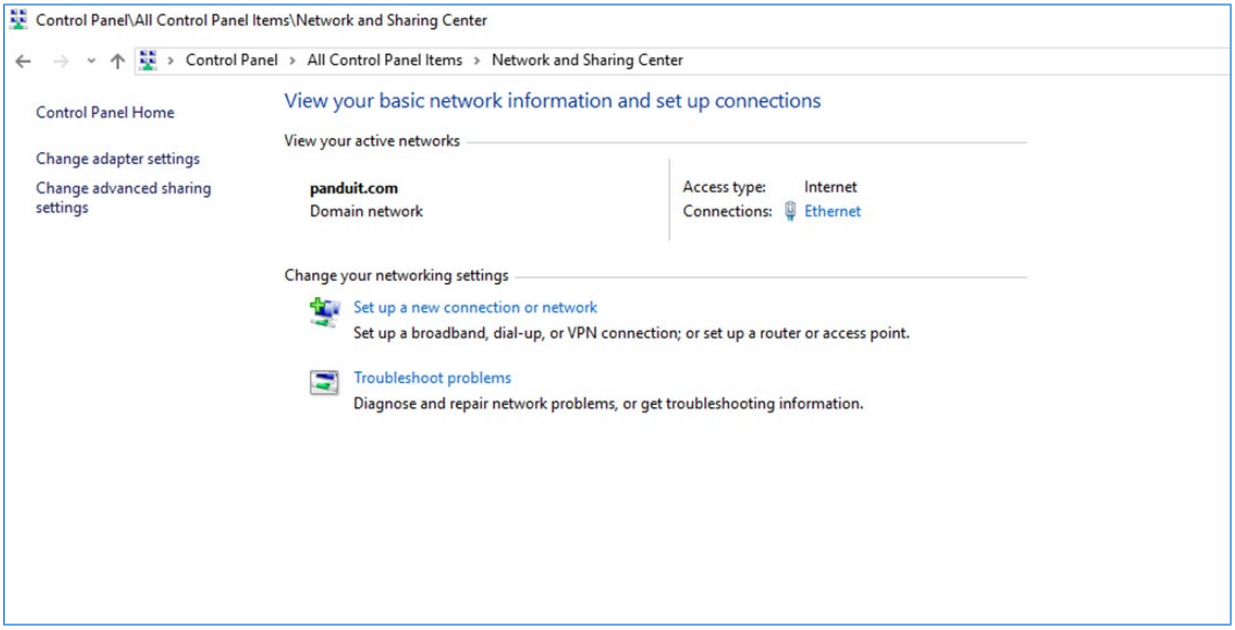


Figure 102: Change Adapter Settings

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

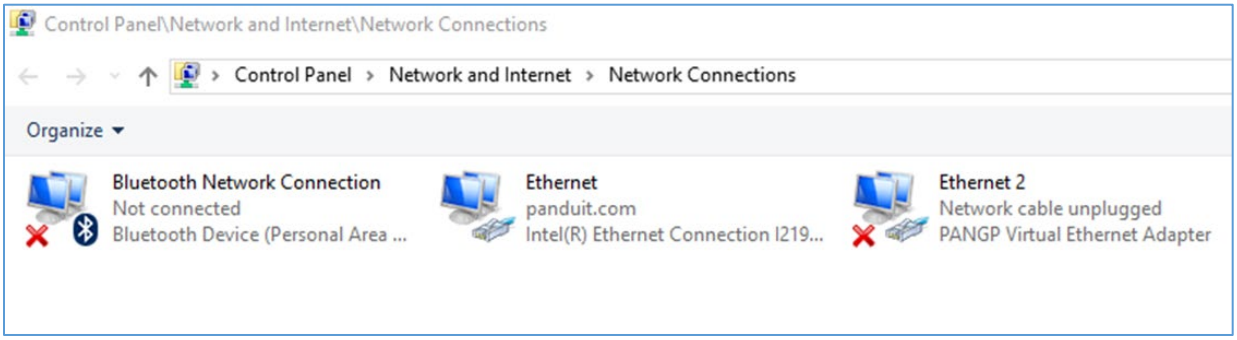


Figure 103: Properties

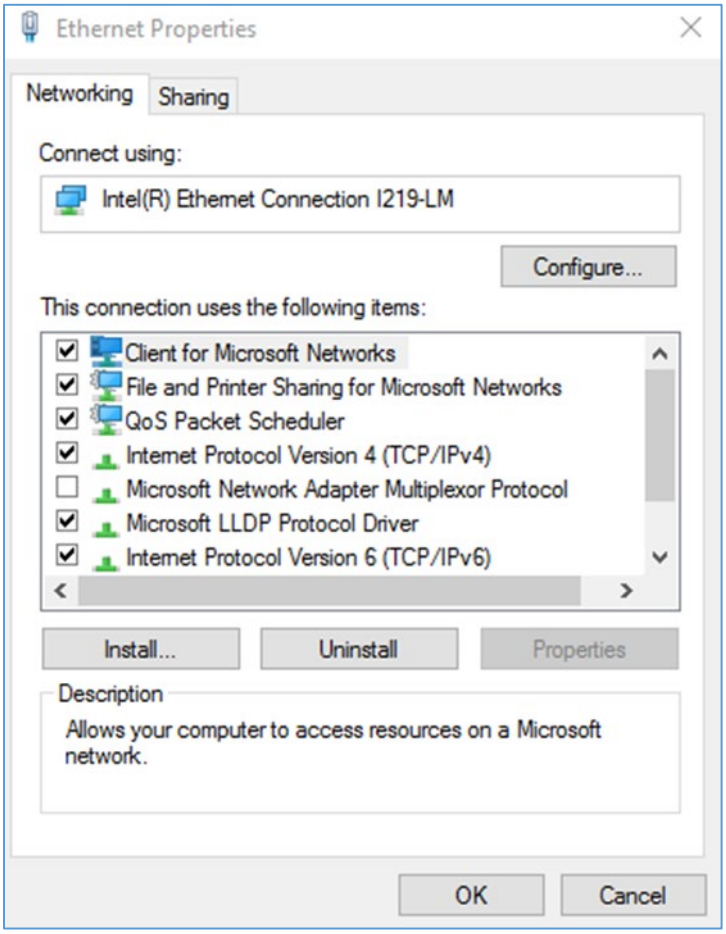


Figure 104: Ethernet Properties

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

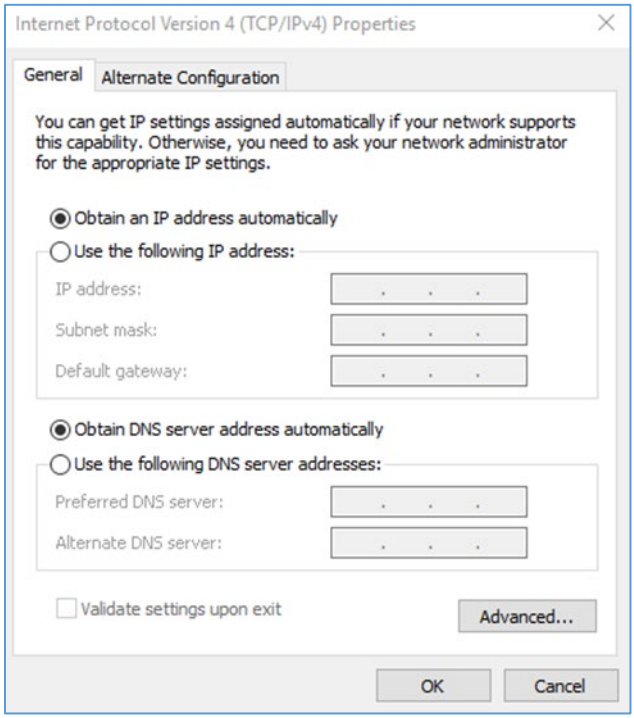


Figure 105: Internet Protocol Version 4

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

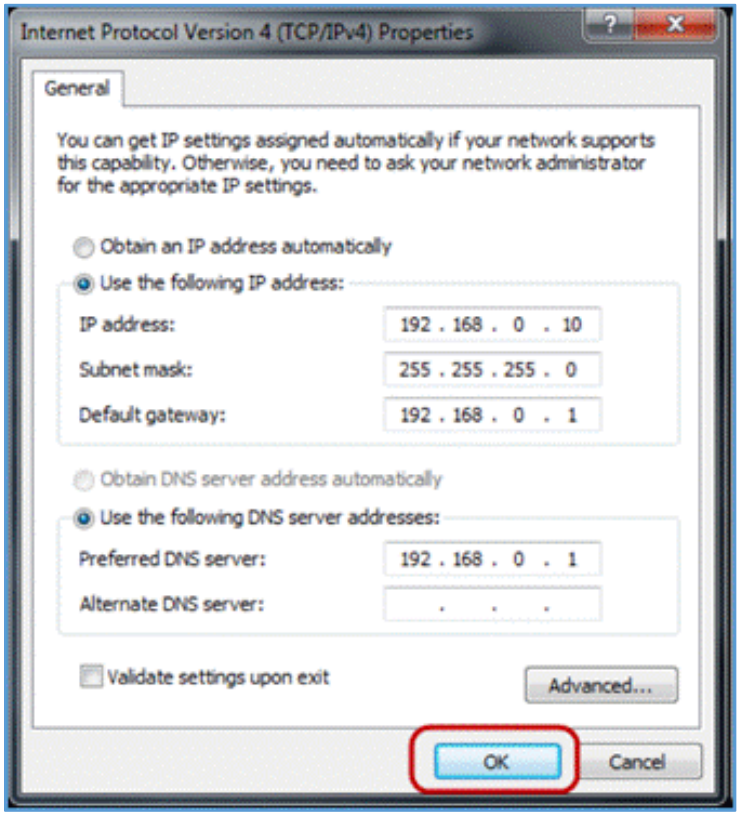


Figure 106: IP Settings for Direct Connection

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.

Appendix H: Command Line Interface (CLI)

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 below for a list of all CLI commands.

Connecting to the CLI through the serial interface

An option to communicating through the serial interface is to use the specialized YOST Serial Data Cable Panduit Part Number: MA017. This cable Remaps Panduit G5 Serial Interface to a YOST interface.

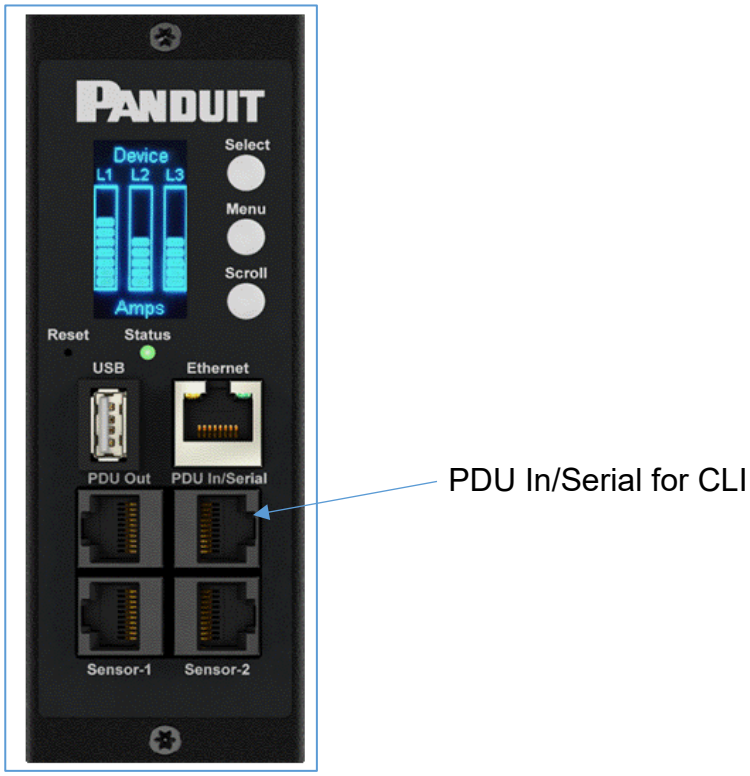


Figure 107: Connect MA017 to the PDU In/Serial port

To connect the PDU to a computer (via Serial Interface):

Using a MA017 YOST Remap cable and a Cisco Compatible Console Cable (USB to RJ45) insert the USB End to an available port of 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

Optionally if you prefer to make your own RJ45-to-DB9 Serial cable, the connections are wired as shown:

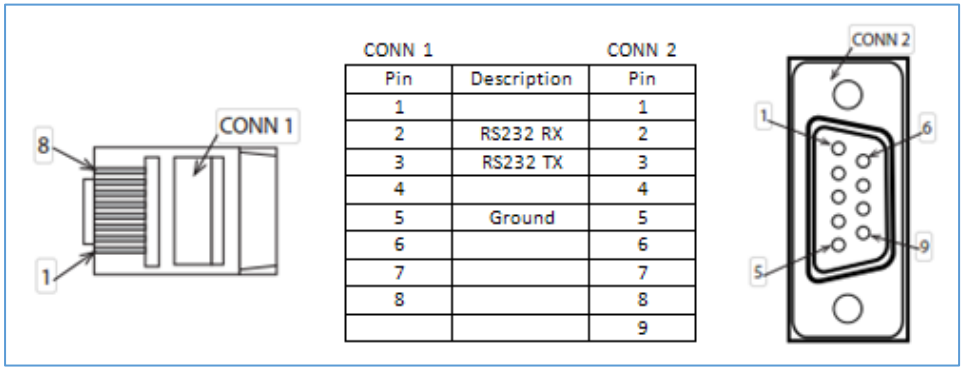


Figure 108: Serial Cable Pinout

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.

CLI Commands

Help Commands

Command	Description	Example
Panduit>?	List all available PDU CLI commands.	Panduit>? **sys** PDU system configure and setting. **net** PDU net application configure and setting. **usr** PDU user operation. **dev** PDU device setting. **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 SUCCESS Panduit>sys date SUCCESS Date: 2013-09-19 Time: 03:49:46
sys time [hour:min:sec]	Query or set system's time.	Panduit>sys time 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 **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 SUCCESS Firmware version: 3.3.2 Bootloader version: 2.65 LANGUAGE version: 4.02 WEB version: 4.22
sys def	Recover PDU to default configuration.	Panduit>sys def SUCCESS Recover Press any key to cancel
sys rst	Reset system.	Panduit>sys rst Reboot required for change to take effort. 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 SUCCESS system will enter upgrade mode after reboot System Reboot now, Are you sure? (Y/N):Y **NOTE 1:** There must be a valid file named Panduit.fw existing in root directory. **NOTE 2:** If in daisy chain configuration, main PDUs will upgrade all daisy chain firmware.
sys upd conf	Update system's configuration.	Panduit>sys upd conf SUCCESS system will enter upgrade mode after reboot System Reboot now, Are you sure? (Y/N):Y

Command	Description	Example
		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, SUCCESS
sys log edit data [on <interval> | off]	Configure data log collection parameters	PANDUIT>sys log edit data on 1 SUCCESS PANDUIT>sys log edit data off SUCCESS
sys log del data	Delete data log file.	Panduit>sys log del data, SUCCESS Panduit>
sys dualinput set <na | emea>	Setting the Region for the Dual rated PDUs Power Capacity.	Panduit> sys dualinput set na SUCCESS System Reboot now, Are you sure? (Y/N):Y

Network Commands

Command	Description	Example
net ssh [on/off]	Query or on/off SSH.	Panduit>net ssh SUCCESS, SSH Port: 22 SSH Server is running Panduit>net ssh on SUCCESS Panduit>net ssh off SUCCESS
net ftps [on/off]	Query or on/off FTPs.	Net ftps SUCCESS FTPS Port: 21 Service is running Is Ftps

Command	Description	Example
net http [on/off]	Query or on/off net http.	Panduit>net http SUCCESS, HTTP Port: 80 HTTPS Port: 443 WEB Protocol: HTTP Panduit>net http off E801 WEB protocol is changed, Please reboot to validate System Reboot now, Are you sure? (Y/N):Y
net mac	Query MAC address.	Panduit>net mac SUCCESS MAC Addr: C8-45-44-66-2B-26
net tcpip	Query network's IP information.	Panduit>net tcpip SUCCESS IPv4 Addr: 192.168.30.39
net tcpip <dhcp>	Set network to dhcp mode.	Panduit>net tcpip dhcp SUCCESS Network is reconfigured, Please reboot to validate 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 192.168.30.39 255.255.255.0 192.168.30.1 SUCCESS Network is reconfigured, Please reboot to validate System Reboot now, Are you sure? (Y/N): Y

User Commands

Command	Description	Example
User List	List all users account existing.	Panduit>usr list SUCCESS Usr Role ---------- admin admin user user
User unlock<username>	Unlock specified user.	Panduit>usr unlock user SUCCESS Panduit>usr unlock admin SUCCESS **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 Panduit>dev usb off Panduit>dev usb on
dev daisy [rna|qna]	Query or set daisy chain mode.	Panduit>dev daisy SUCCESS daisy chain unit number: 1 daisy chain address list: 000 Daisy Mode: RNA Panduit>dev daisy qna SUCCESS System Reboot now, Are you sure? (Y/N): N
dev daisy <rna|qna> init	Initialize daisychain.	Panduit>dev daisy qna init

Command	Description	Example
		SUCESS 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 SUCCESS
dev outlet <PDUID> status	Query all outlets' status with specified PDUID.	Panduit>Dev outlet 1 status SUCCESS Relay Outlet Status Outlet#1: Close Outlet#2: Close Outlet#3: Close Outlet#4: Close Outlet#5: Close Outlet#6: Close Outlet#7: Close Outlet#8: Close Outlet#9: Close Outlet#10: Close Outlet#11: Close Outlet#12: Close **NOTE 1:** For M pdu, this command is in valid. **NOTE 2:** PDUID index from 1; if in daisy chain, the main PDUID is 1,the Daisy chain PDUID's are 2,3,4.
dev outlet <PDUID> <outlet index> [on|off]	Query or set specified PDUID and outlet-index's outlet status.	Panduit> dev outlet 1 1 off SUCCESS **NOTE:** For Monitored PDUs, this command is invalid.
dev sensor	List all sensors equipped.	Panduit> dev sensor SUCCESS Sensor count 4 ----------

Command	Description	Example
		Name Type, SN Value ---------- T1,TEMP 012345678 27.5 T3,TEMP 012345678 27.2 T2,TEMP 012345678 27.3 RH HUMI 012345678 44
dev ver <slipaddr>	Query sensor/power/delay's firmware version.	Panduit> dev ver 1 Panduit> dev ver 15 Panduit> dev ver 35 **NOTE:** relay: start from 1 power: start from 15 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 SKU: P9S20A , , , , Serial: , , , , , FuncType: PDU Monitored Rating :220-240V, 16A, 3.5-3.8kVA, 50/60Hz Mac :C8:45:44:66:2B:26 Tcpip :192:168:30:38 Panduit>pwr unit 1 SUCCESS PDU UNIT 1 power Feature voltage: 0V current : 0.0A active power: 0W apparent power: 0W power factor: 0.00 energy: 0.000kWh

Command	Description	Example
pwr phase <idx>	Query specified phase's electric information.	Panduit> pwr phase 1 SUCCESS PDU PHASE 1 power Feature voltage: 0V current : 0.0A active power: 0W apparent power: 0W power factor: 0.00 energy: 0.000kWh
pwr cb <idx>	Query specified circuit breaker's Electric information.	Panduit> pwr cb 1 SUCCESS PDU CB 1 power Feature voltage: 0V current : 0.0A active power: 0W apparent power: 0W power factor: 0.00 energy: 0.000kWh
pwr outlet <idx>	Query specified outlet's electric information.	Panduit> pwr outlet 1 SUCCESS PDU OUTLET 1 power Feature voltage: 0V current : 0.0A active power: 0W apparent power: 0W **NOTE:** For Monitored PDUs, this command is invalid.

Appendix I: RADIUS Server Configuration

To allow users to login as the admin User-Role

This example demonstrates how to configure freeradius with users that can login as the admin User-Role. It assumes a clean installation of freeradius on Ubuntu or and equivalent installation.

1. Install freeradius or start with a pre-existing installation.
2. Create authorized client configuration statements in `/etc/freeradius/3.0/clients.conf` that are configured for your security requirements.
3. Create a dictionary at /usr/share/freeradius/dictionary.Panduit containing:

```
# -*- text -*-
VENDOR          Panduit         19536
BEGIN-VENDOR    Panduit
ATTRIBUTE       User-Role       1       integer
VALUE           User-Role       User    1
VALUE           User-Role       Admin   2
END-VENDOR      Panduit
```

4. Load dictionary.Panduit by appending the following line to `/etc/freeradius/3.0/dictionary`:

```
$INCLUDE /usr/share/freeradius/dictionary.Panduit
```

5. Add authorized users to `/etc/freeradius/3.0/mods-config/files/authorize` with the desired role. (Note: the ‘users’ file location may vary based on unique customizations or different package managers.) When specified, the User-Role MUST be the first attribute of the user. Use passwords that are configured for your security requirements.
    a. User-Role is not specified: (This user logs in as the default “user” Role)

```
raduser         Cleartext-Password := "23456789"
                 Service-Type = 1
```

    b. User-Role is set to Admin: (This user logs in as the “admin” Role)

```
radroleadmin    Cleartext-Password := "34567890"
                 User-Role = Admin,
                 Service-Type = 1
```

    c. User-Role is set to User: (This user logs in as the “user” Role)

```
radroleuser     Cleartext-Password := "45678901"
                 User-Role = User,
                 Service-Type = 1
```

6. If you started with a clean install of freeradius, you may need to configure these

options to enable authentication in `/etc/freeradius/3.0/radiusd.conf`: (make sure they are configured for your security requirements)

```
auth_badpass = yes
auth_goodpass = yes
auth = yes
```

7. Restart the RADIUS server for the configuration changes to take effect.

```
systemctl stop freeradius
systemctl start freeradius
```

8. Verify the server is able to perform authentication and returns the configured User-Role. Note: You may need to change this example based on any client restrictions that are enforced.

```
Usage: radtest [OPTS] user passwd radius-server[:port] nas-port-number secret


# radtest 'radroleadmin' '34567890' 192.0.2.1 0 'panduit#1' ''
Sending Access-Request of id 212 to 192.0.2.1 port 1812
        User-Name = "radroleadmin"
        User-Password = "34567890"
        NAS-IP-Address = 127.0.1.1
        NAS-Port = 0
        Message-Authenticator = 0x00000000000000000000000000000000
rad_recv: Access-Accept packet from host 192.0.2.1 port 1812, id=212, length=38
        User-Role = Admin
        Service-Type = Framed-User
```

Appendix J: Panduit G5 Accessories

Accessory P/N	Accessory Description
EA001	Panduit G5 Temperature Sensor
EB001	Panduit G5 Temperature + Humidity Sensor
EC001	Panduit G5 (3) Temperature + Humidity Sensor
ED001	Panduit G5 Liquid Rope Sensor
EE001	Panduit G5 Liquid Spot Sensor
EF001	Panduit G5 (3) Sensor Hub
EG001	Panduit G5 Liquid Rope Extension
ACA01	Panduit G5 Door Switch (magnetic 2 piece)
ACC01	Panduit G5 Dry Contact Input
ACD01	Panduit G5 USB Light Strip
ACF05	Panduit Security Handle with Integral Humidity Sensor
ACF06	Panduit Security Handle with Integral Humidity Sensor and Keypad
ACF10	Temperature and Door Sensor; connects to Electronic Security Handle. (Rear)
ACF11	(3) Temperature and Door Sensor, connects to Electronic Security Handle (Front)
ACF20	Electronic Security Handle Patch Cord (JST to RJ45 Male)
MA030	Electronic Security Handle Patch Cord (RJ45 Female to RJ45 Male)
MA031	Panduit PDU Power Share Patch Cord (RJ45 Male to RJ45 Male)
MA005	Panduit PDU Controller
MA017	Category 6, PDU YOST Serial Data Cable Assembly
CRD-02-10PK	Electronic Security Handle HID CARDS 125 KHZ (10 PACK)
CRD-03-10PK	Electronic Security Handle HID CARDS 13.56 MHZ (10 PACK)
TU020X	Base Tumbler for Key KE020X, for ACF05, ACF06
TU021X	Option 1 Tumbler for Key KE021X, FOR ACF05, ACF06
TU022X	Option 2 Tumbler for Key KE022X, FOR ACF05, ACF06
TU023X	Option 3 Tumbler for Key KE023X, FOR ACF05, ACF06
TU024X	Option 4 Tumbler for Key KE024X, FOR ACF05, ACF06
TU025X	Option 5 Tumbler for Key KE025X, FOR ACF05, ACF06
KE020X	Base Key for Tumbler TU020X
KE021X	Option 1 Key for Tumbler TU021X
KE022X	Option 2 Key for Tumbler TU022X
KE023X	Option 3 Key for Tumbler TU023X
KE024X	Option 4 Key for Tumbler TU024X
KE025X	Option 5 Key for Tumbler TU025X

Note: Panduit G5 PDU Controller can handle a maximum of 8 sensors. Some part numbers have multiple sensors built in (e.g. EC001 has 4 sensors, ACF05 or ACF06 has 2 sensors).

Appendix K: Compliance Model Number Details

PP#&*%%-XXXX, where:

XXXX: Series number. Shown different outlet combination

%%: Input Current. 16 means 16A

*: Form 0:0U 1:1U 2:2U

&: Power Input: 1: 200-240Vac, 1 phase

2: 200-240/346-415 Vac (Wye), 3 phase

3: 100-120Vac, 1 phase

4: 200-240Vac (Delta), 3 phase

5: 100-240Vac, 1 phase

6: 120-208Vac (Wye), 3 phase

#: Different management feature.

0: Basic PDU

1: Metered iPDU

2: Metered, Outlet switched iPDU

5: Outlet Metered iPDU

6: Outlet Metered, Outlet switched iPDU

Appendix L: JSON API Web Service

This API enforces constraints on certain JSON types:

- Objects: may only be nested one level in a resource or 2 levels in a resource collection.
- Numbers: must be within the range and precision defined by the property.
- Strings: must not exceed the maximum (encoded) length defined by the property AND must contain only ASCII printable characters, except where noted. Some strings have a no space requirement or special format requirement.
- Arrays: must not be nested and must contain delimited strings or primitive numbers.

General PDU Limitations:

- String encoded tabs, backspaces, form feeds and Unicode are not supported.
- Exponential numbers are not supported.
- Nested arrays or arrays of objects are not supported.
- Maximum object depth is 2.

Method	Supported URLs
GET Response	/redfish/v1/SessionService
	/redfish/v1/SessionService/Sessions
	/redfish/v1/SessionService/Sessions/{session_ids}
	/redfish/v1/AccountService
	/redfish/v1/AccountService/Accounts
	/redfish/v1/AccountService/Accounts/{username}
	/redfish/v1/AccountService/Roles
	/redfish/v1/AccountService/Roles/{rolename}
	/redfish/v1/Managers

	/redfish/v1/Managers/manager
	/redfish/v1/Managers/1/NetworkService
	/redfish/v1/RackPower/PowerDistribution
	/redfish/v1/PowerDistribution/{pdu_id}<1>
	/redfish/v1/PowerDistribution/{pdu_id}/PowerMeasurement/Loadsegment/{loadsegment_id}/OutletMeasurement
	/redfish/v1/PowerDistribution/{pdu_id}/PowerMeasurement/LoadsegmentMeasurement
	/redfish/v1/EventService
POST Response	/redfish/v1/AccountService/Accounts
	/redfish/v1/SessionService/Sessions
DELETE Response	/redfish/v1/AccountService/Accounts/{username} /redfish/v1/SessionService/Sessions/{session_id}

For the code on any of the above listed interfaces – please refer to Panduit TR128-SZ G5 RestfulAPI.pdf

For a copy of this document send a request to systemsupport@panduit.com