PANDUIT®
infrastructure for a connected world

PANDUIT™

G6

Intelligent PDU User Manual v1.2

Table of Contents

Table of Figures

Section 1 – System Overview

PDU Controller

Panduit G6 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).

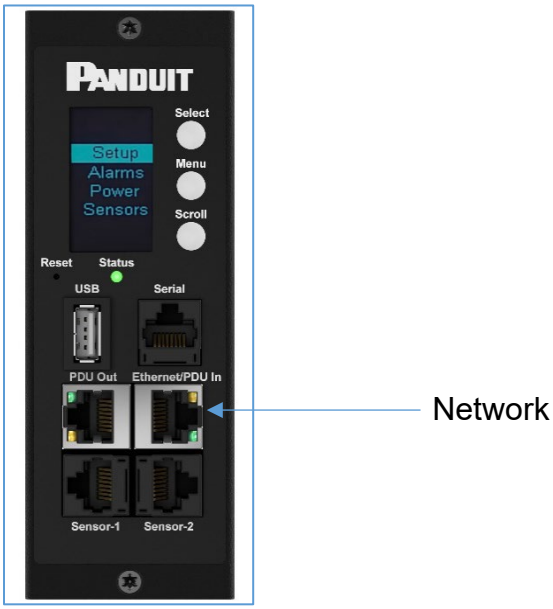


Figure 1: Primary GB Ethernet Port for Network Connection

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).

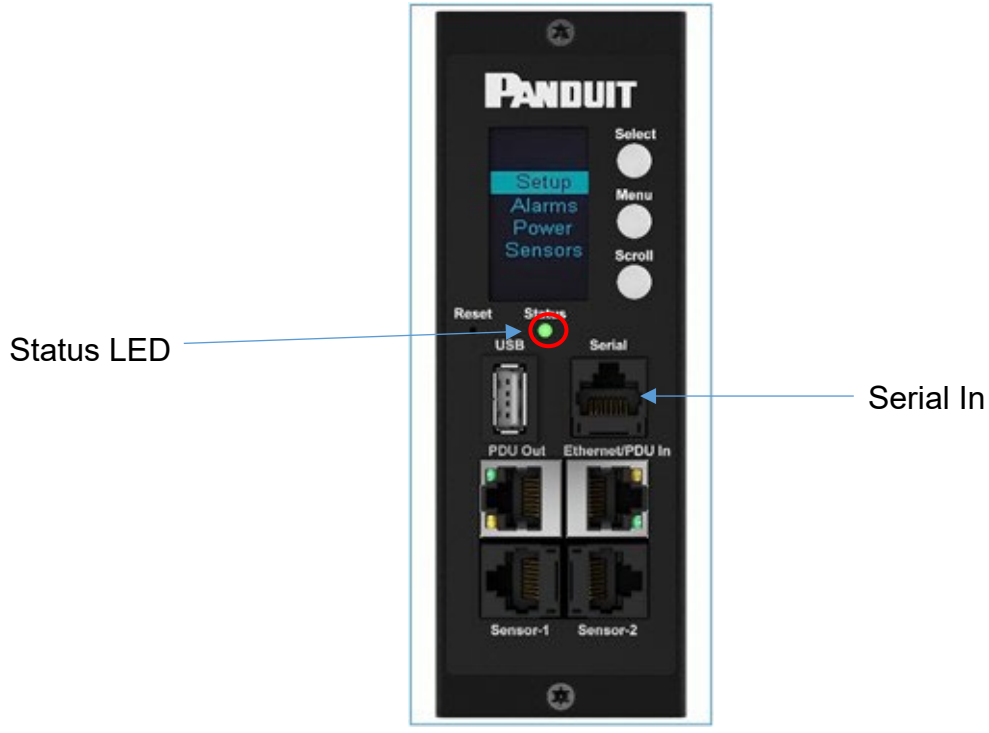


Figure 2: Status LED & Serial In Port Identified

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).

IPV4, IPV6 or Dual

Panduit G6 iPDU features a Dual Ethernet interface where ETH0 is the primary and ETH1 is the internal ethernet interface used during daisy chain. The Panduit G6 also features a full IP stack for either IPV4 or IPV6. The PDU can also be placed in Dual (IPV4 or IPV6) Mode.

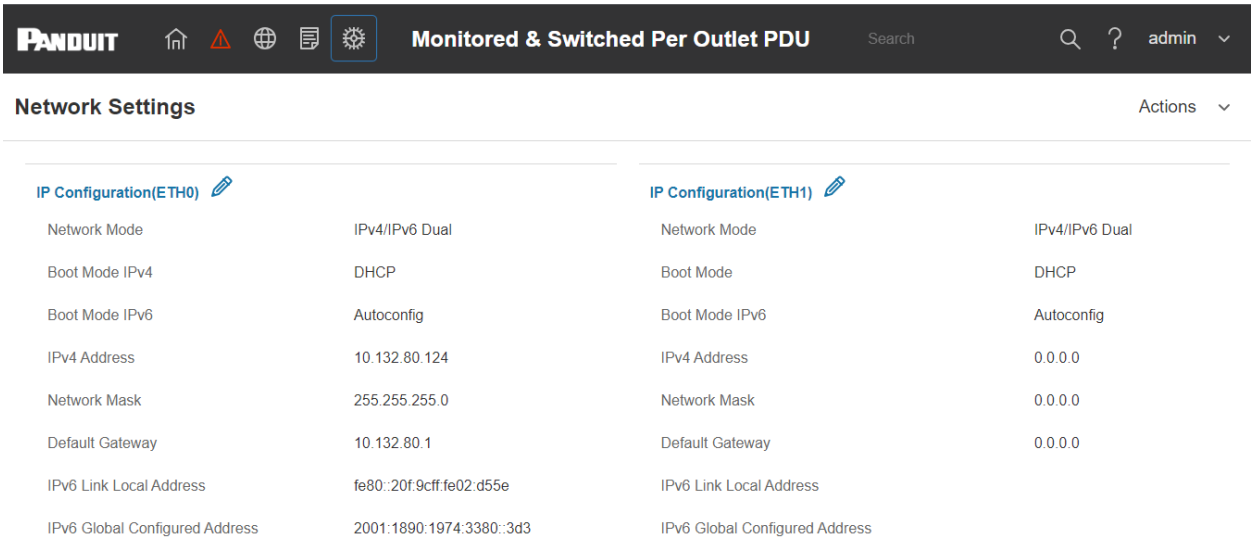


Figure 3: Shows ETH0 & ETH1 and Dual IP Modes

In the Edit IP Configuration (ETH0) user can:

1. Select whether they want the PDU to be in IPV4, IPV6 or Dual Mode
2. Selected Boot Mode to be DHCP or Static for IPV4 or IPV6

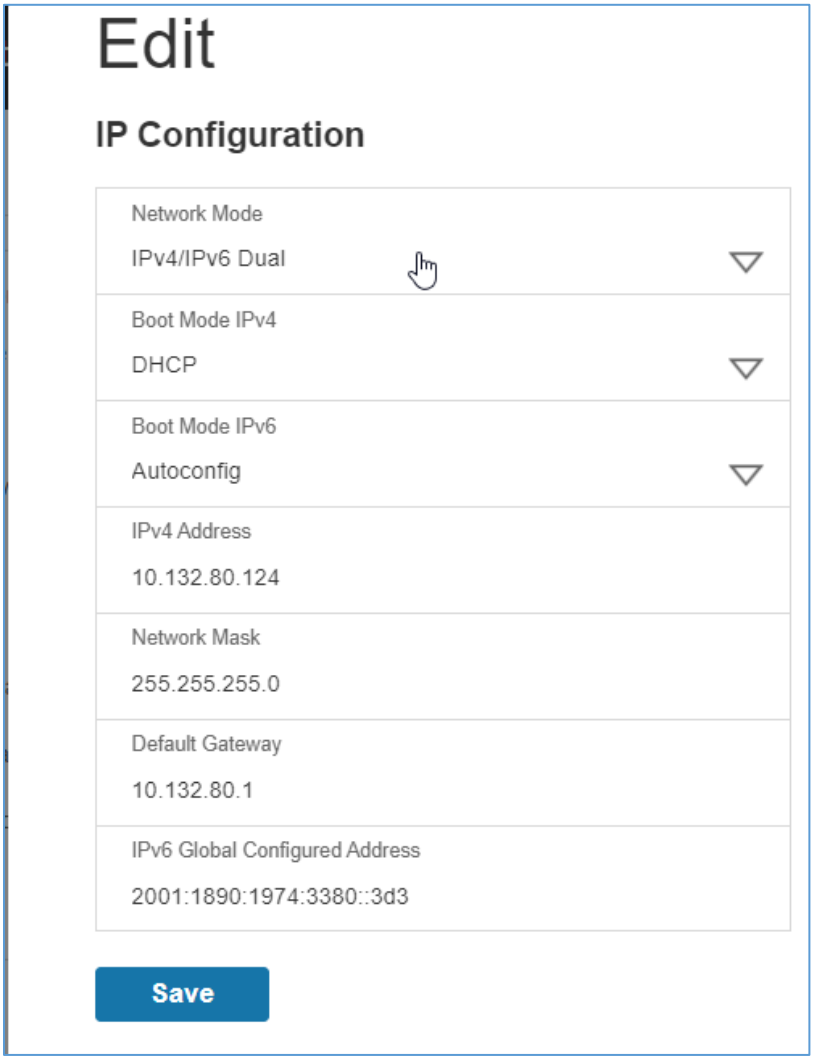


Figure 4: Edit ETH0

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 IPV4 or IPV6 address (**Error! Hyperlink reference not valid.** or https://[IPv6Address]/ respectively) 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.

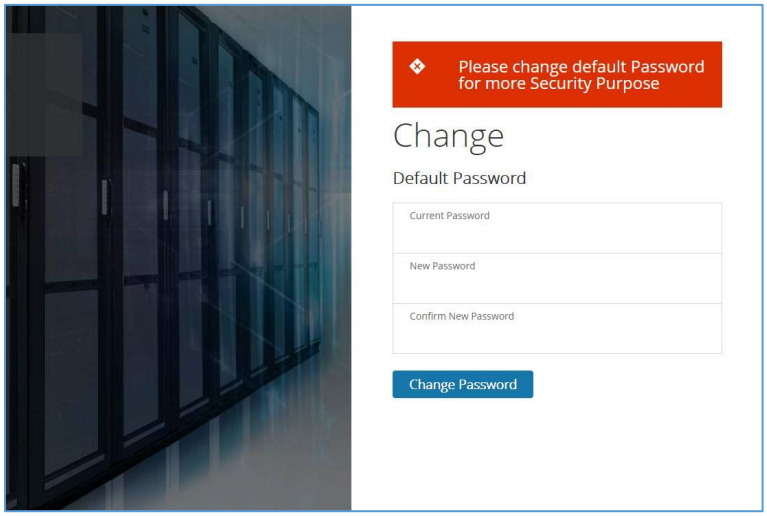


Figure 5: Changing Your Password

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.

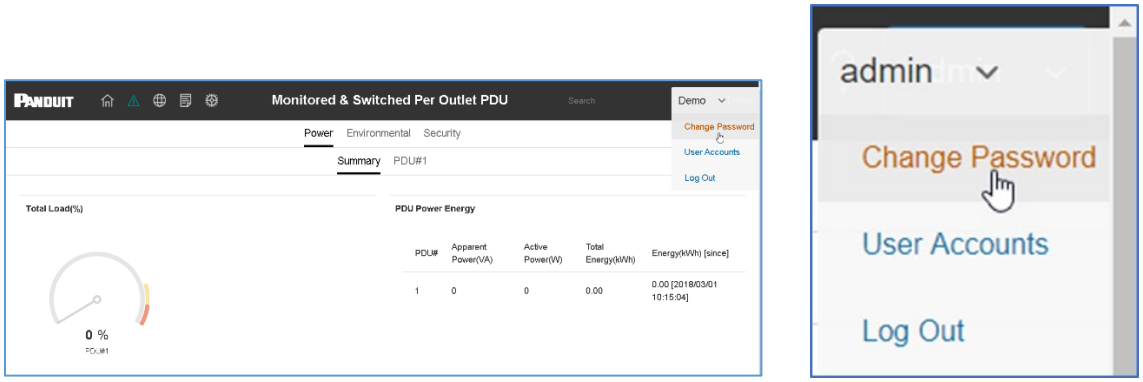
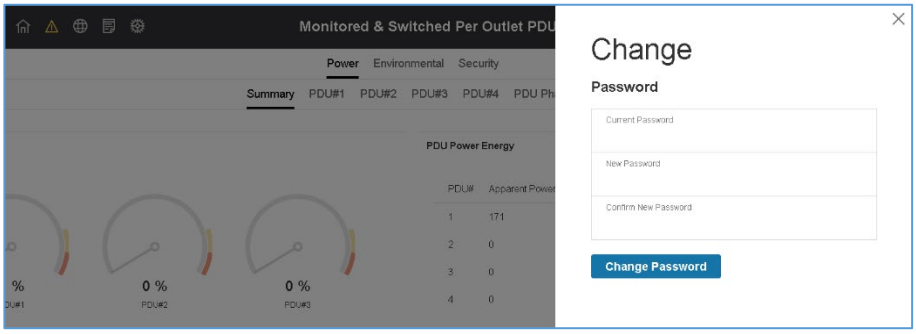


Figure 6: After Login

2. The Change User Password window opens.

Figure 7: 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.

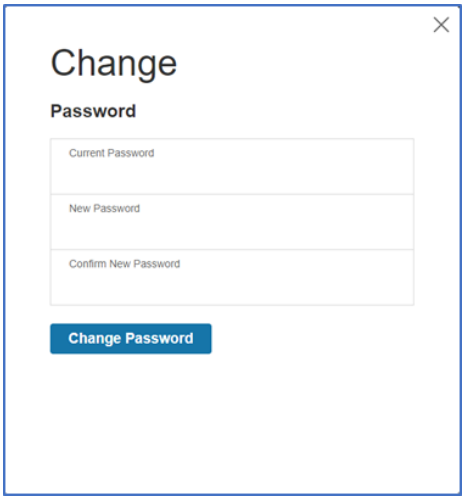
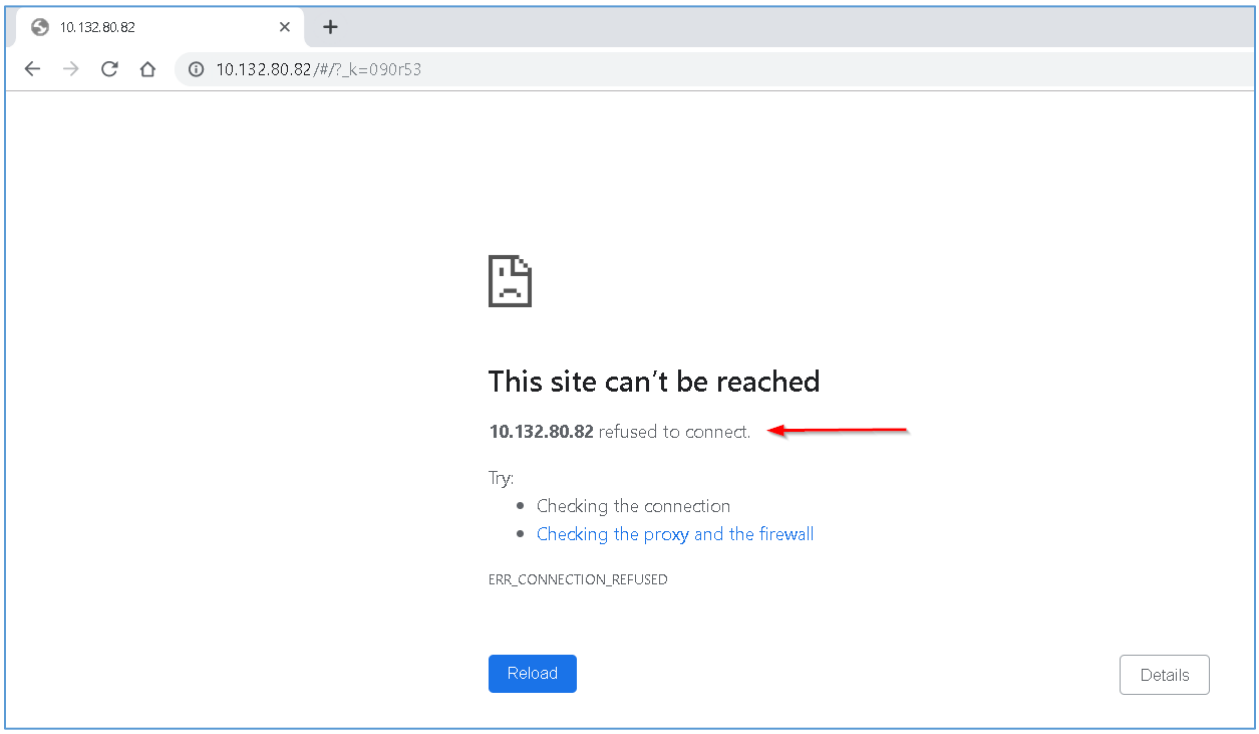


Figure 8: Change Password

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 9: Login Page

Landing Page/Dashboard

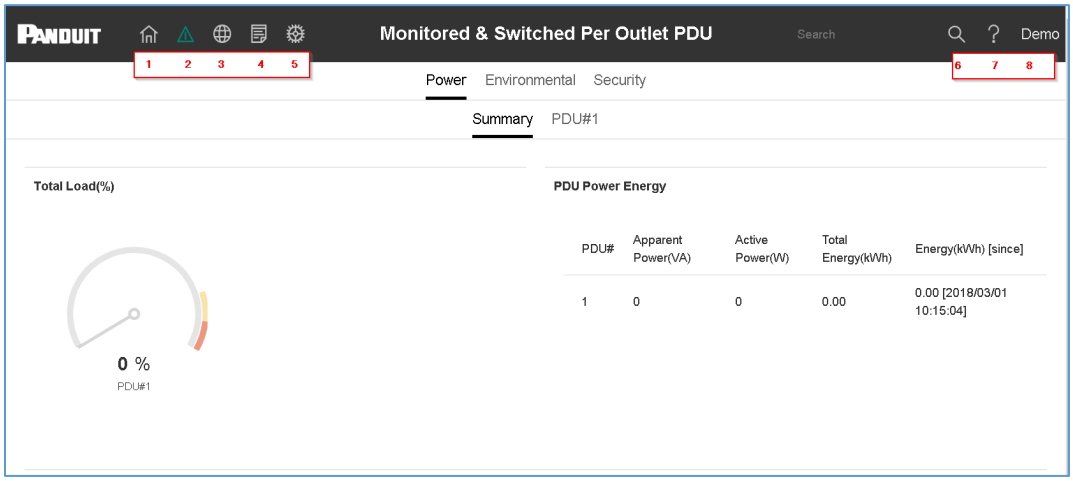


Figure 10: Landing Page/Dashboard

Number	Icon	Description
1		The home icon provides an overview of the PDU with access to the Dashboard,

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

Number	Icon	Description
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.

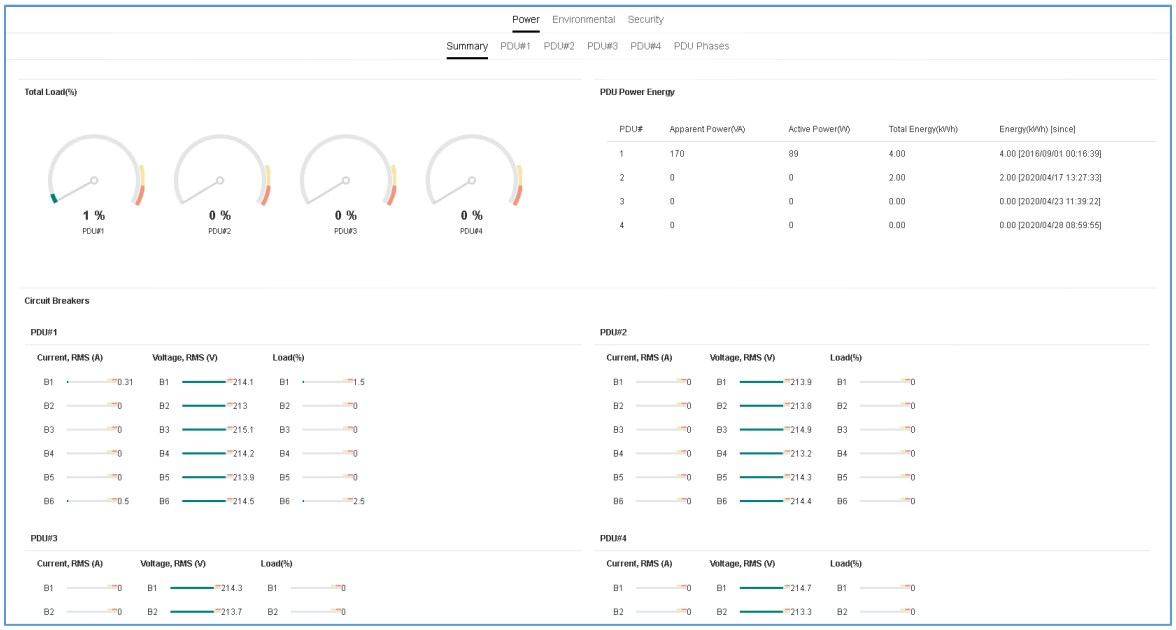


Figure 11 - Resized Dashboard Screen

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

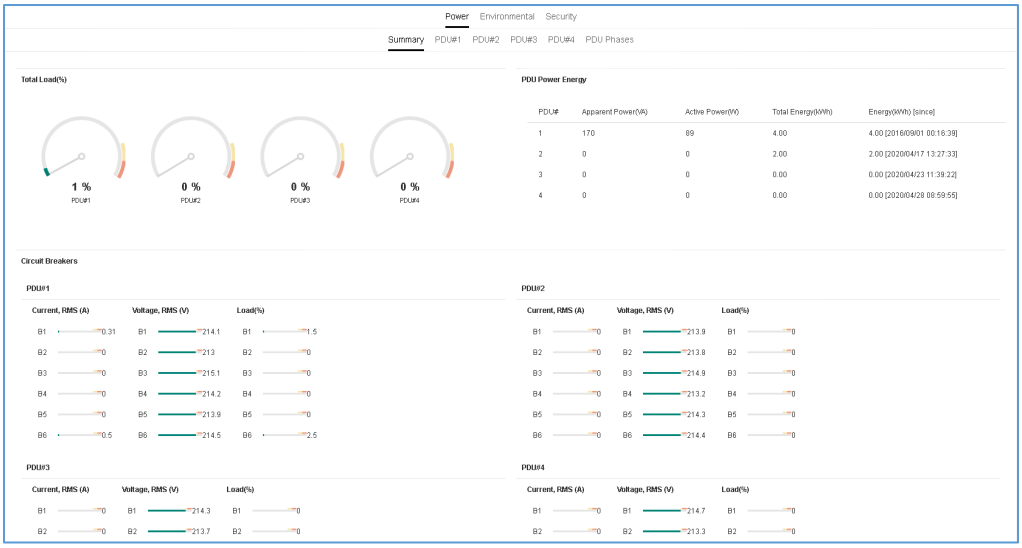


Figure 12: Power Summary Page

Outlet Monitoring Page

Figure 13: Outlet Monitoring Page

Environmental Monitoring Page

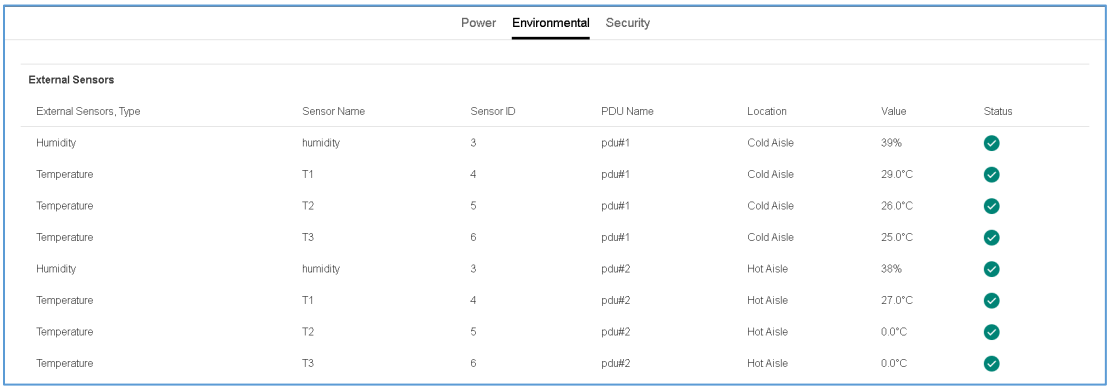


Figure 14: Environmental Monitoring Page

Security Monitoring Page

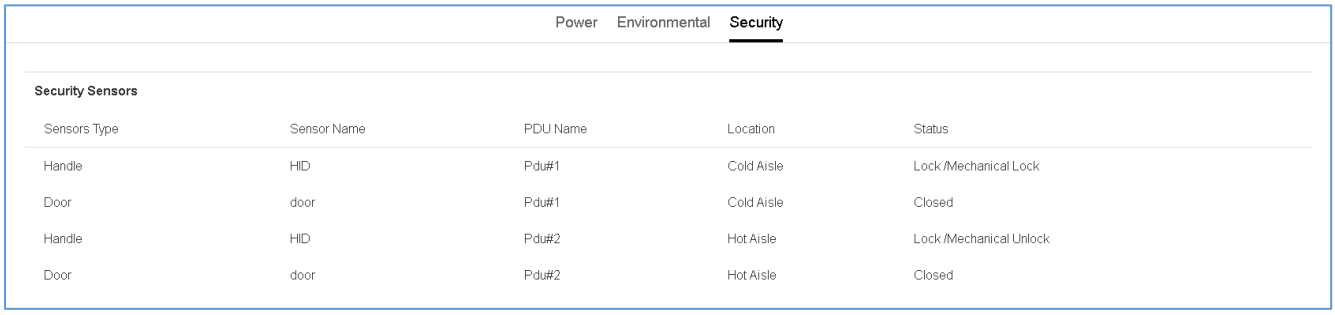
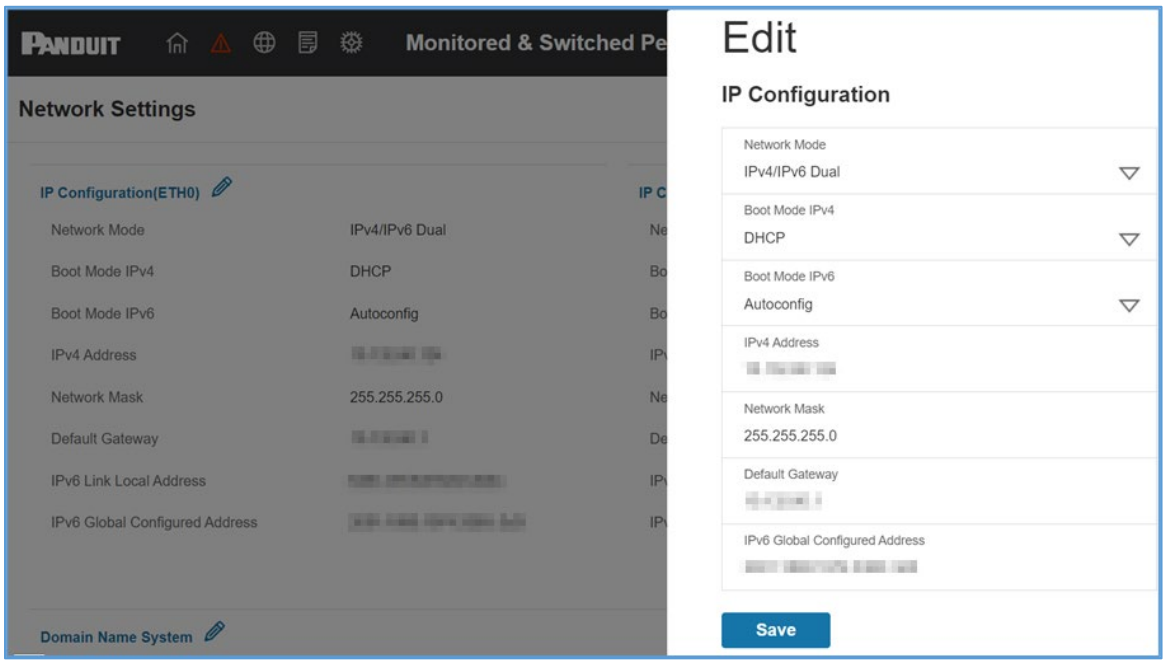


Figure 15: Security Monitoring Page

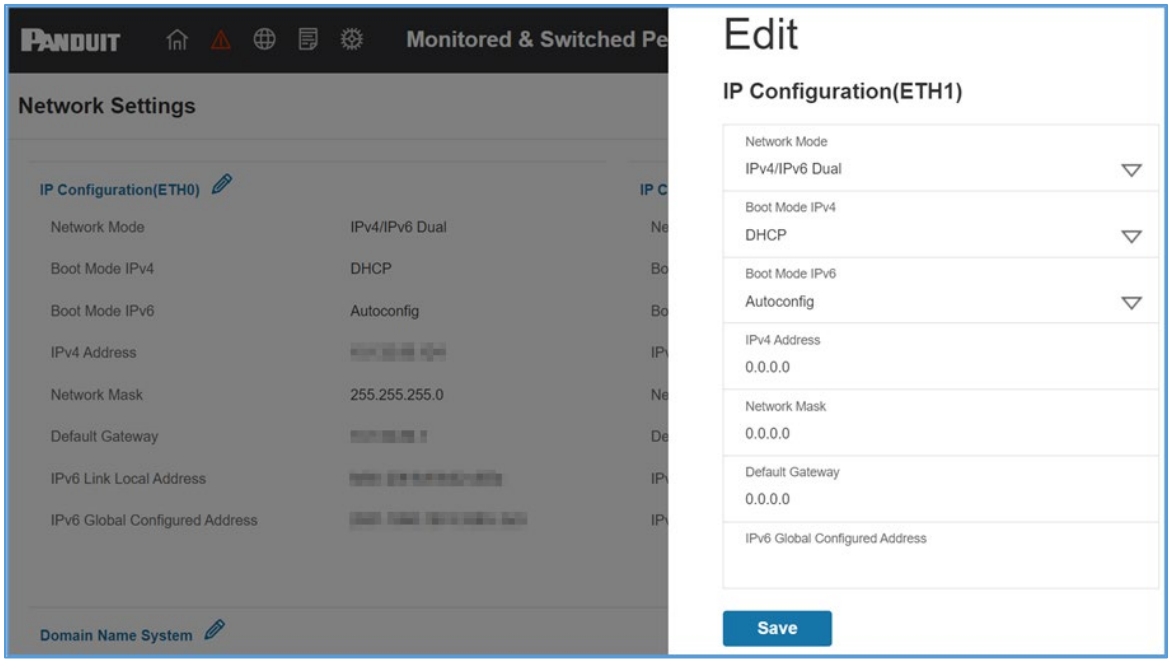
Network Settings

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.

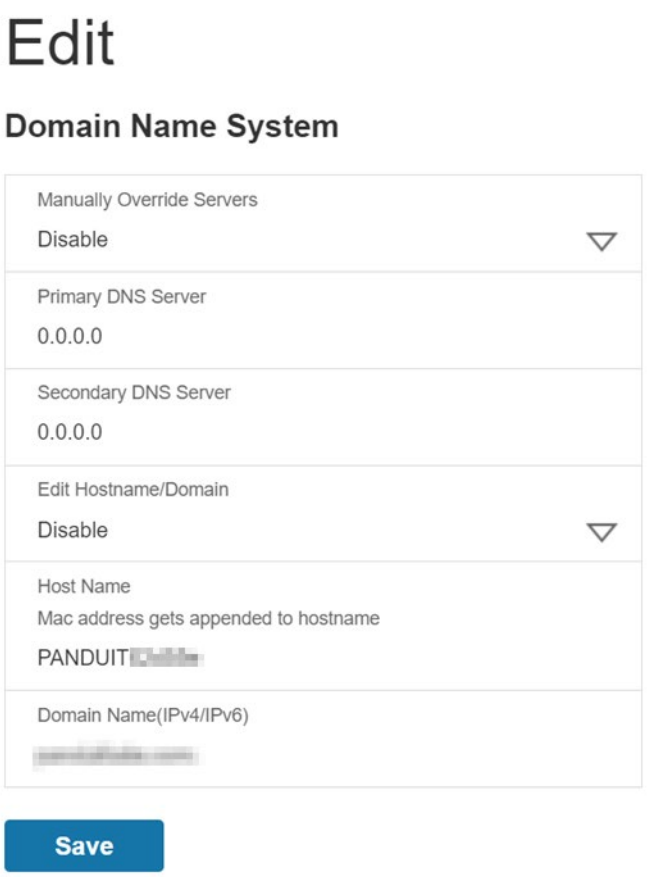
IP Configuration (ETH0):



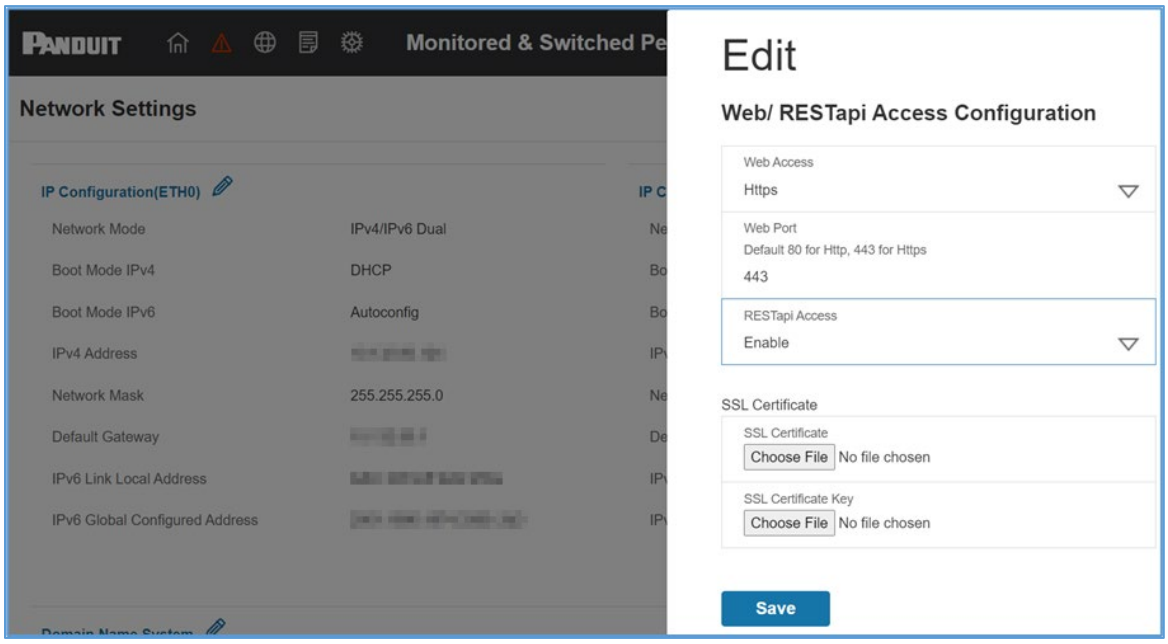
IP Configuration (ETH1):



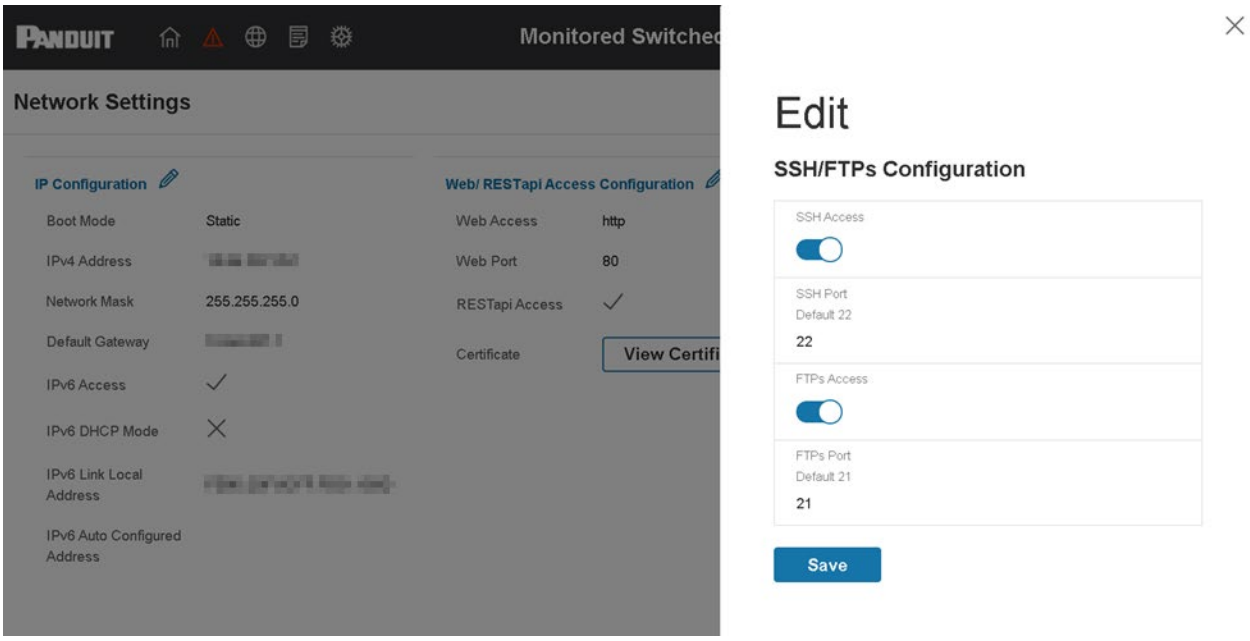
Domain Name System (DNS):



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.

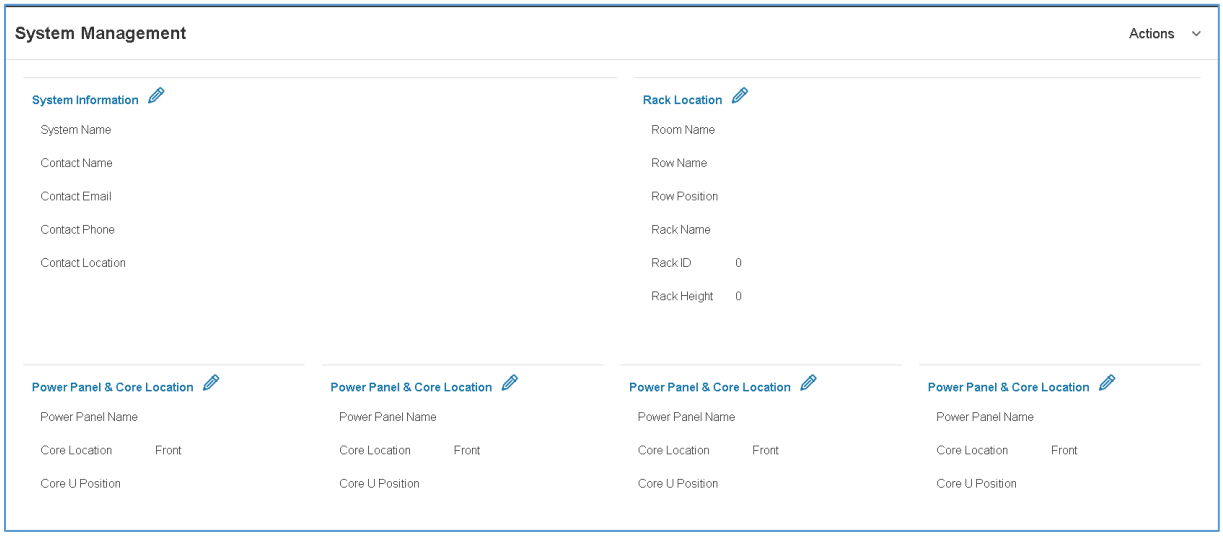


Figure 16: System Management

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.**

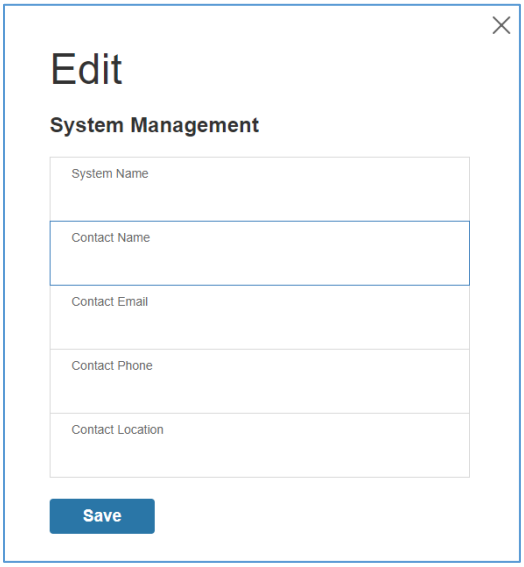


Figure 17: System Management Configuration

2. Enter the **System Name**: The “system” is the main PDU and all daisy-chained PDUs. A system can have 6 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**.
3. 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.**

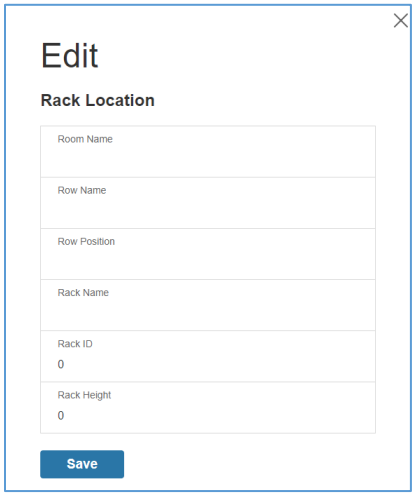


Figure 18: Rack Location Configuration

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.

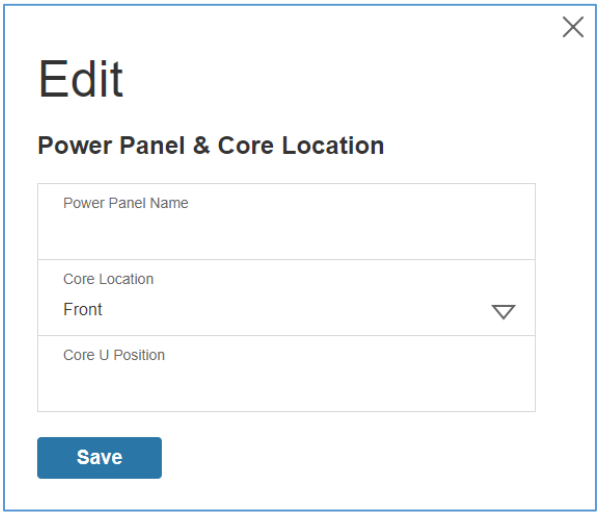


Figure 19: Power Panel & Core Location

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**.

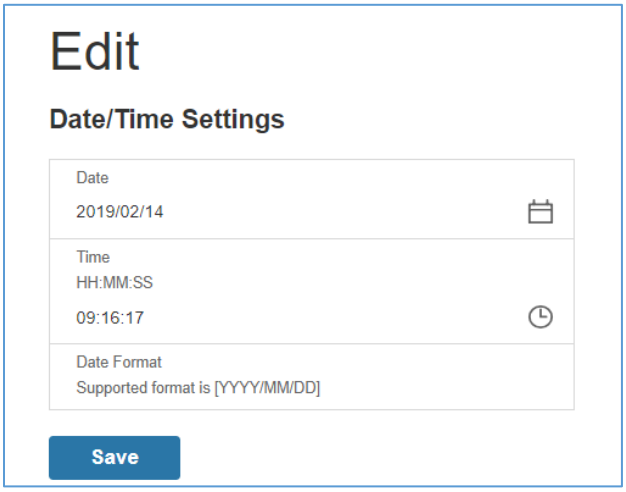
Note: If editing 'Power Panel & Core Location' – all fields are required to be filled to save the information.

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).

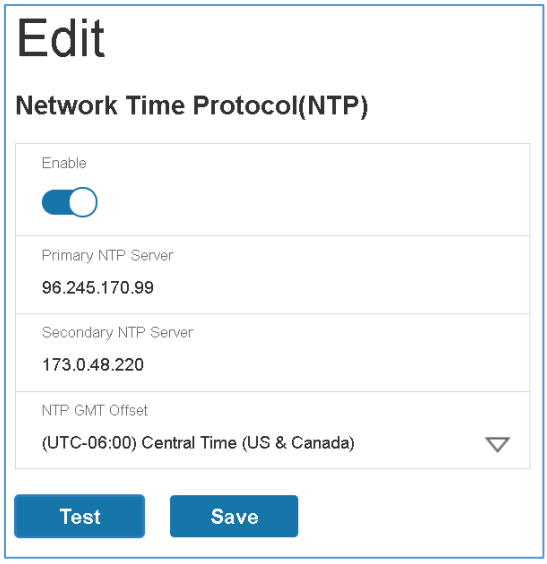


Figure 20: NTP Configuration

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.

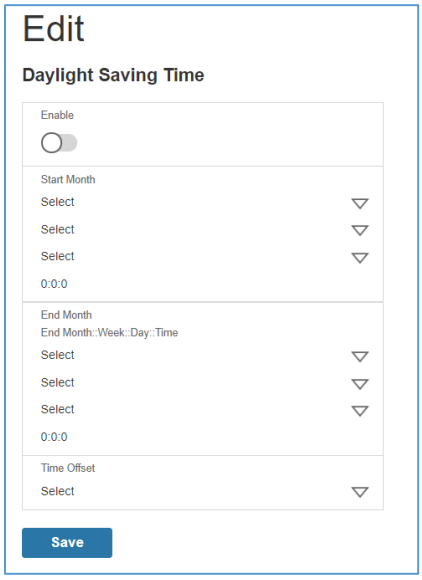


Figure 21: Daylight Saving Time Configuration

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**.

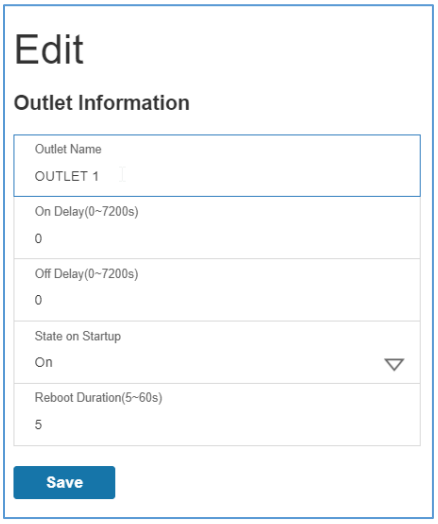


Figure 22: Outlet Naming, Time Delay, State on Startup or Reboot

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.

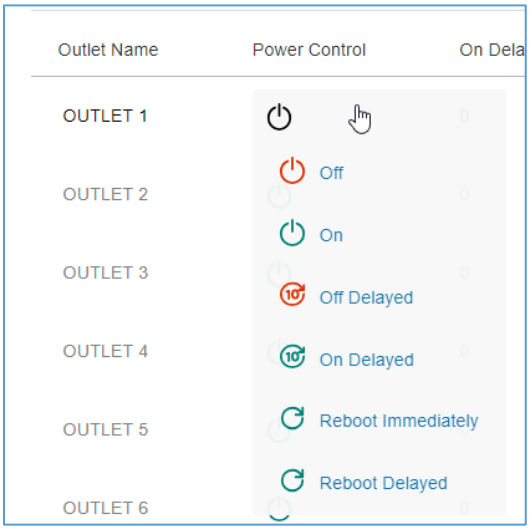


Figure 23: Outlet Control

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**.

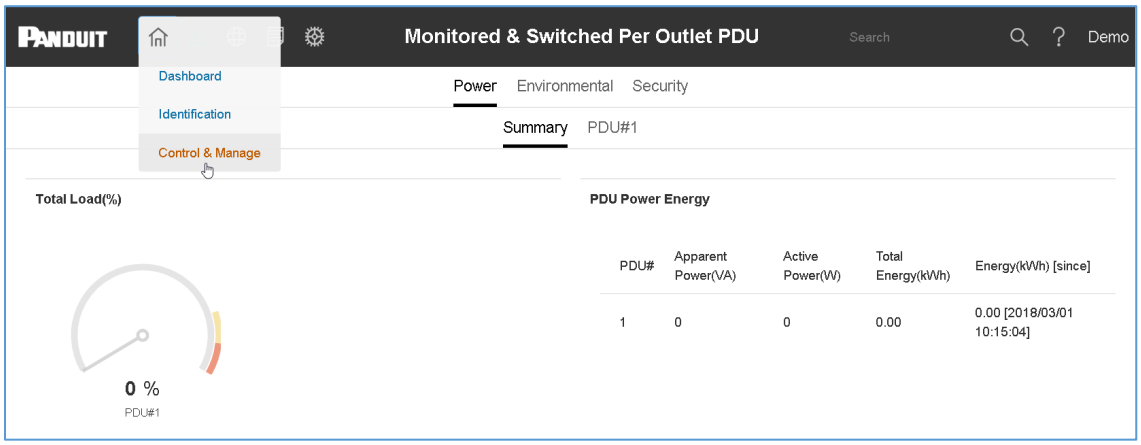


Figure 24: Control & Manage PDU

2. Select Outlet Control Enabled.

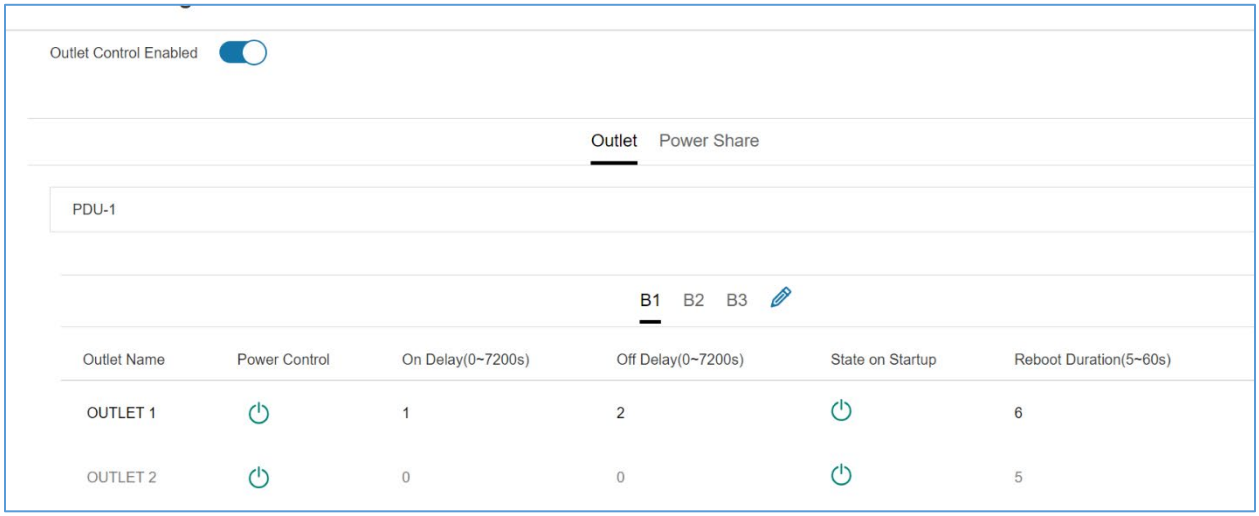


Figure 25: Outlet Control Enabled

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

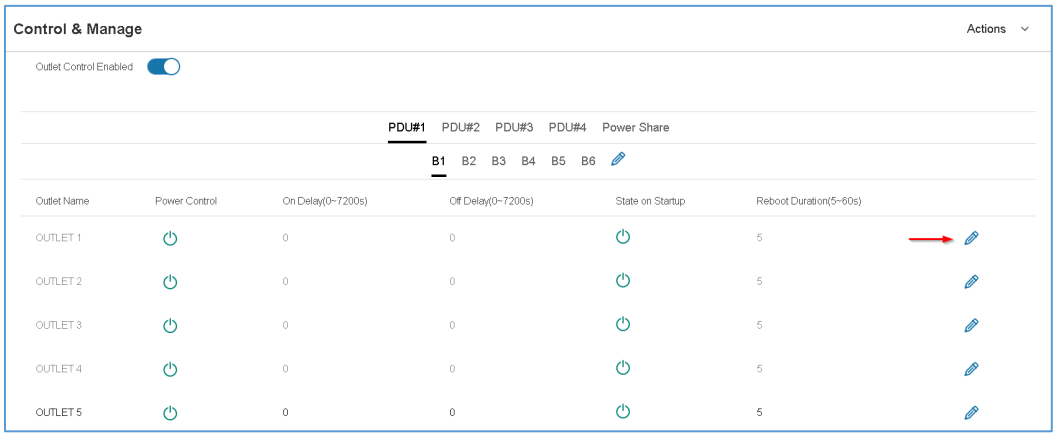


Figure 26: Edit Outlets

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

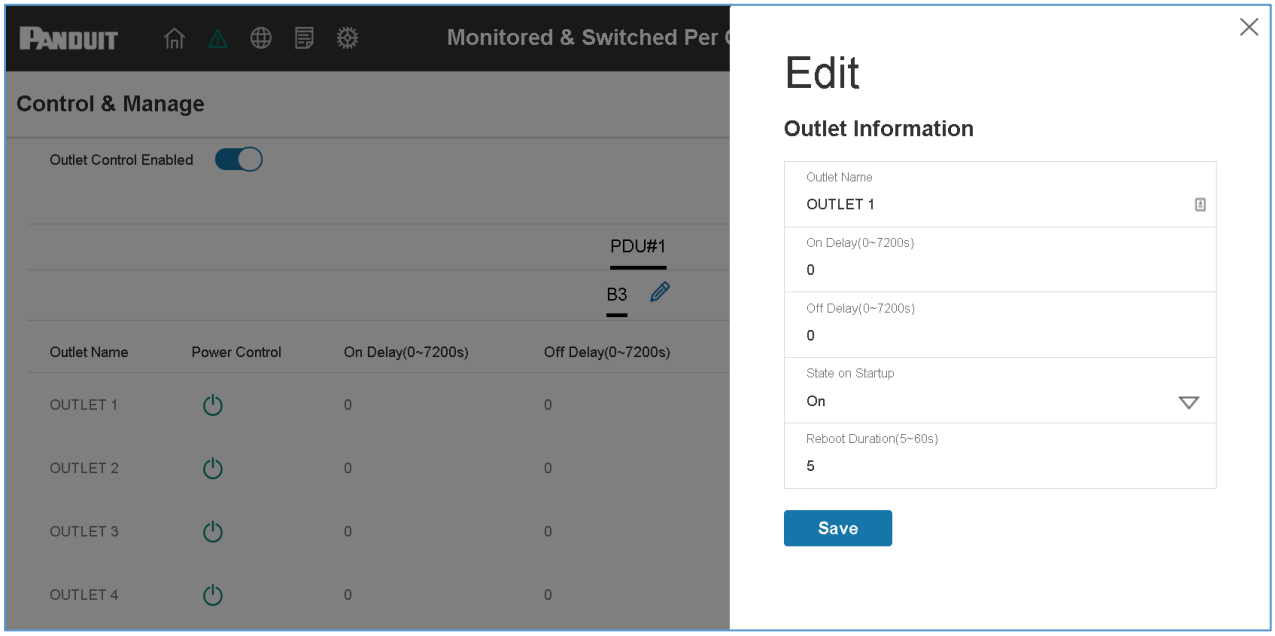


Figure 27: One-Delay Time

5. Your Outlet Power Sequence has been set.

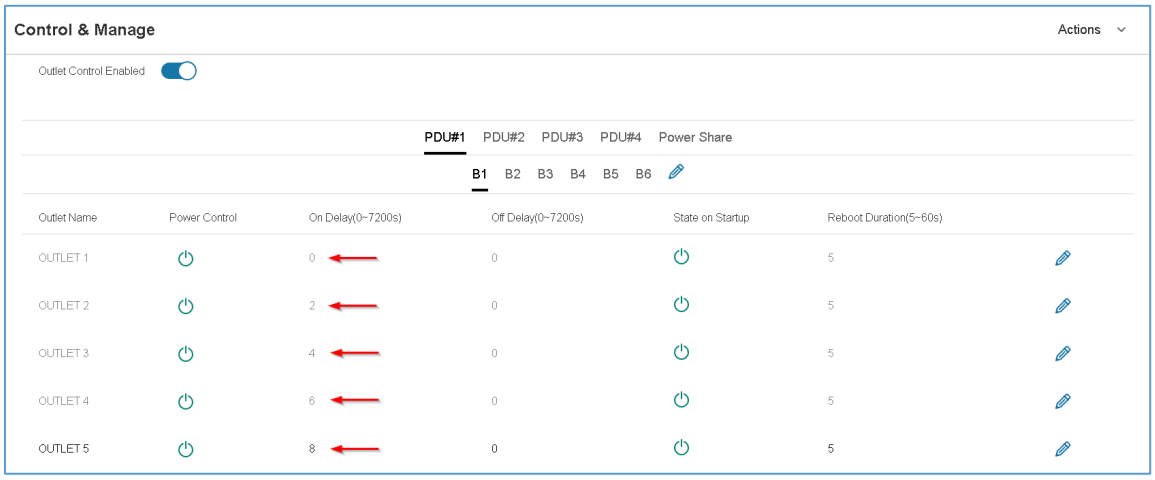


Figure 28: Saved Sequence

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.

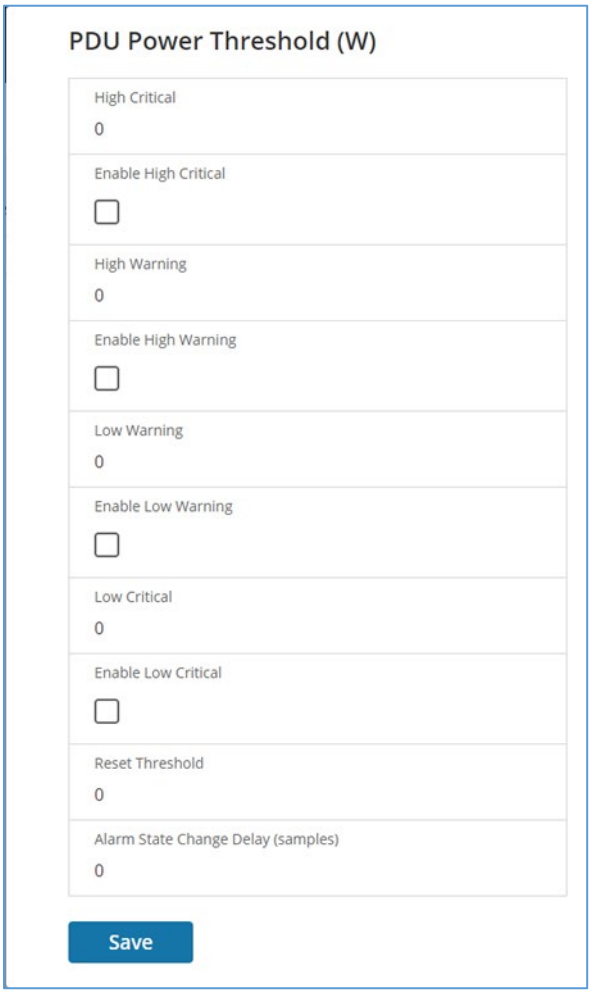


Figure 29: Power Threshold

3. Select and enter the appropriate thresholds in amps and click **Save**.
4. Lower Critical (W)
5. Lower Warning (W)
6. Upper Warning (W)
7. Upper Critical (W)
8. 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.

9. 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.

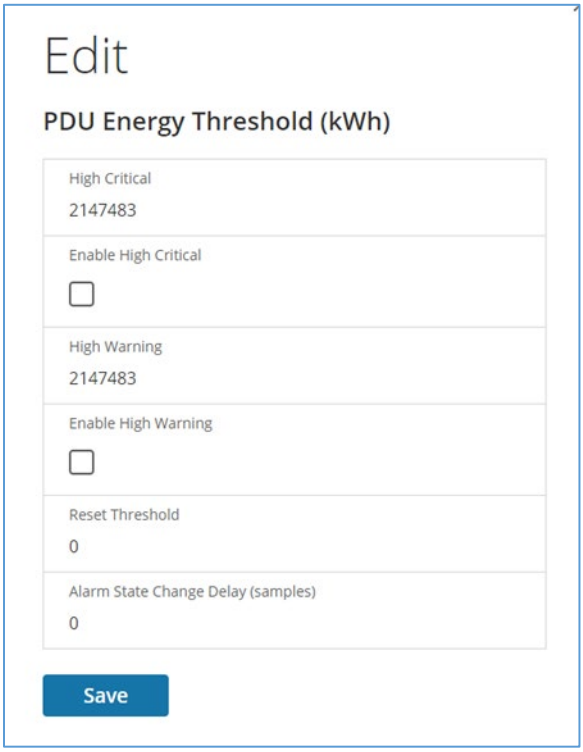


Figure 30: Energy Threshold

3. Select and enter the appropriate thresholds in kilowatts and click **Save**.

10. Upper Critical (kWh)

11. Upper Warning (kWh)

12. Reset Threshold (kWh)

13. 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.

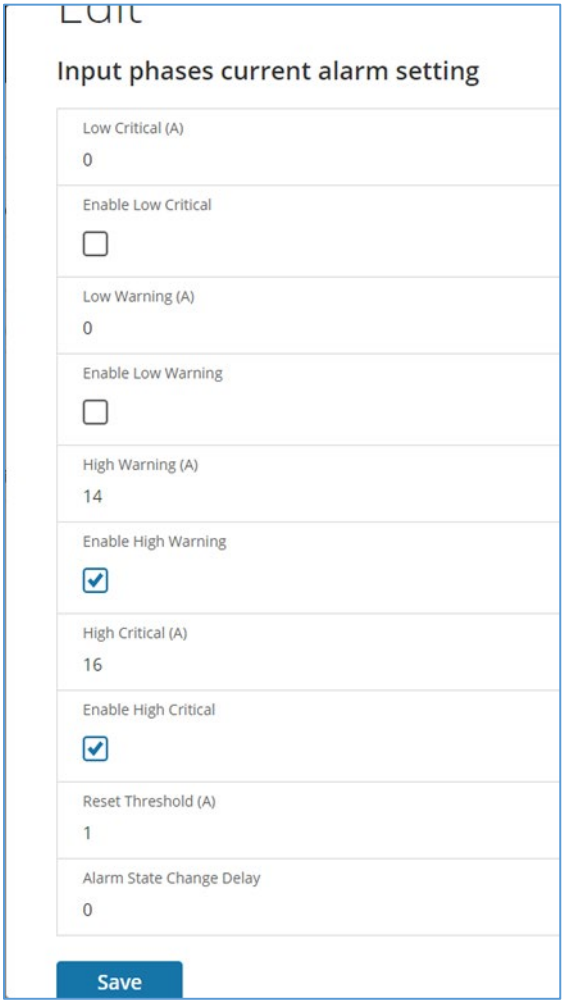


Figure 31: Phase Current Alarm

3. Select and enter the appropriate thresholds in amps and click **Save**.

14. Lower Critical (A)

15. Lower Warning (A)
16. Upper Warning (A)
17. Upper Critical (A)
18. Reset Threshold (A)
19. Alarm State Change Delay (A)

    The Reset threshold is the number of amperes 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.

20. 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.

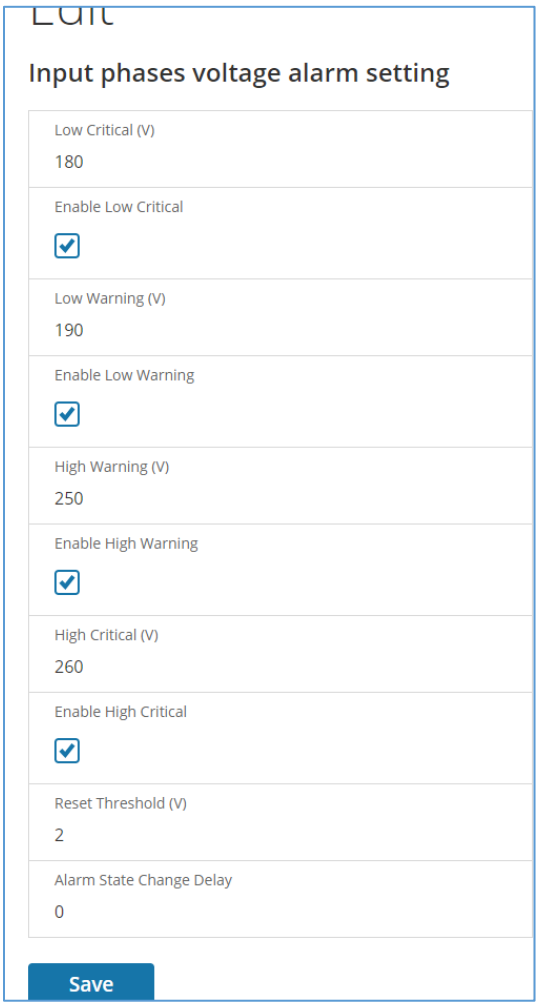


Figure 32: Phase Voltage Alarm

3. Select and enter the appropriate thresholds in voltage and click **Save**.

21. Lower Critical (V)

22. Lower Warning (V)

23. Upper Warning (V)

24. Upper Critical (V)

25. 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.

26. 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.

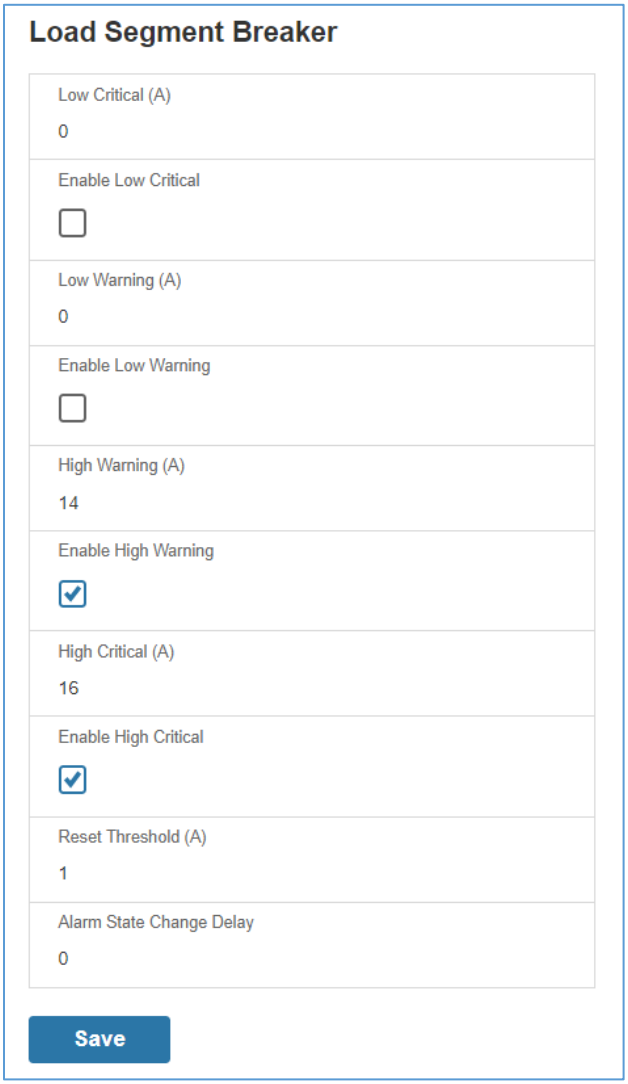


Figure 33: Load Segment Breaker

3. Select and enter the appropriate thresholds in amps and click **Save**.

27. Lower Critical (A)
28. Lower Warning (A)
29. Upper Warning (A)
30. Upper Critical (A)
31. 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.

32. 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**.

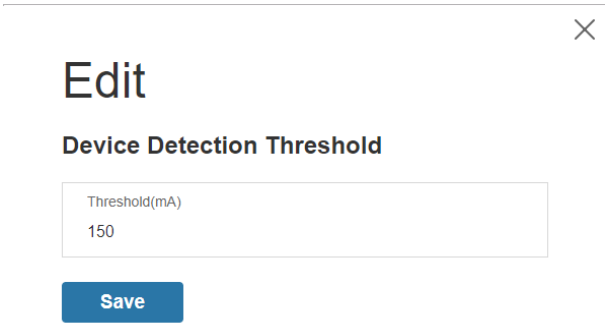


Figure 34: Device Detection Threshold Information

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.

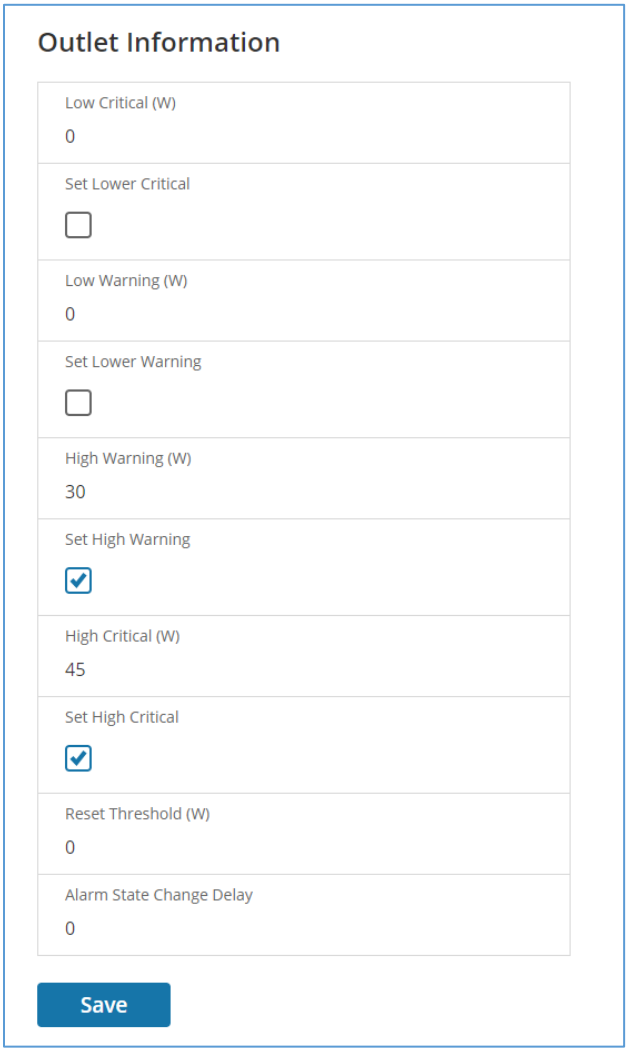


Figure 35: Outlet Information

3. Select and enter the appropriate thresholds in amps and then click Save.

33. Lower Critical (W)
34. Lower Warning (W)
35. Upper Warning (W)
36. Upper Critical (W)
37. 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.

38. 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**.

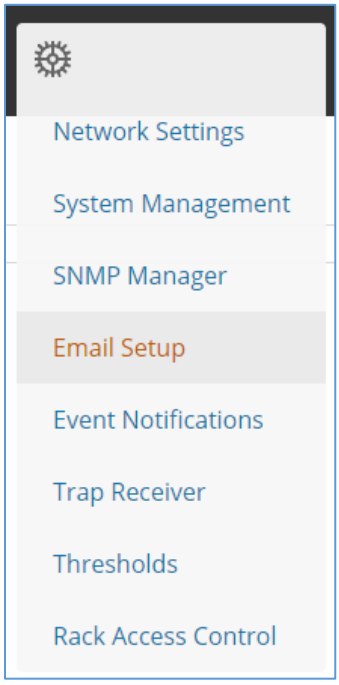


Figure 36: Email Setup

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

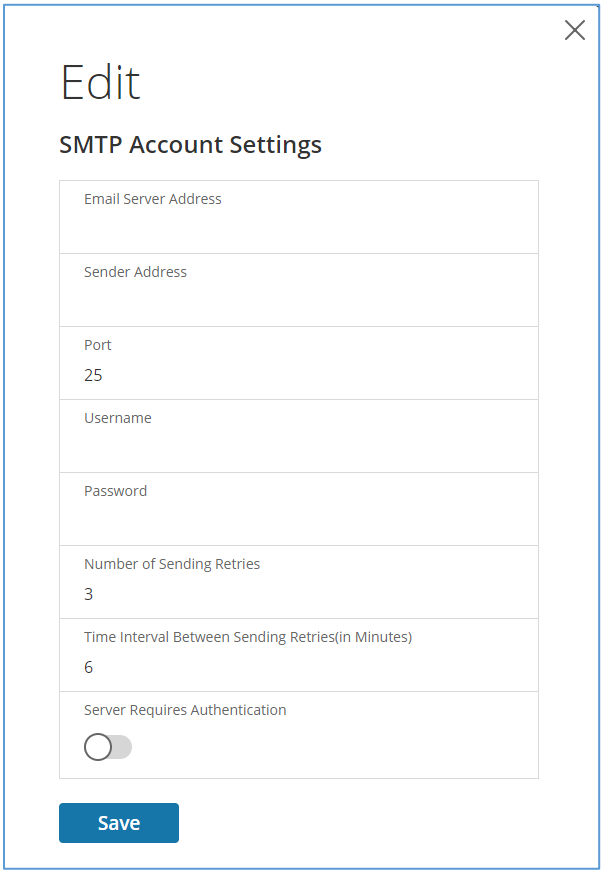


Figure 37: SMTP Account Settings

39. Set the **Email Server Address**. This is the IP address of the SMTP that is going to accept the messages.
40. 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.
41. 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
42. 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.
43. 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.

44. 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.

45. 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.

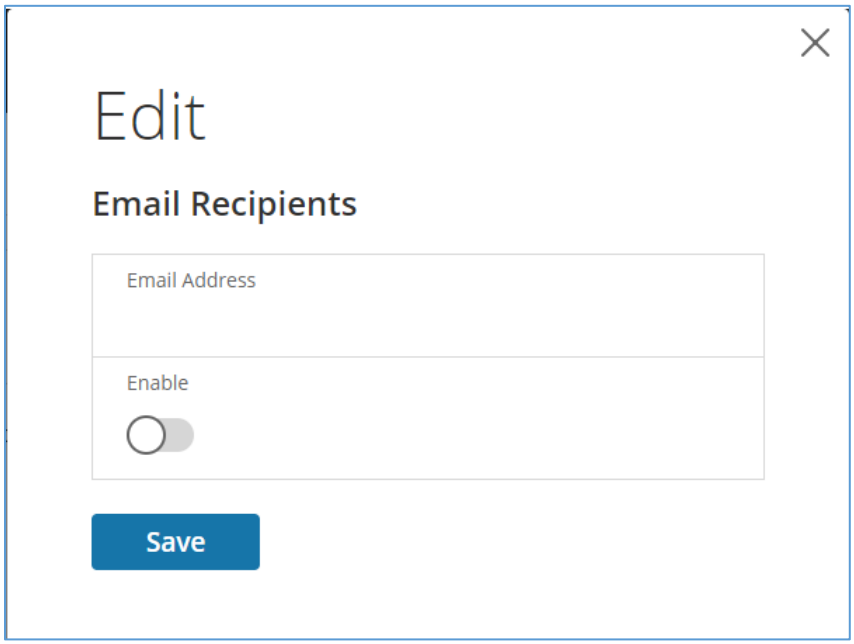


Figure 38: Email Recipients

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 G6 iPDU can be configured to provide event notifications.

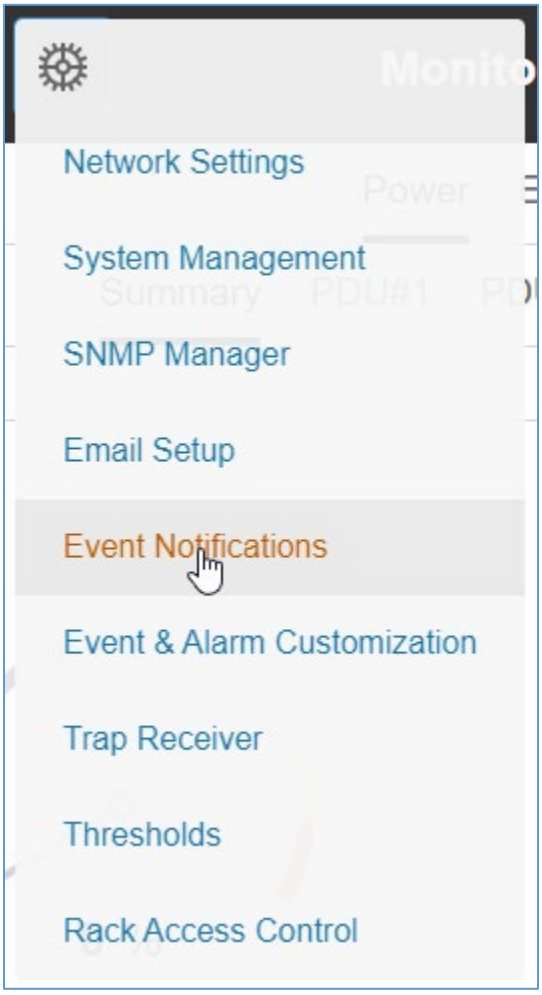


Figure 39: Event Notifications

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**.

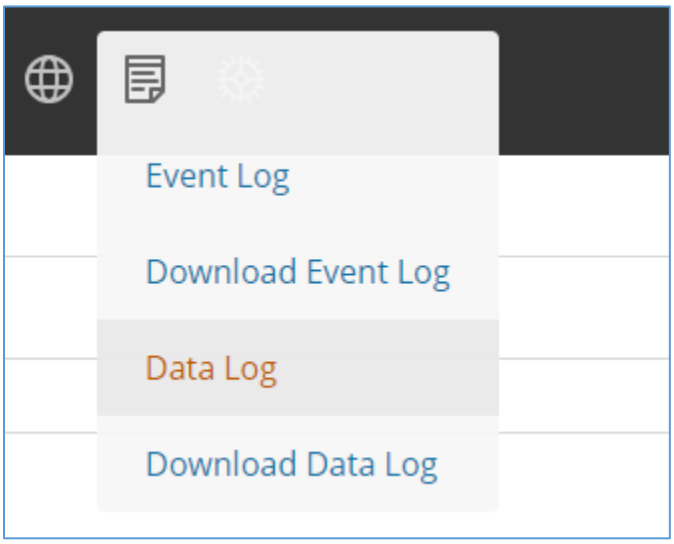


Figure 40: Data Log

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

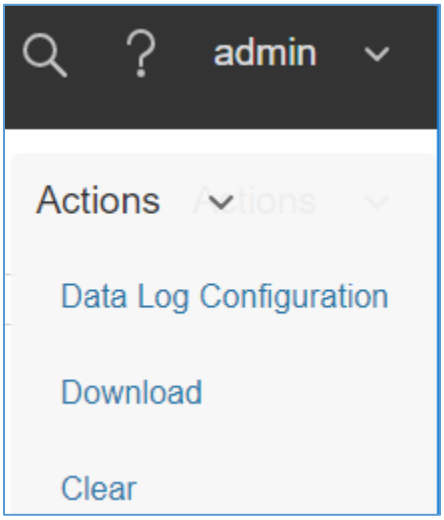


Figure 41: Data Log Configuration

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.

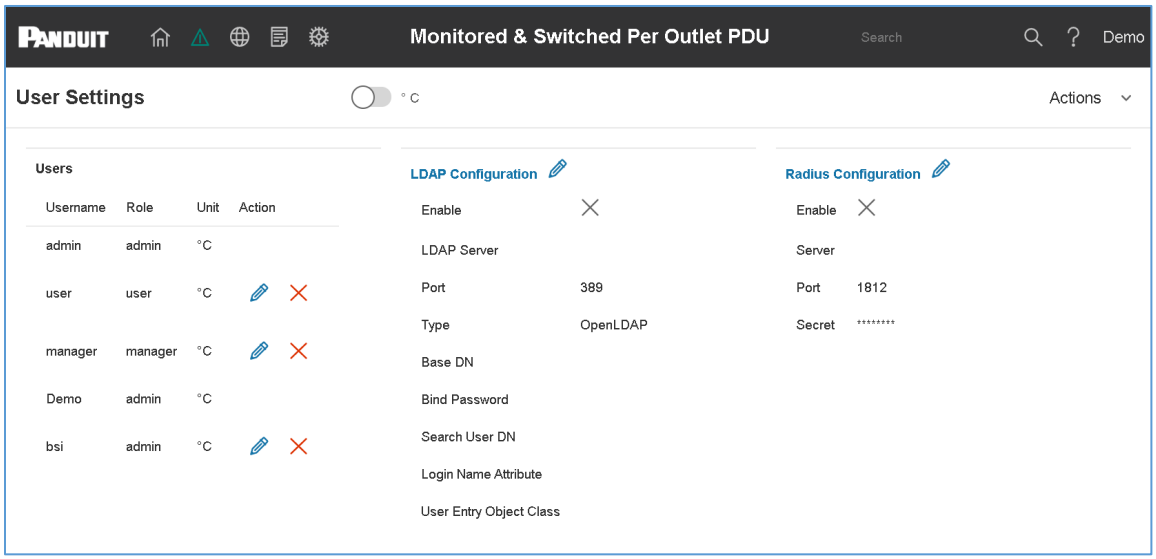


Figure 42: User Settings

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

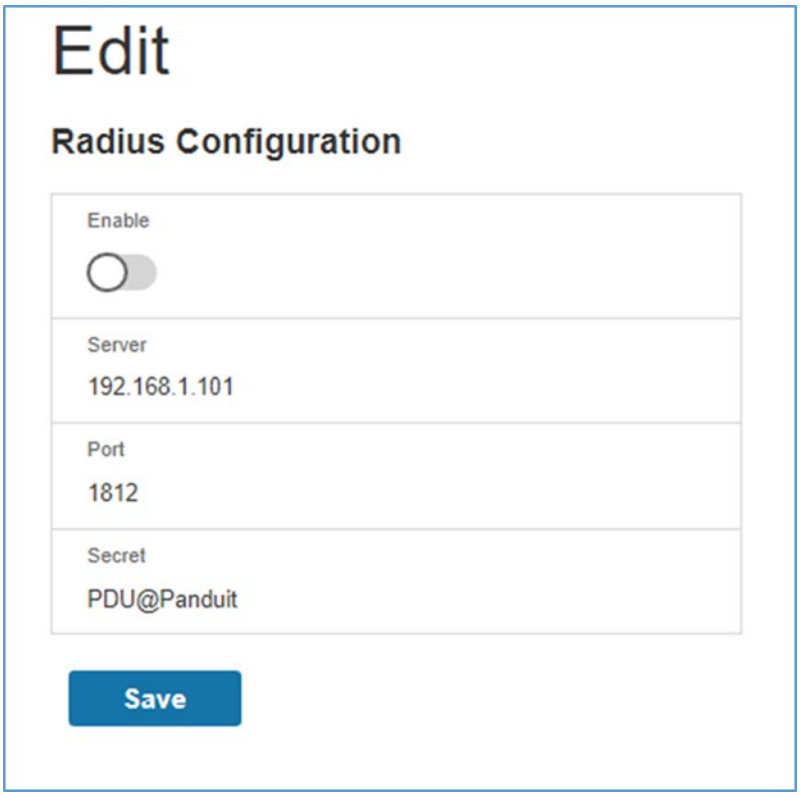


Figure 43: RADIUS Configuration

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.

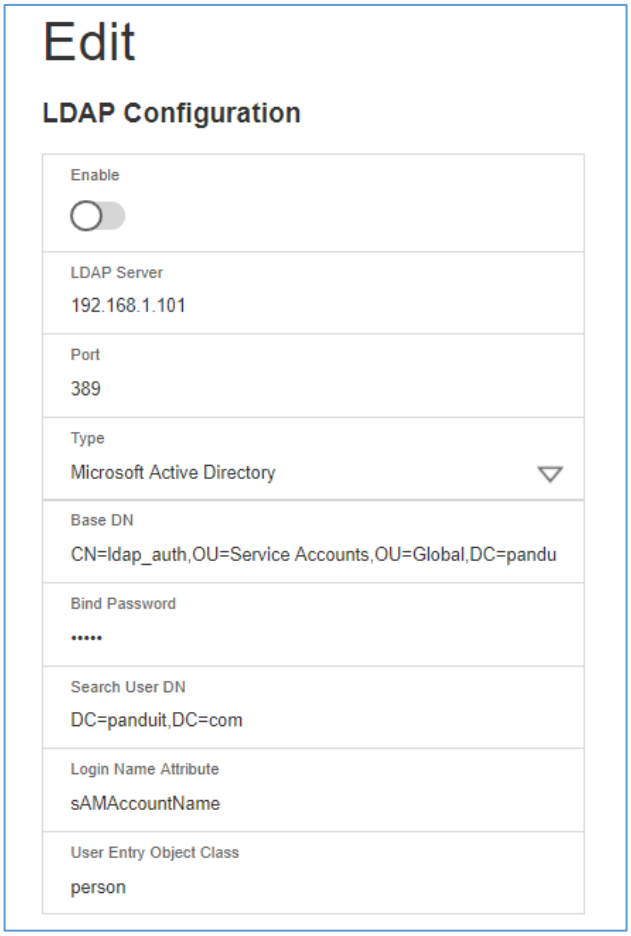


Figure 44: LDAP Configuration

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).

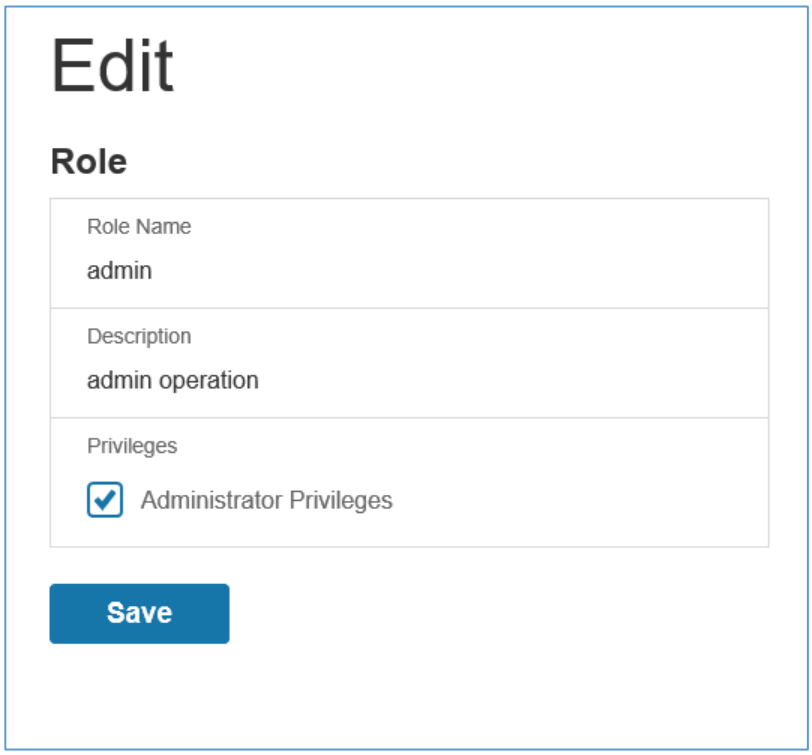


Figure 45: Enable Role Privileges

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.

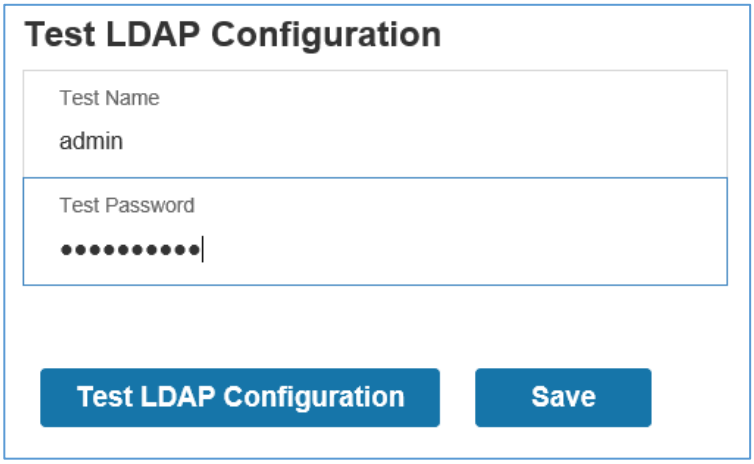


Figure 46: Test LDAP Configuration

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.

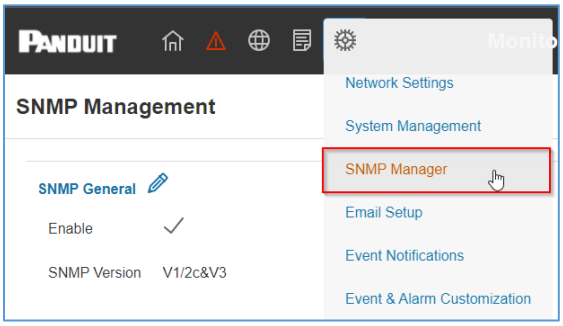


Figure 47: SNMP Management

3. The SNMP General includes SNMP Access and Version.

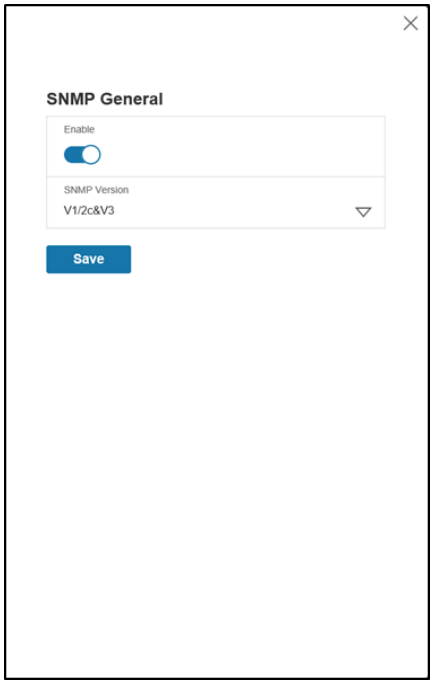


Figure 48: SNMP General

Setup SNMP Port

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

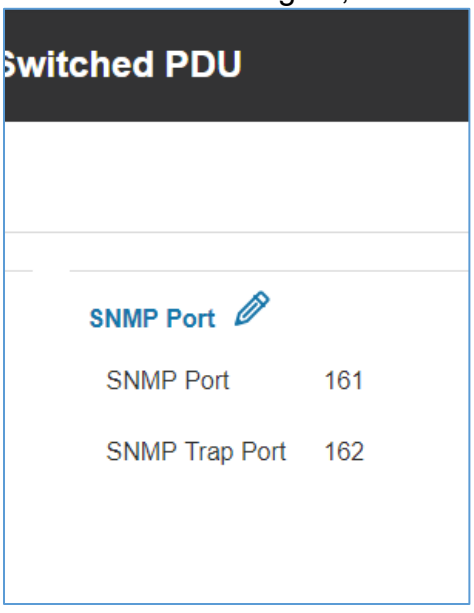


Figure 49: SNMP Port

3. Set up SNMP Port and SNMP Trap Port.

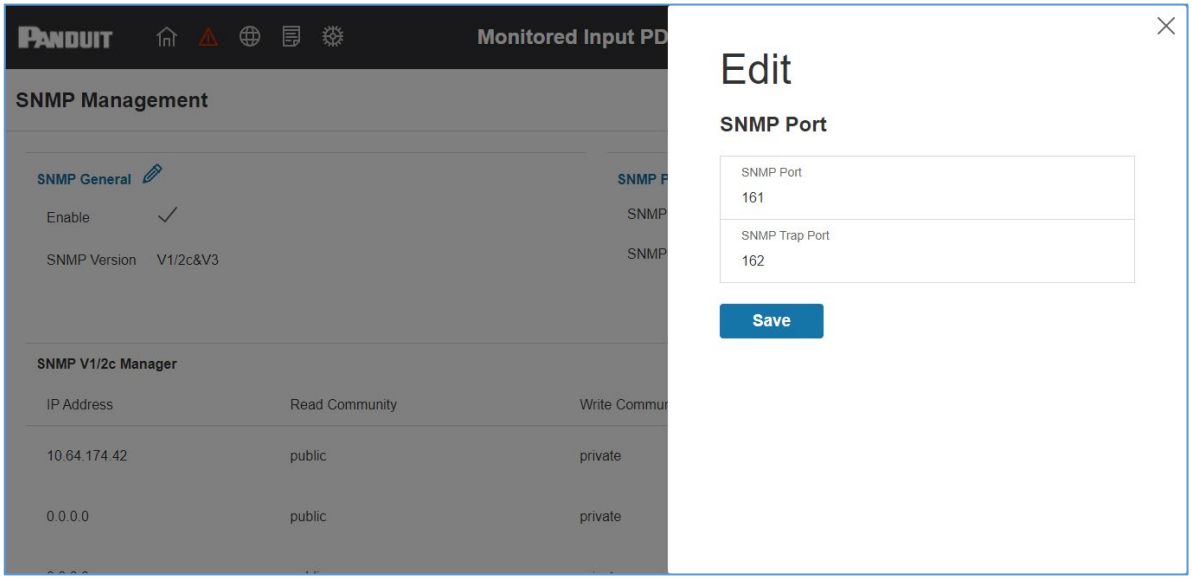


Figure 50: Setup SNMP Port and Trap Port

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 51: Define SNMP V1/V2c User

4. The Edit panel pop up displays.

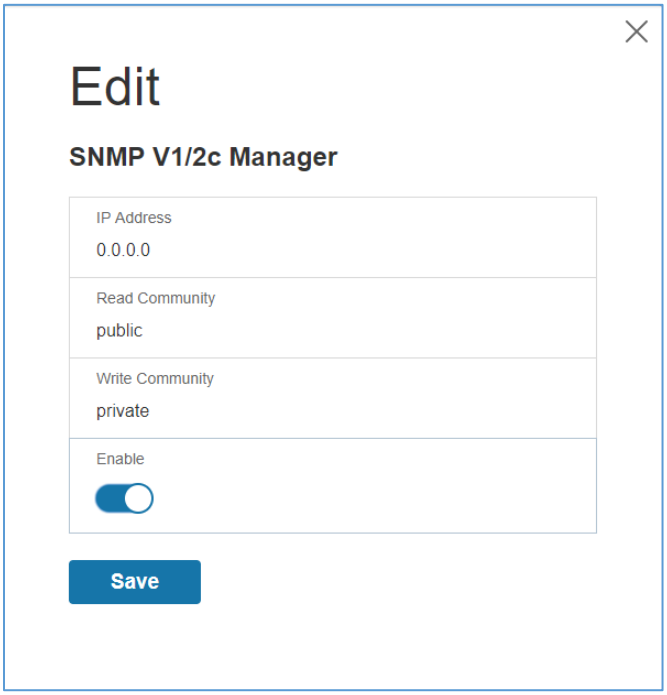


Figure 52: Edit V1/2c Manager

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.

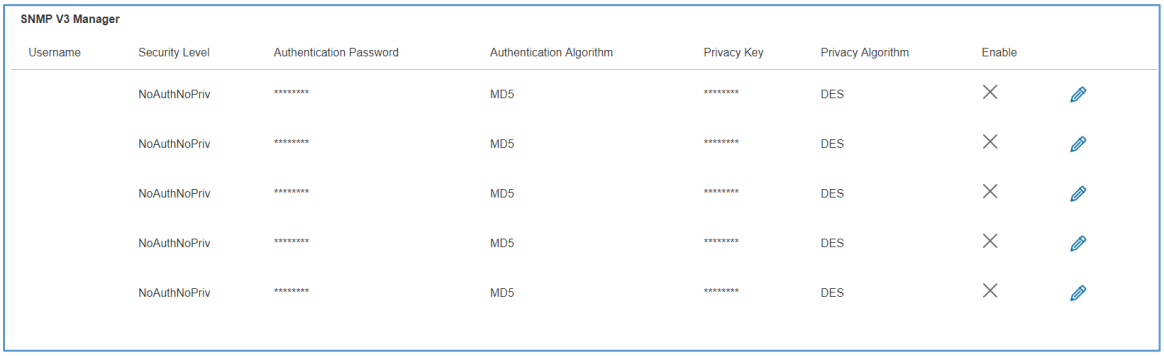


Figure 53: SNMP V3 Manager

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

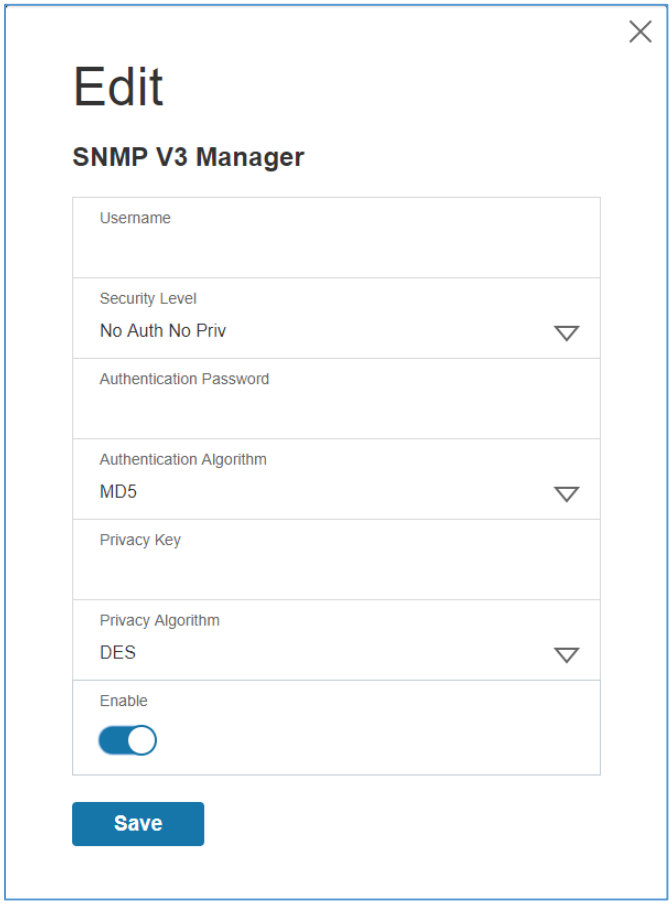


Figure 54: SNMP V3 Edit

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.

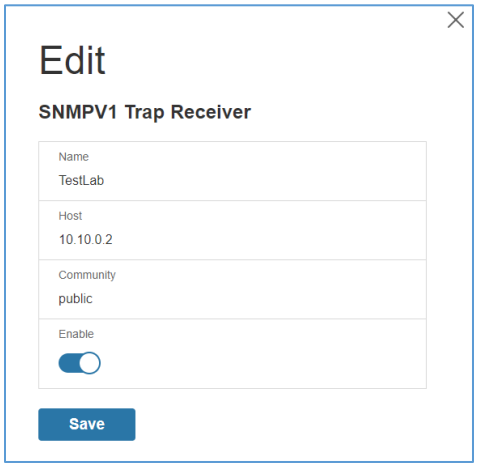


Figure 55: SNMPv2 Configuration Information

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.

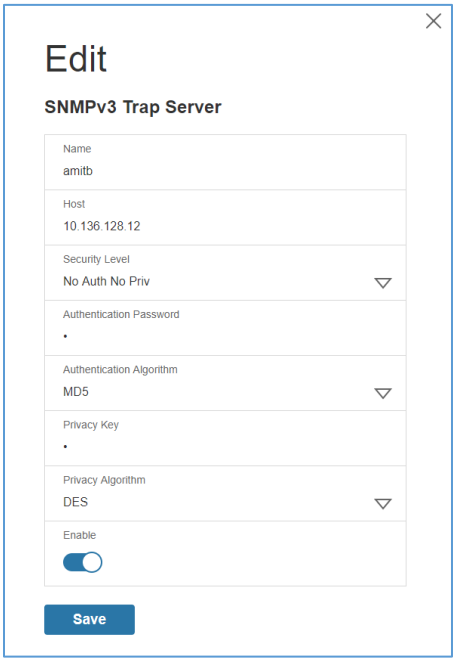


Figure 56: SNMPv3 Trap Server Information.

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.

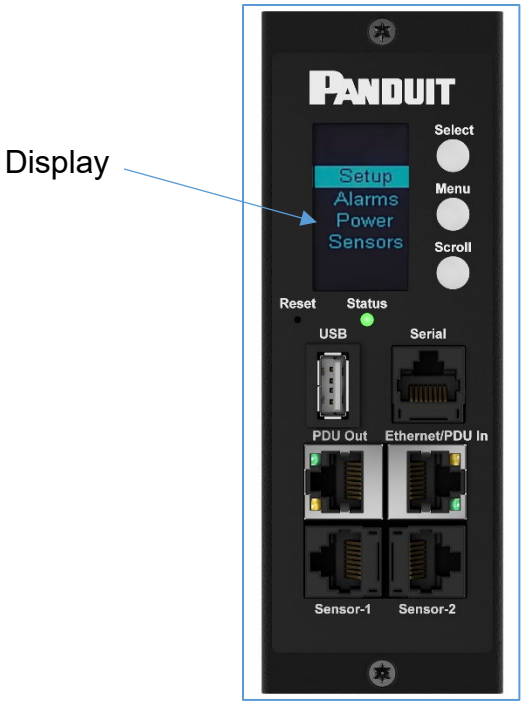


Figure 57: Network Controller

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

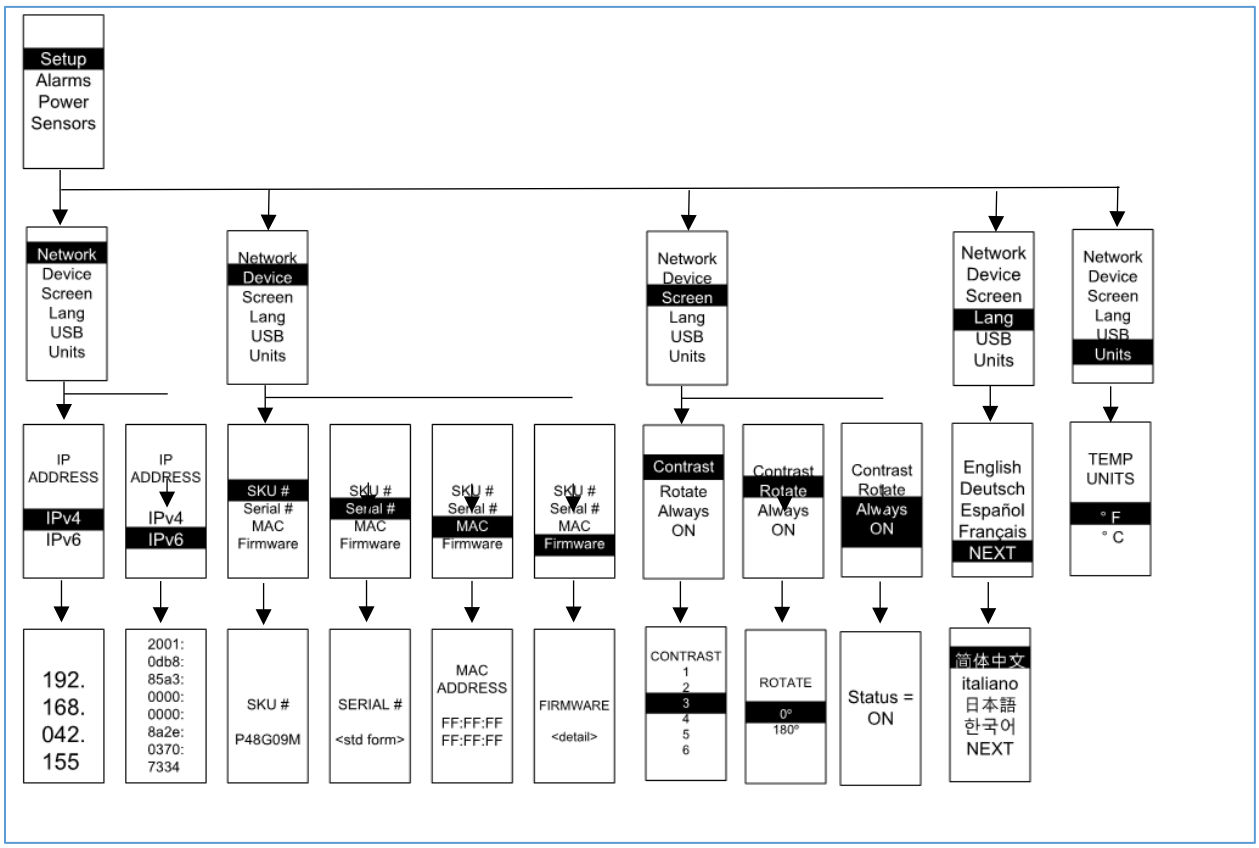


Figure 58: Network Controller Menu Structure

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.

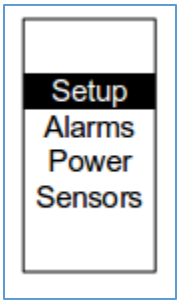


Figure 59: Main Menu Selections

Setup Menu

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

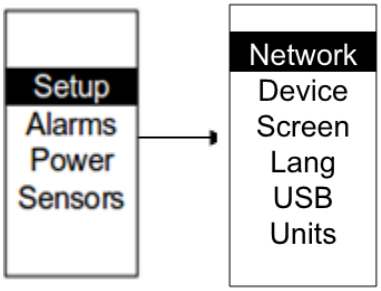


Figure 60: Setup Menu

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.

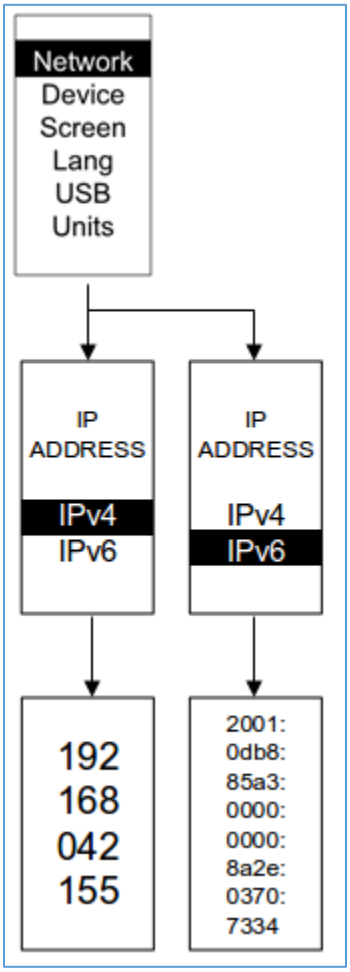


Figure 61: Network Submenu

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.

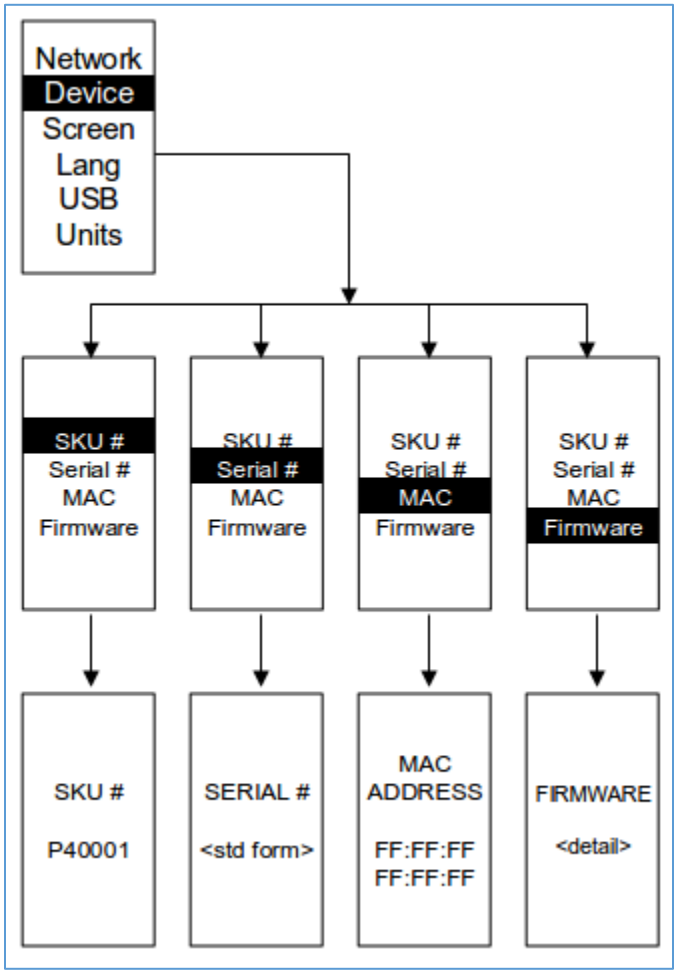


Figure 62: Device Submenu

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.

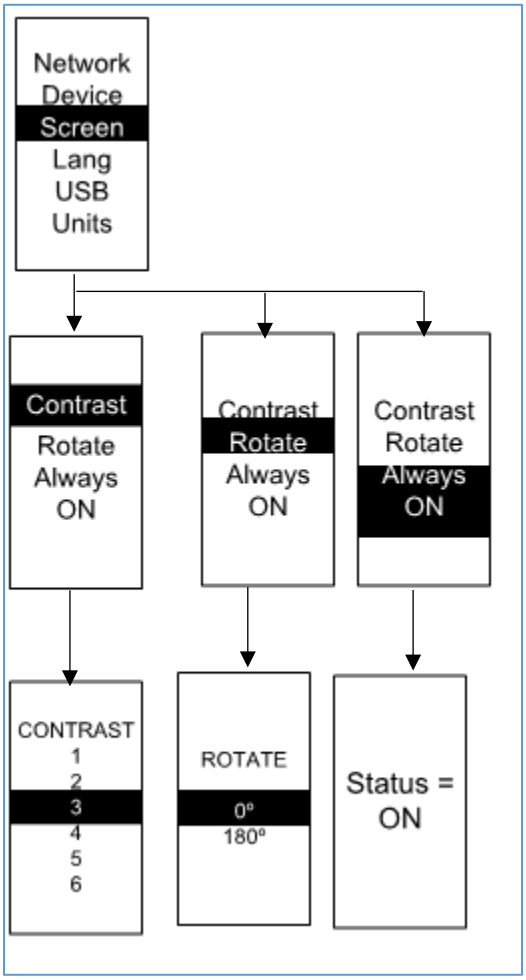


Figure 63: Screen Submenu

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 64: 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.

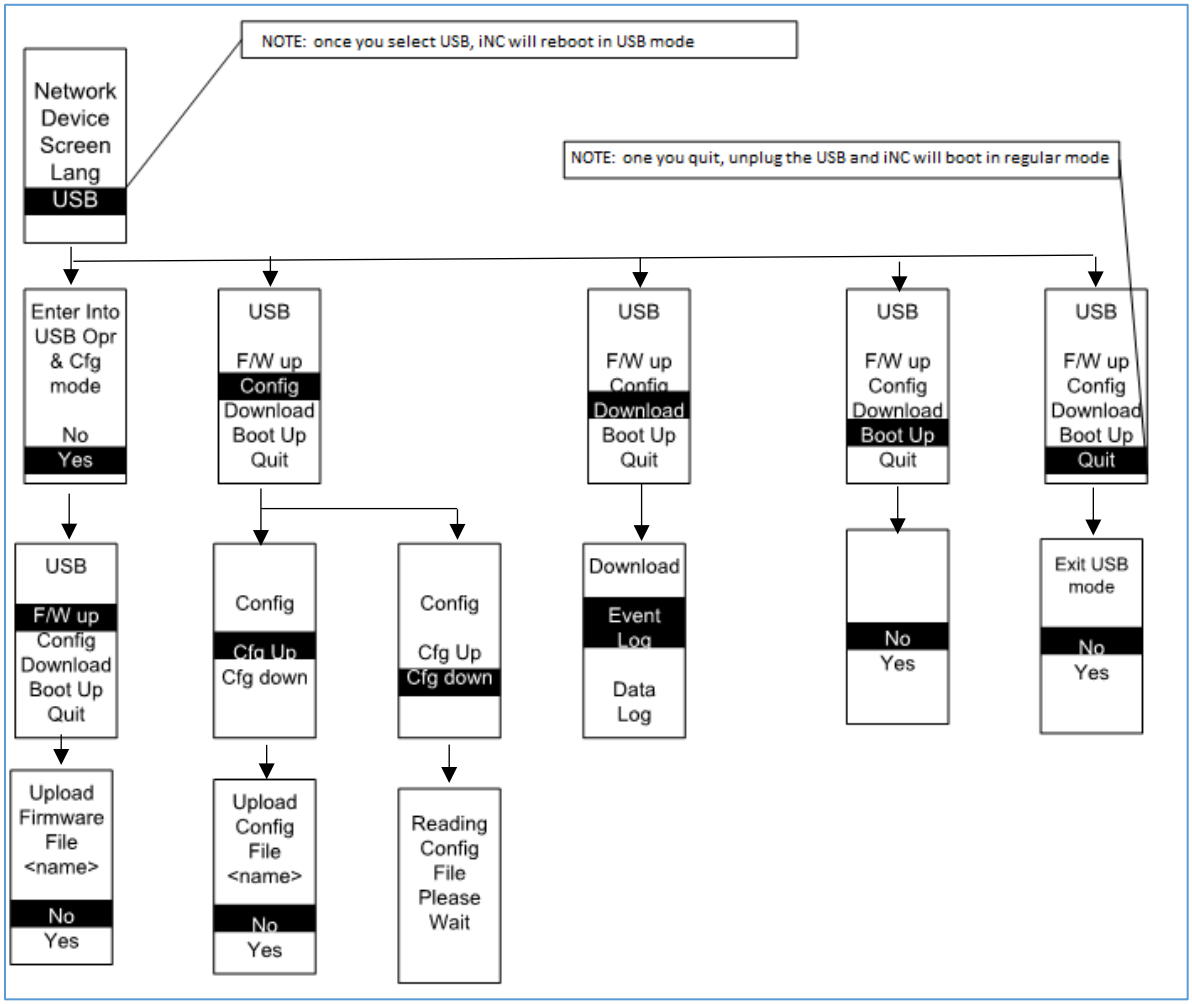


Figure 65: USB Submenu

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.

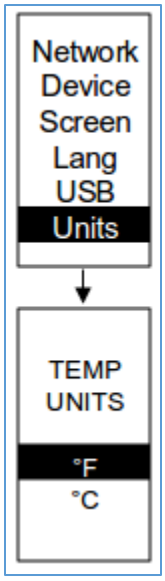


Figure 66: Units Submenu

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.

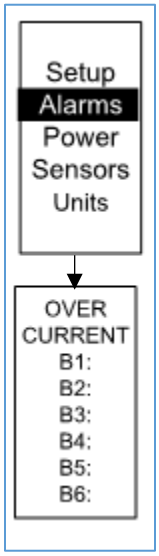


Figure 67: Alarms Menu

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.

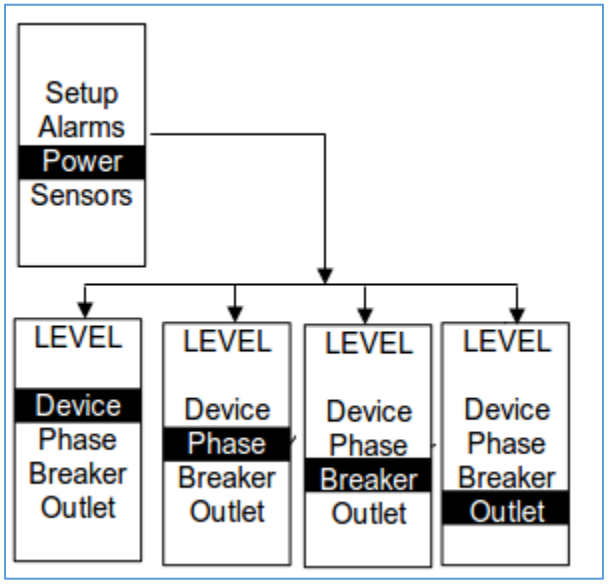


Figure 68: Power Menu

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.

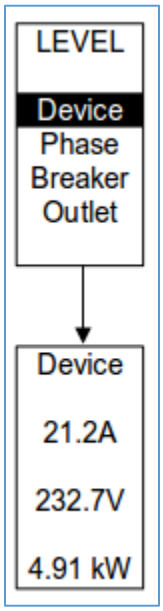


Figure 69: Device Submenu

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.

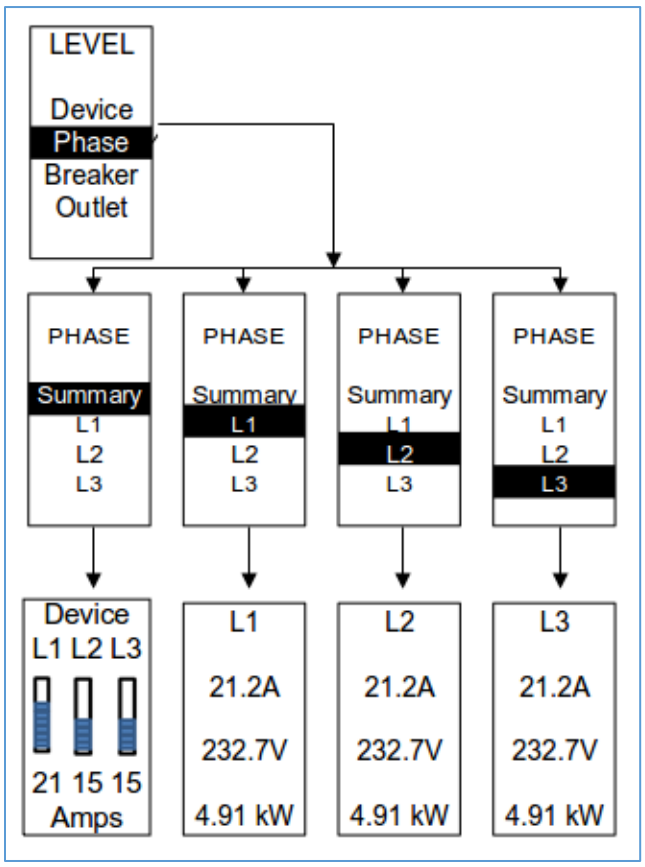


Figure 70: Phase Submenu

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.

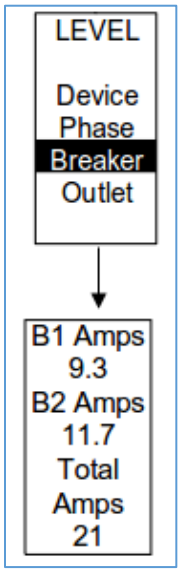


Figure 71: Breaker Submenu

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.

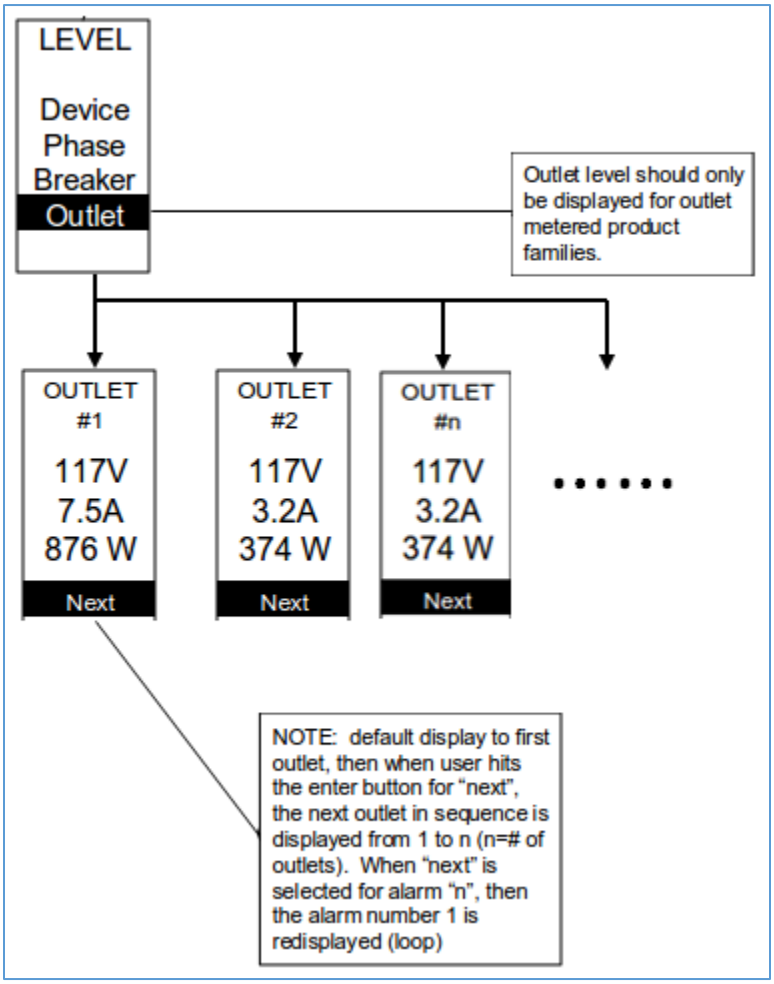


Figure 72: Outlet Submenu

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.

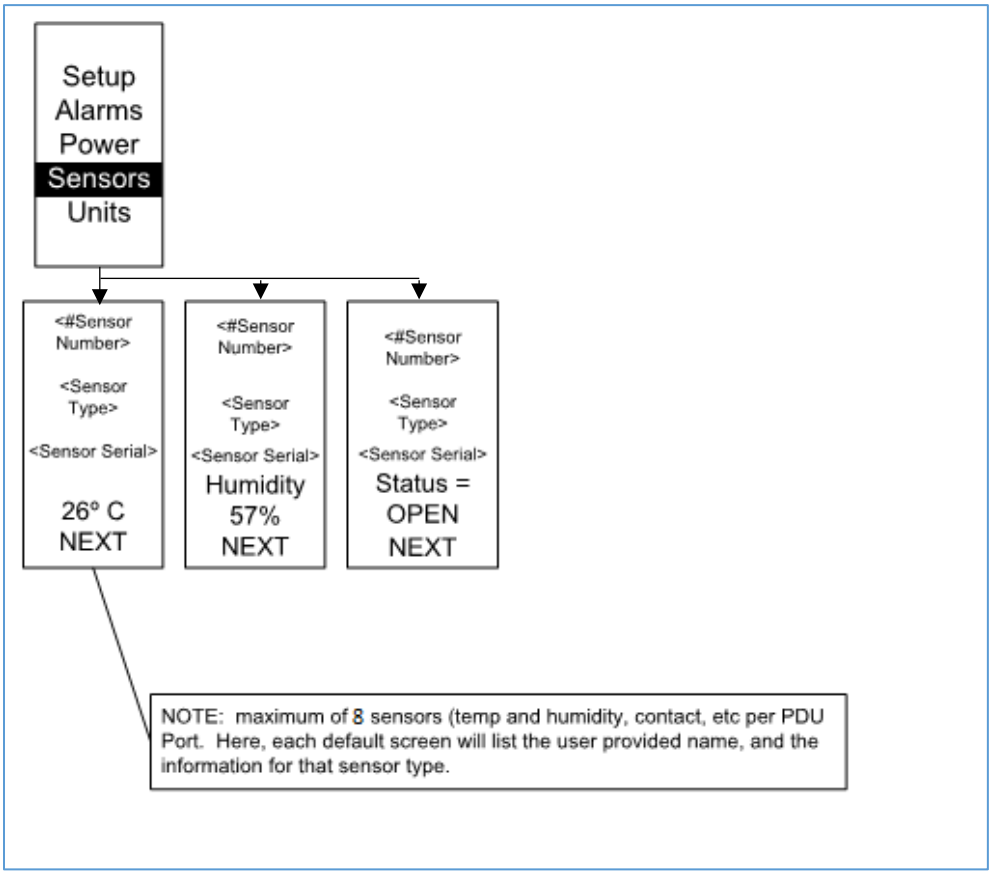


Figure 73: Sensors

NOTE: Maximum of 8 sensors are configured per PDU.

Section 5 – Daisy Chain Configuration

Daisy-Chain Overview

In daisy chain mode, up to (32) 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.

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 **Ethernet/PDU In** port on the second PDU in the daisy chain line.
2. Repeat step 1, connecting PDUs from the **PDU Out** port to the **Ethernet/PDU In** port.

   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.

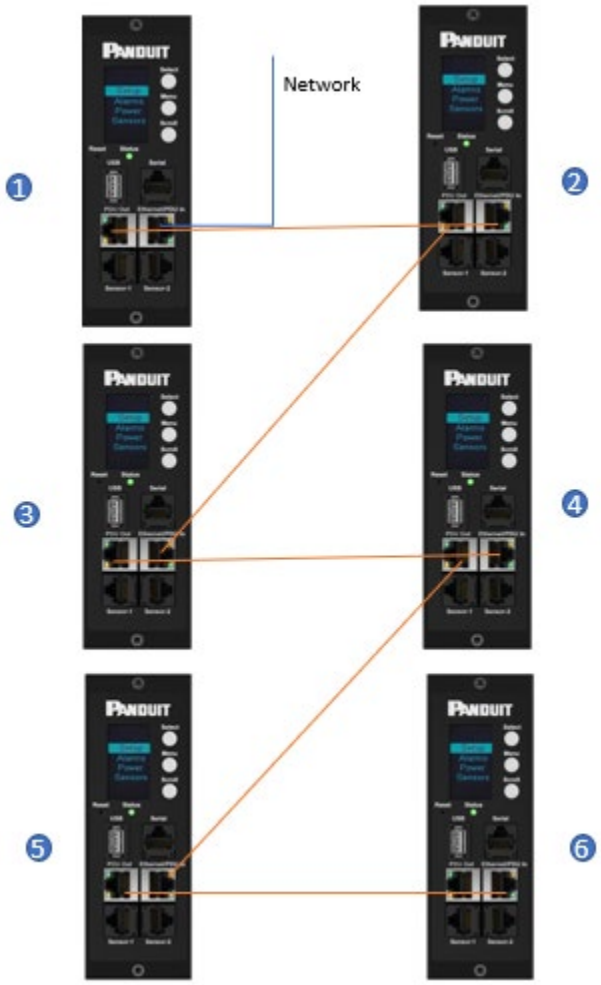


Figure 74: Connection Diagram 6 PDU Daisy Chain

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.

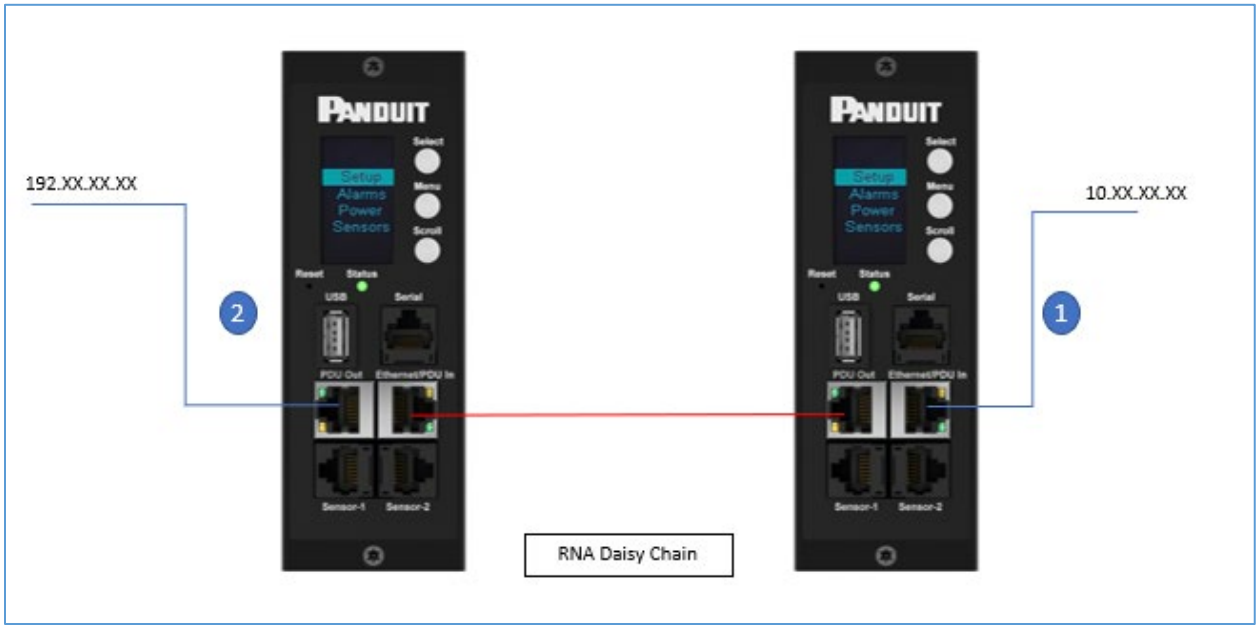


Figure 75: Connection Diagram RNA Daisy Chain

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.
   a. Connect an Ethernet cable from the **PDU In/Serial** port on first PDU to the **PDU Out** port on the second PDU.
3. Connect another Ethernet cable from the **PDU Out** port on the first PDU to the **PDU In/Serial** port on the second PDU.
4. 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.
5. To enable this account, login to the CLI with admin credentials.
6. Enter the command ‘**dev daisy rna init**’.
7. The following message will appear to confirm the landlord account is enabled: SUCCESS.
8. RNA is now configured and enabled.

Power Share

Power Share is designed to allow for continual sensor monitoring and electronic rack access if (1) 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 Intelligent Rack 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.

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.

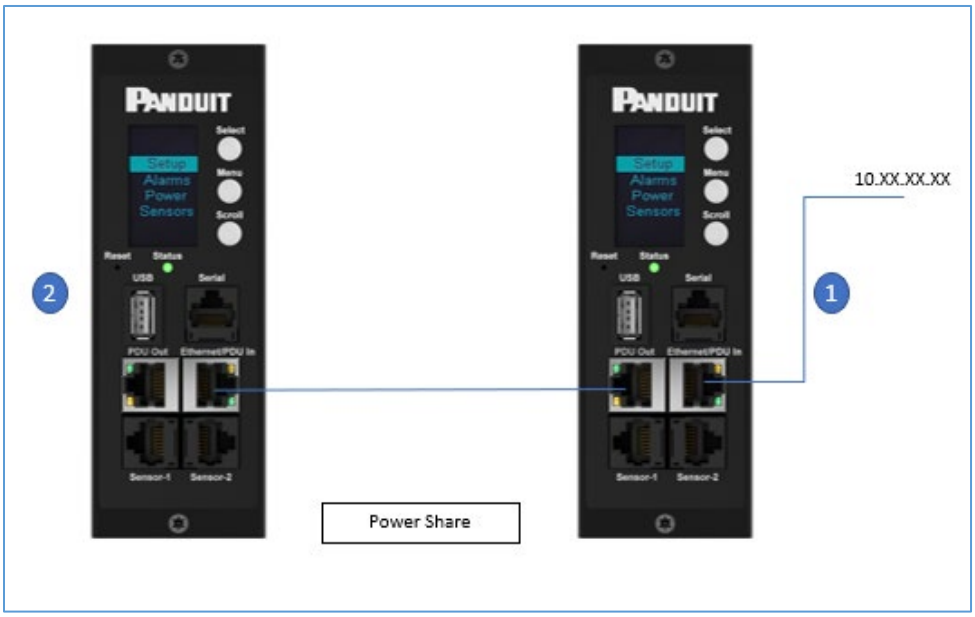


Figure 76: Connection Diagram Power Share & Daisy Chain

Section 6 – Intelligent Rack Security Handle

The Panduit Intelligent PDUs allow users to electronically secure and control access to cabinets. 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 77: Intelligent Rack Security Handles

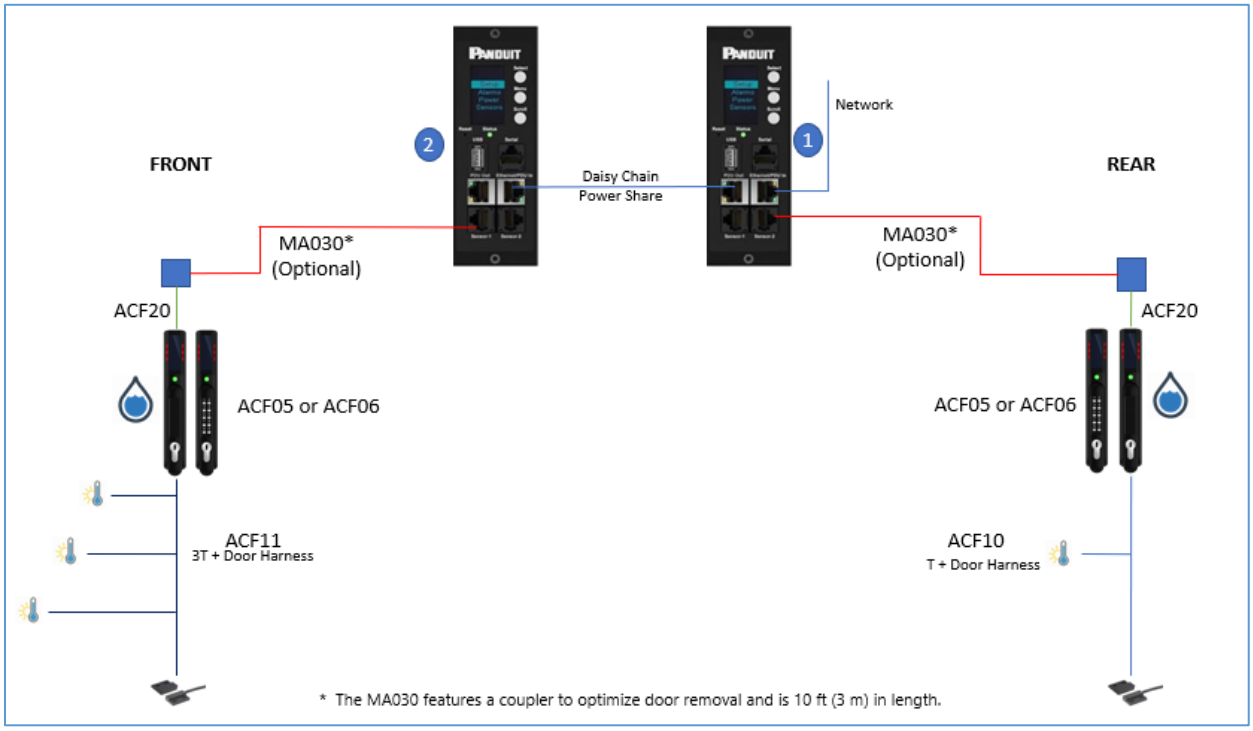


Figure 78: Connection Diagram for Intelligent Rack Security Handle

Note: Specialized sensors were developed for attaching directly to the Intelligent Rack 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 G6 PDU*
ACF06	*2*	*Panduit G6 PDU*
ACF11	*4*	*Panduit G6 Handle*
ACF10	*2*	*Panduit G6 Handle*
ED001	*1*	*Panduit G6 PDU*
EE001	*1*	*Panduit G6 PDU*

ACA01	*1*	*Panduit G6 PDU*
ACC01	*1*	*Panduit G6 PDU*
EA001	*1*	*Panduit G6 PDU*
EB001	*2*	*Panduit G6 PDU*
EC001	*4*	*Panduit G6 PDU*

Note: A maximum of 8 sensors can be managed by the Panduit G6 PDU controller. A maximum of 2 handles can be managed by each individual Panduit G6 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.

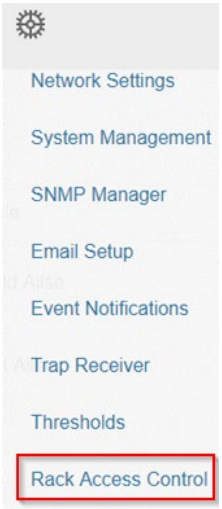


Figure 79: Rack Access Control Web GUI

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.

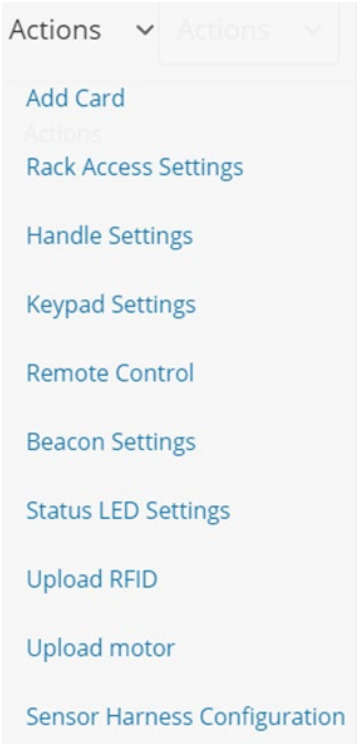


Figure 80: Rack Access Control Actions Web GUI

Adding a User for Local Rack Access

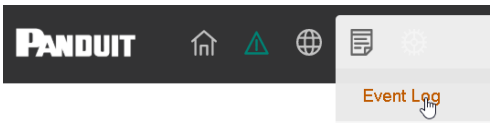
Every user that needs access to the cabinet needs to have their access card added into the PDU. Each card (or user) must have a username and either a card ID or keypad PIN code.

> **Note**: A maximum of 200 cards can be programmed per cabinet. When a user is added to one 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.

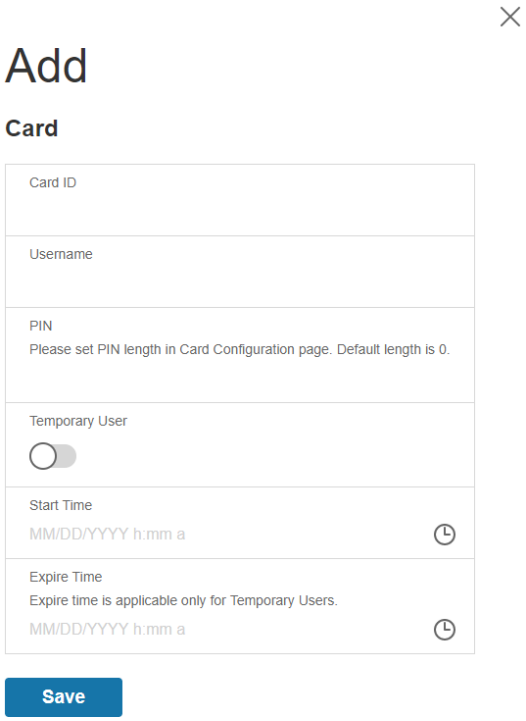


Figure 81: Local Rack Access Web GUI

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.
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.

1. To update the rack access settings, select **Rack Access Settings** from the

Actions menu.

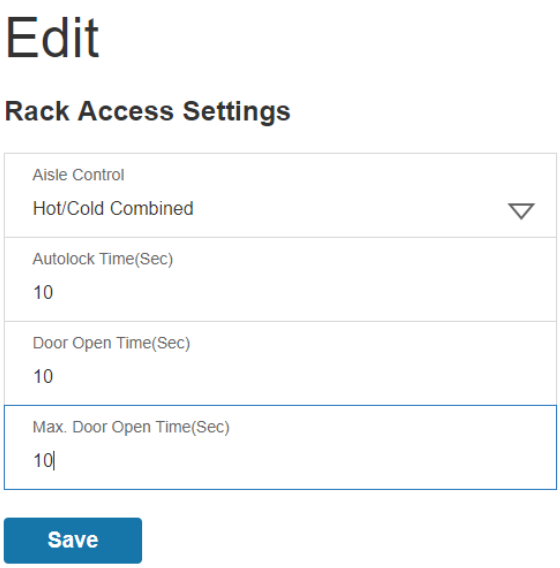


Figure 82: Rack Access Settings Web GUI

2. 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
3. The **AutoLock Time** is the number of seconds after the handle will automatically lock.
4. The **Door Open Time** is the number of seconds after the handle alerts door open
5. The **Max. Door Open Time** is the number of seconds before a critical alarm announces, door open.
6. 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.

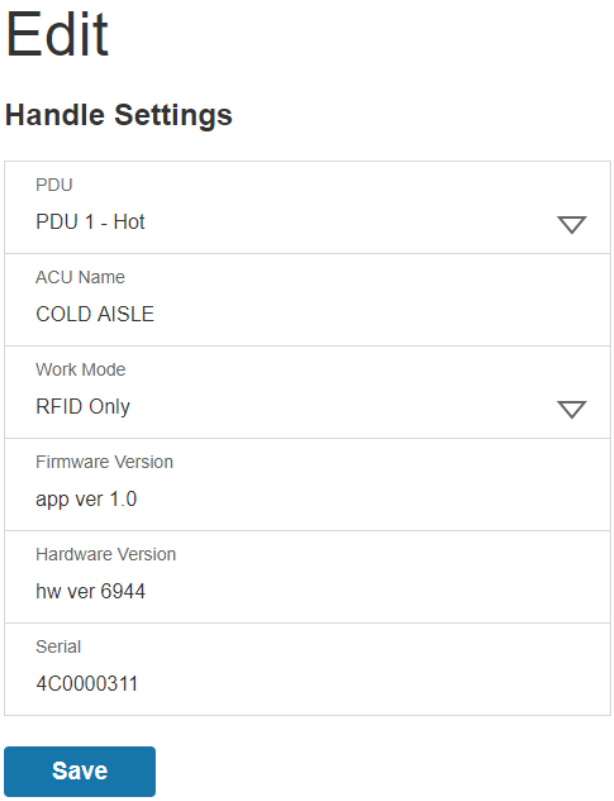
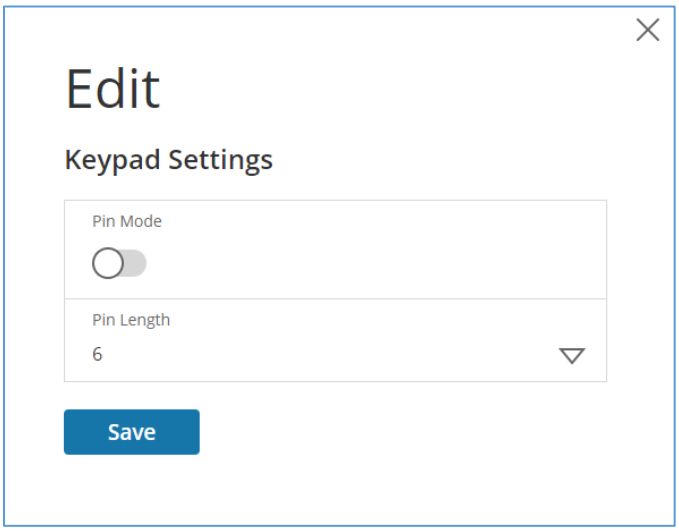


Figure 83: Handle Settings Web GUI

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 Intelligent Rack 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.

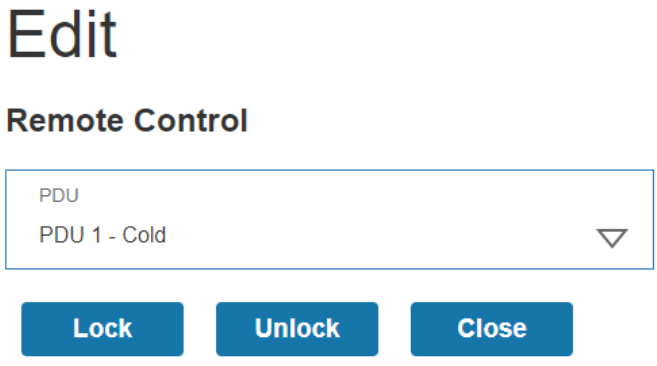


Figure 84: Remote Control

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 85: 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.

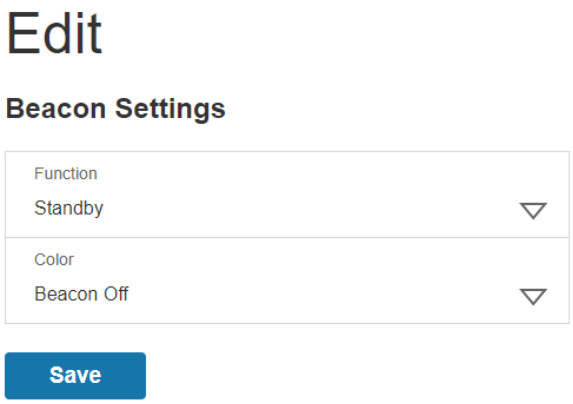
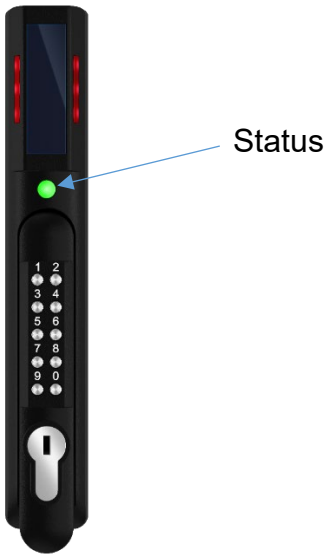


Figure 86: Beacon Settings Web GUI

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 Intelligent Rack 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.

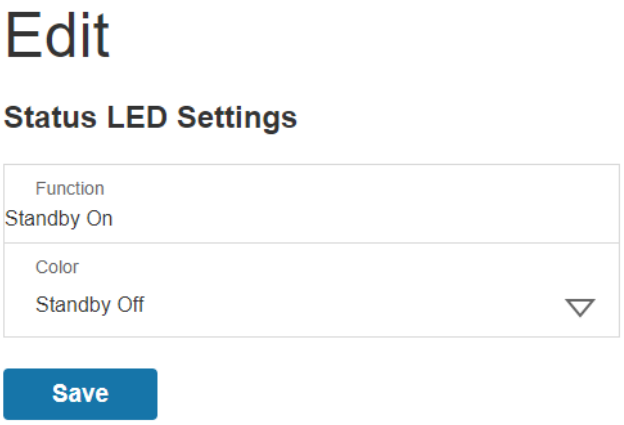


Figure 87: Status LED Settings Web GUI

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 G6 Accessories

Hardware Overview

The Panduit G6 accessories are specially designed to interoperate Panduit G6 iPDU controller. Connecting unapproved sensors to the G6 iPDU controller or connecting Panduit G6 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 G6 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 G6 Dry Contact Sensor (ACC01)	Input to the G6 iPDU and designed to monitor a change in contact state.	1

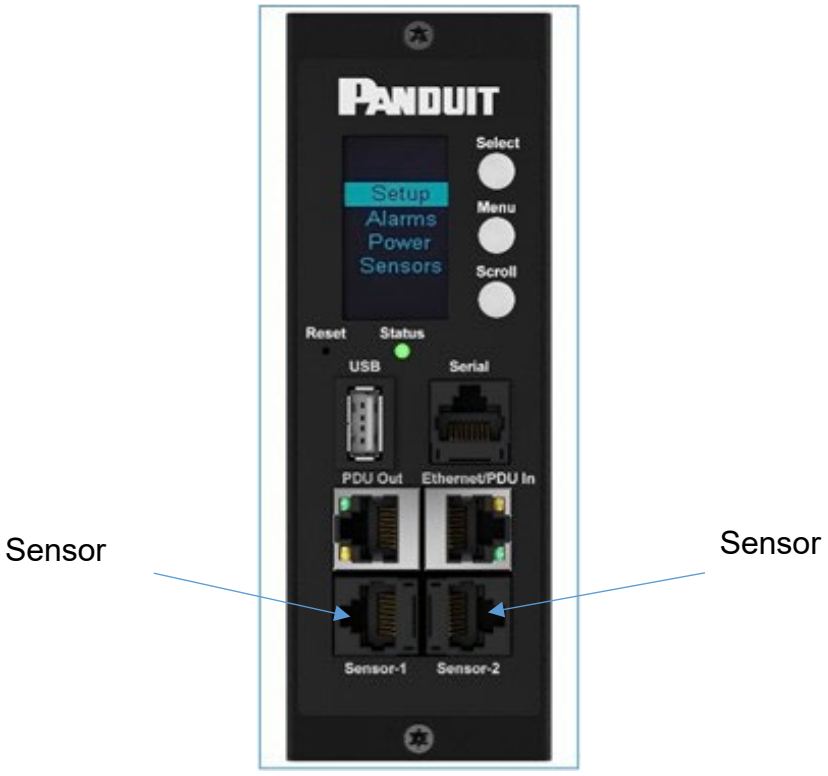


Figure 88: Sensor Ports for Vertical PDU

Configuring Temperature Scale

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

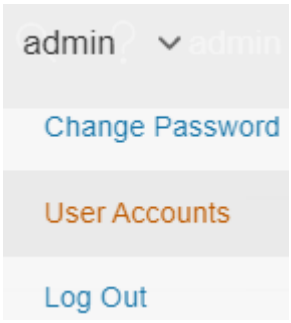
1. Go to User Accounts.
4. 

Figure 89: User Settings

2. The button at the top of the screen can be used to select Celsius or Fahrenheit.
5. 

Figure 90: Celsius Setting

6. 

Figure 91: 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 G6 iNC Controller uses non-volatile storage on the G6 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

https://www.panduit.com/en/legal-information/panduit-limited-product-warranty.html

Regulatory Information

Safety and regulatory compliance

For important safety, environmental, and regulatory information, reference Panduit website:

https://www.panduit.com/en/support/download-center/certifications.html

Panduit Support and Other Resources

Majority of your support needs can be met by visiting Panduit.com → Support. 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.

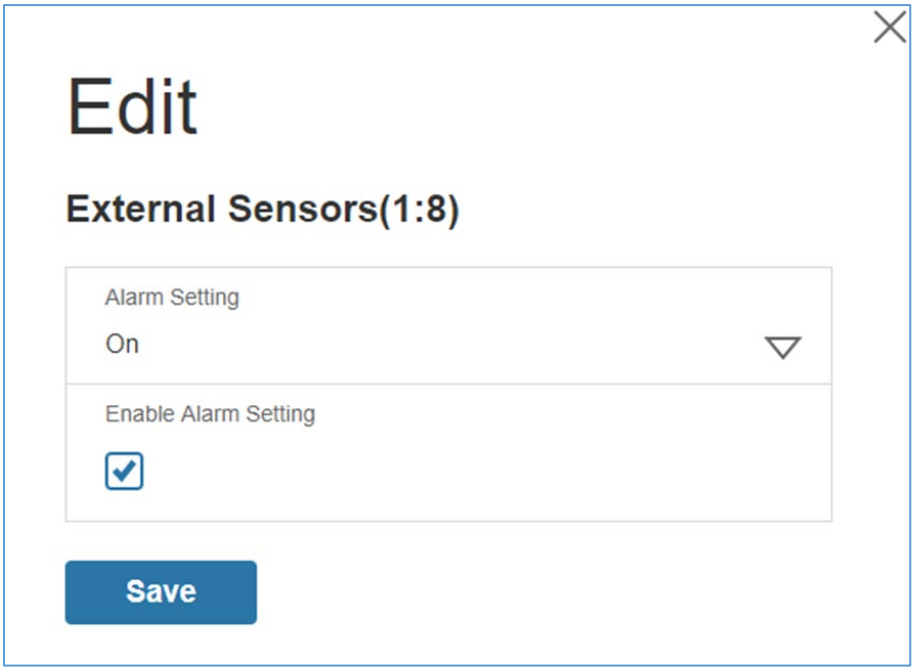


Figure 92: Door Switch Sensor Configuration

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.

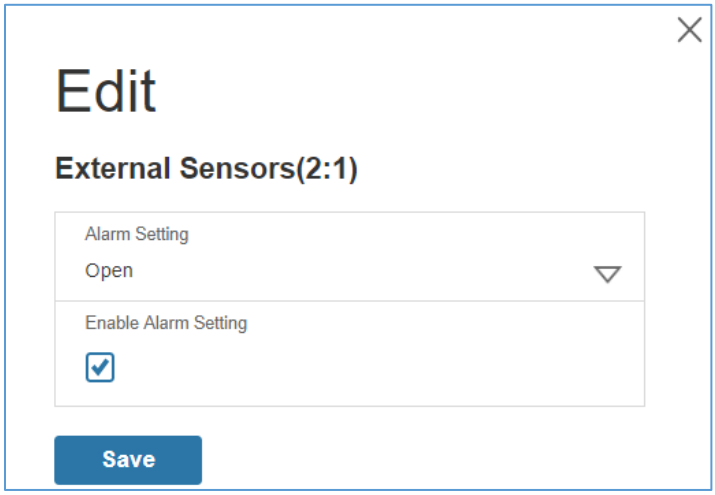


Figure 93: Dry Contact Cable

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.

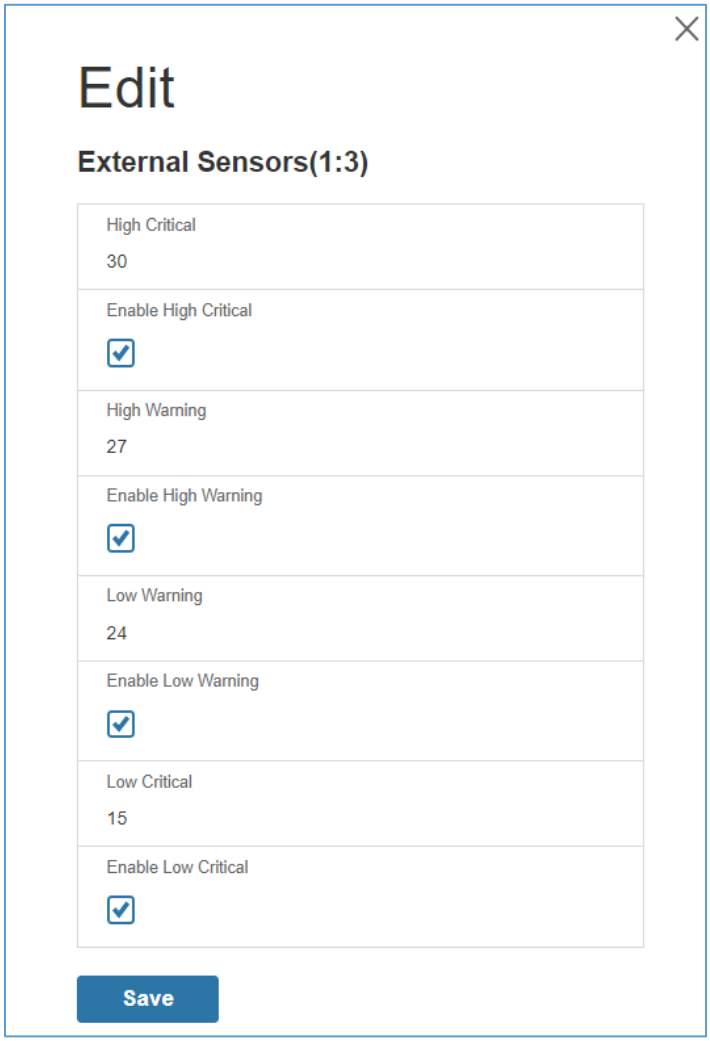


Figure 94: Temperature and Humidity Sensors

Configuring Environmental Sensors

Each Panduit G6 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.

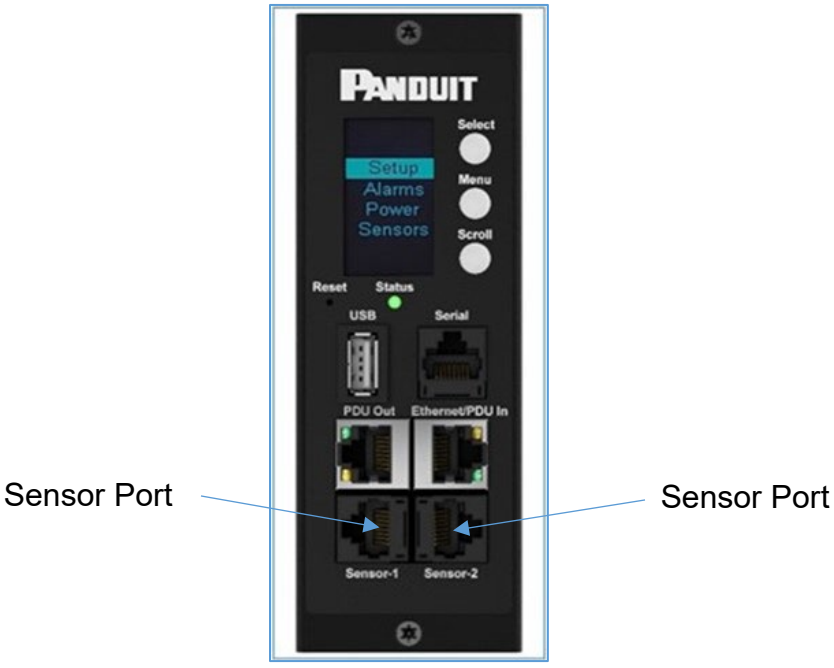


Figure 95: Sensor Ports on controller

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.

G6 Upgrade Tool (GUT)

The 'G6 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.

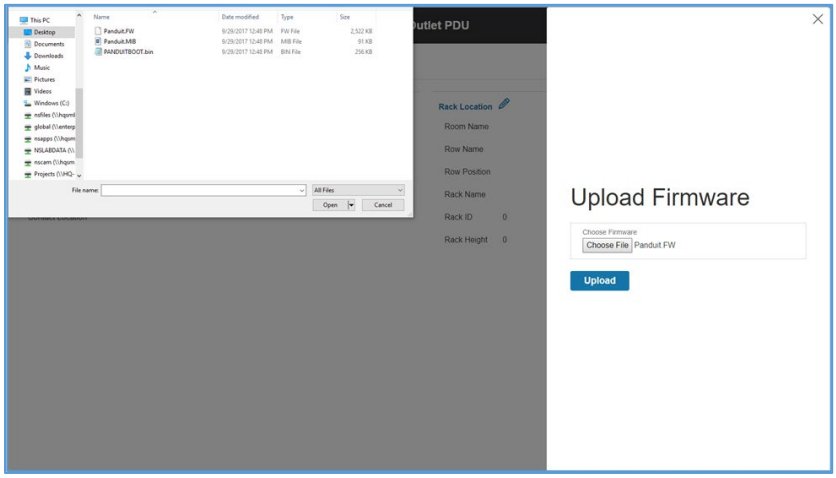


Figure 96: Upload Firmware

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: The USB drive must be **unencrypted** and formatted as the FAT32 filesystem.

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 G6 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.

G6 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'

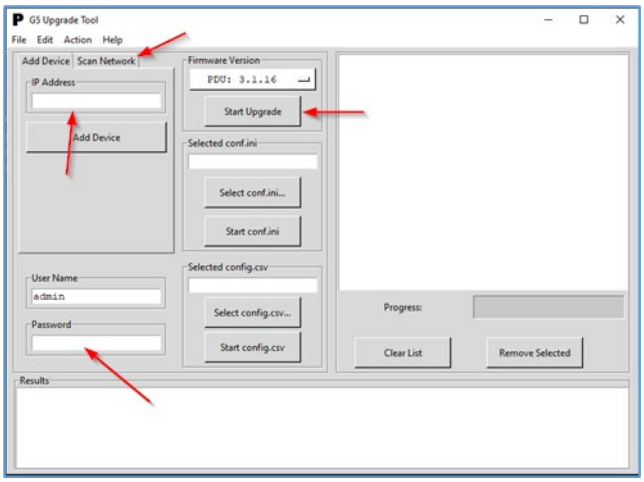


Figure 97: G6 Upgrade Tool Interface

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.

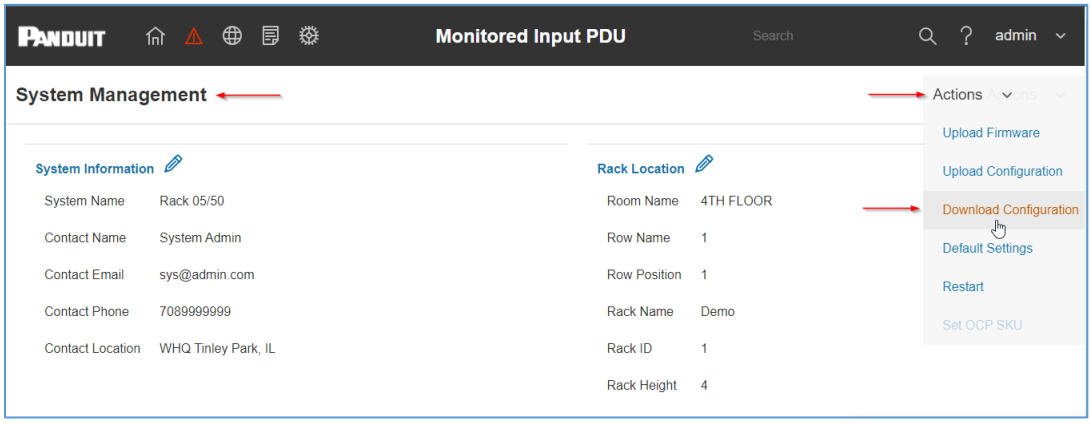


Figure 98: System Management Download Configuration Web GUI

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

c. Insert admin credentials

d. Load the confi.ini file to the G6 Upgrade Utility and click Start Conf.ini

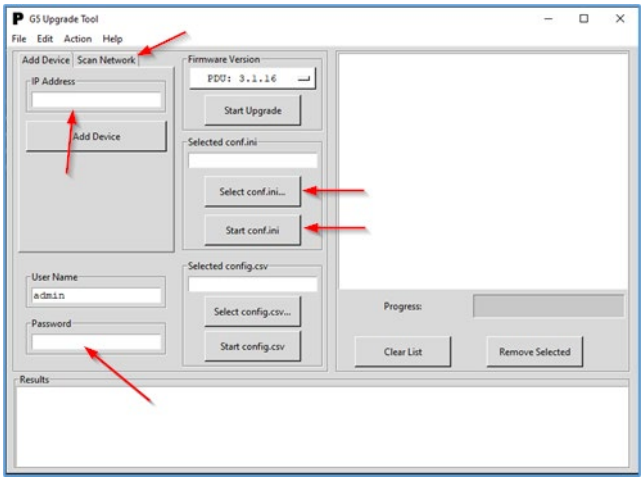


Figure 99: G6 Upgrade Tool Interface

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				[redacted].42	[redacted].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 100: Example CSV File

d. Load the Config.csv file to the G6 Upgrade Utility and click Start Config.csv

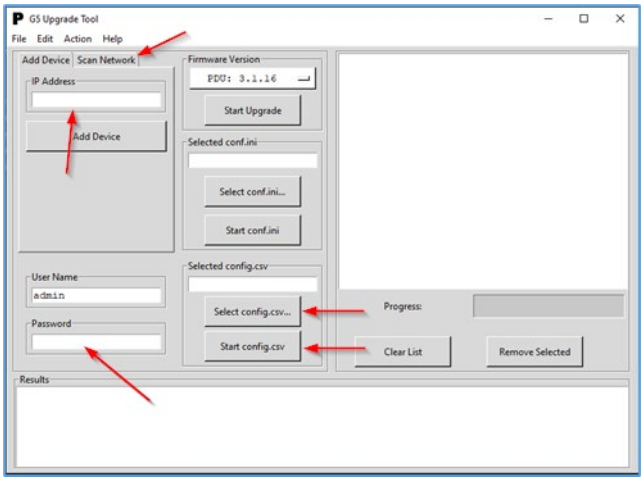


Figure 101: G6 Upgrade Tool Interface

Appendix D: System Reset or Password Recovery

Use Reset Button on Controller

Restart – retains all configurations

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**.

Factory Default – removes all configurations

To Default the controller to factory settings, press and hold the Reset Button for **a minimum of 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 102: 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.

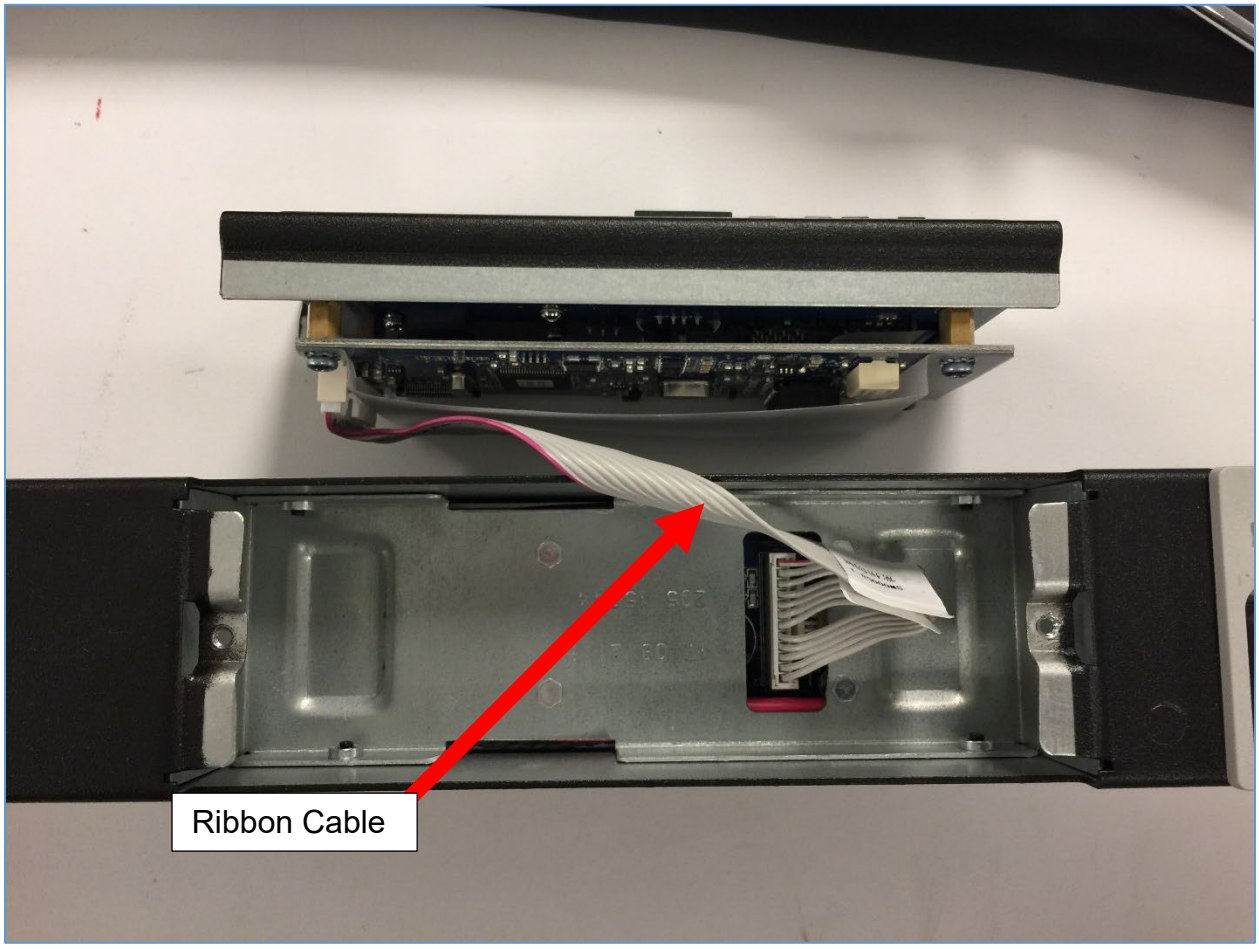


Figure 103: Ribbon Cable for the Network Controller

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**.

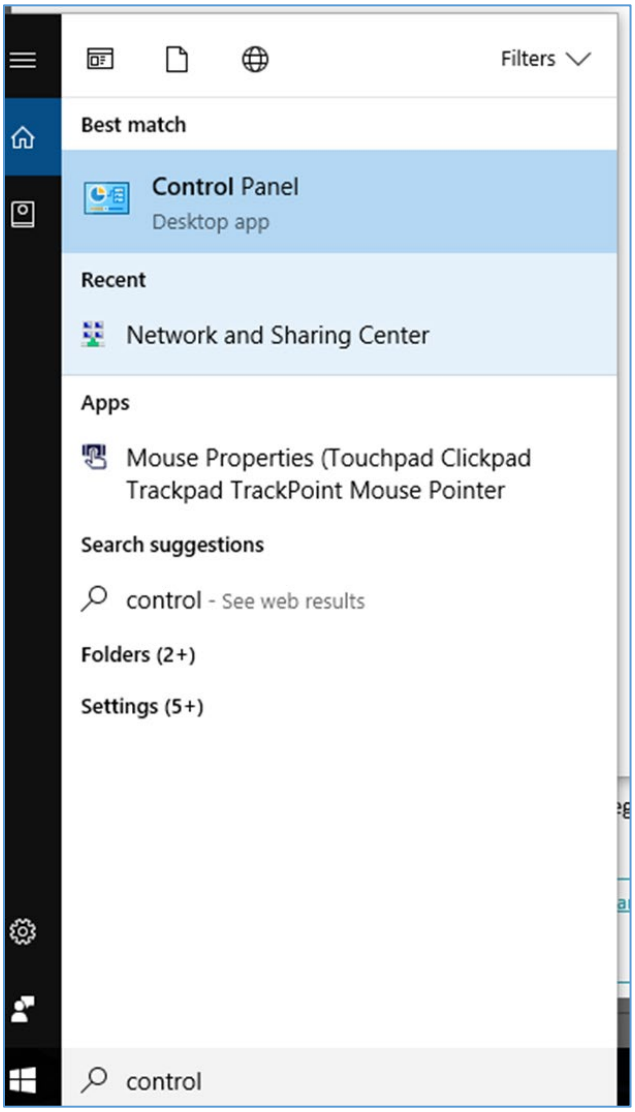


Figure 104: Control Panel

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

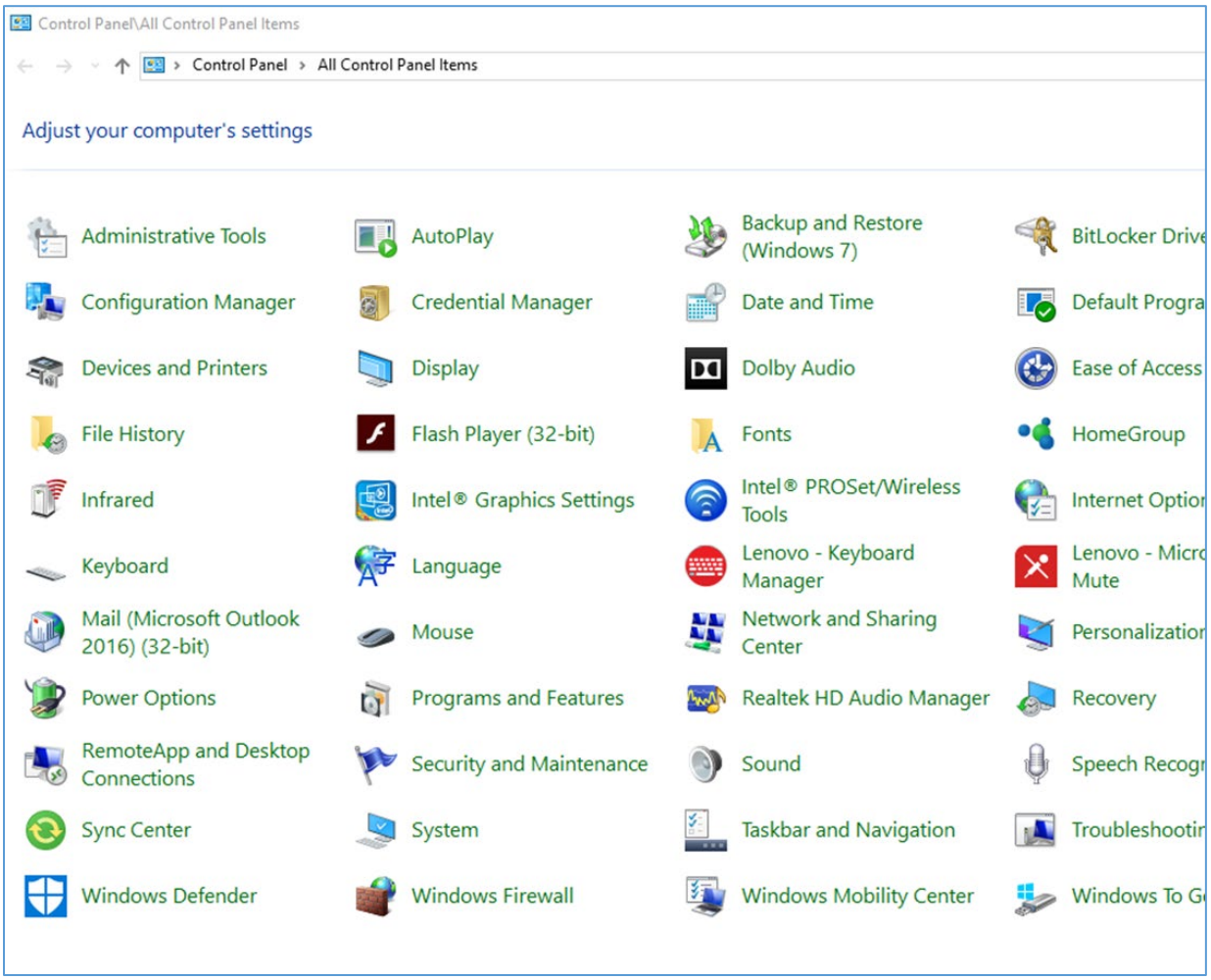


Figure 105: Network Status and Tasks

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

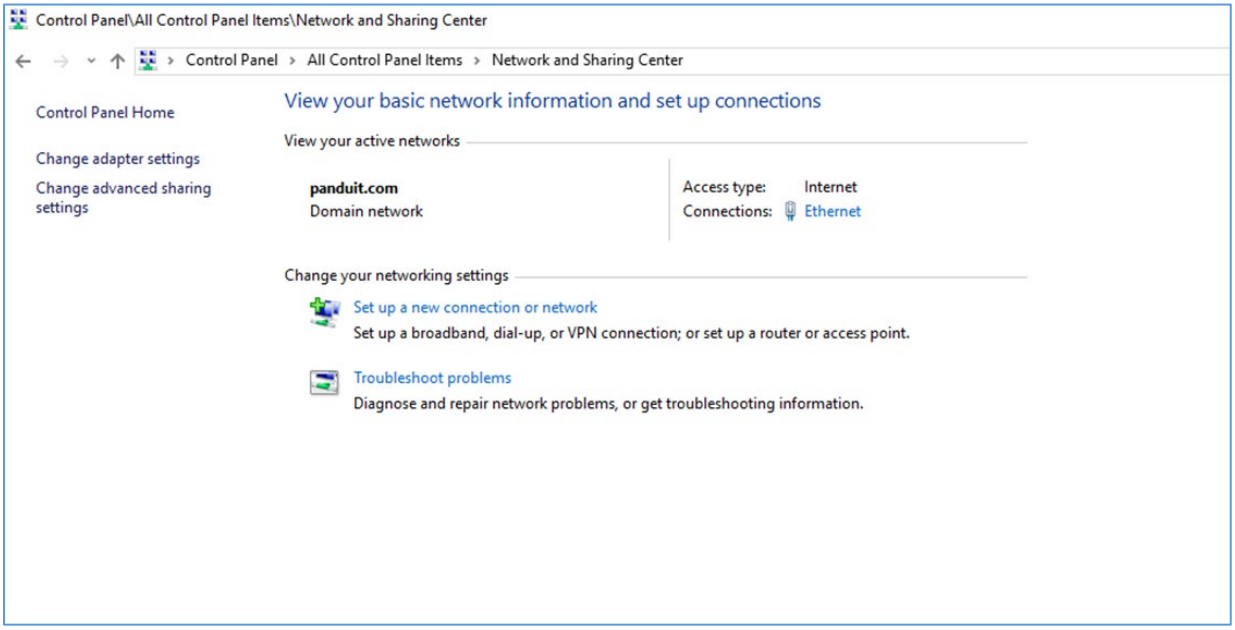


Figure 106: Change Adapter Settings

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

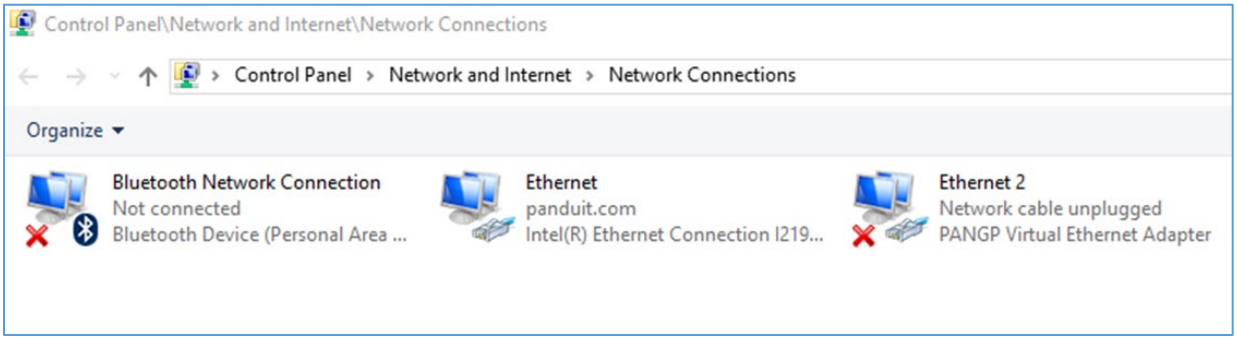


Figure 107: Properties

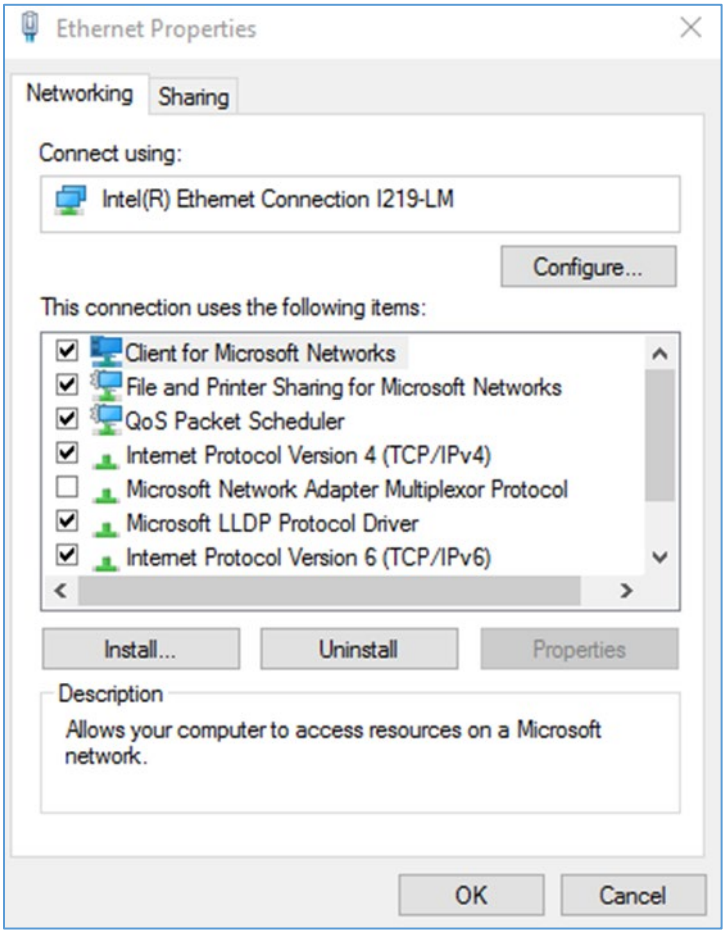


Figure 108: Ethernet Properties

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

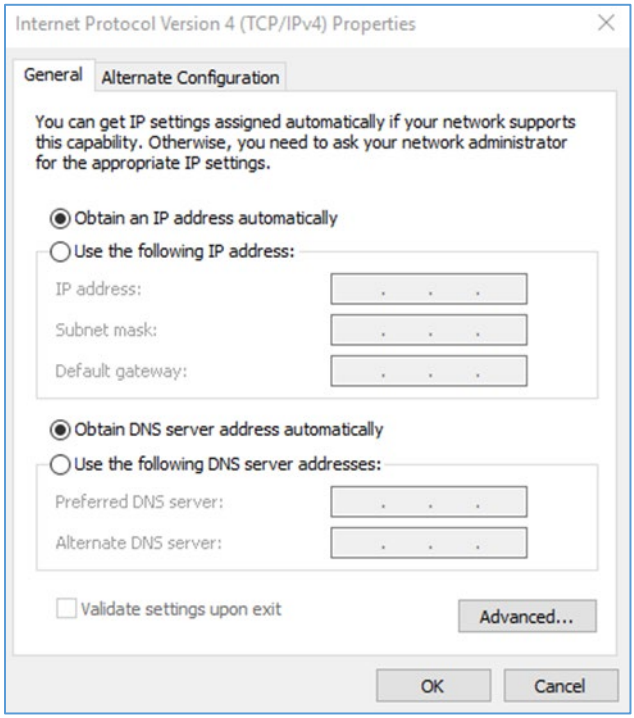


Figure 109: Internet Protocol Version 4

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

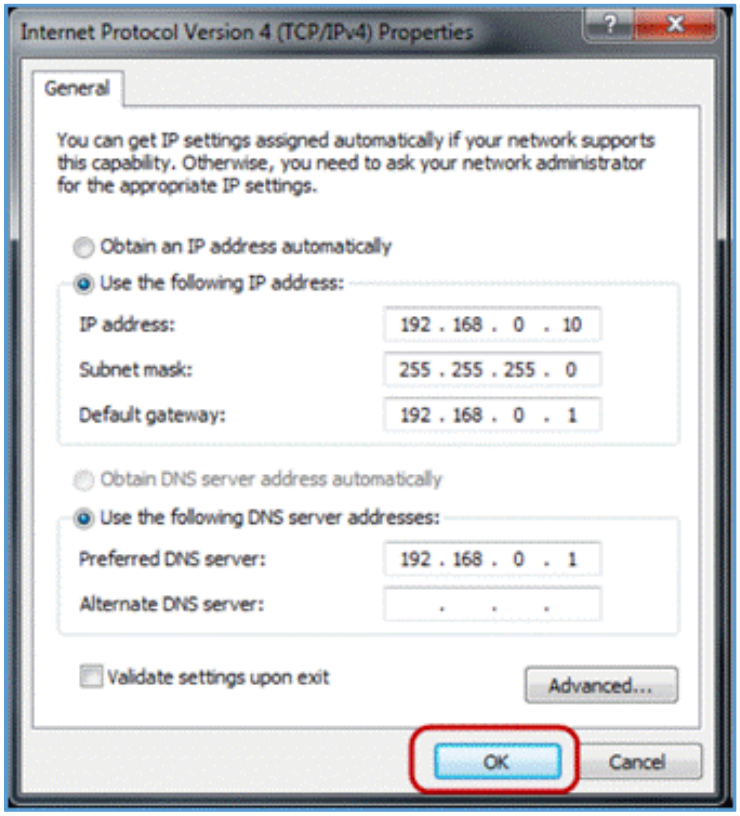


Figure 110: IP Settings for Direct Connection

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 G6 Serial Interface to a YOST interface.

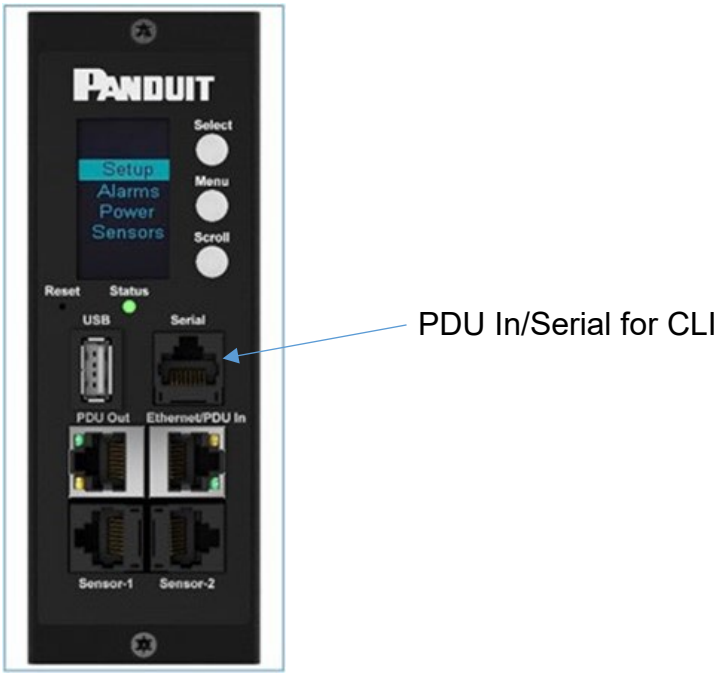


Figure 111: Connect MA017 to the PDU In/Serial port

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:

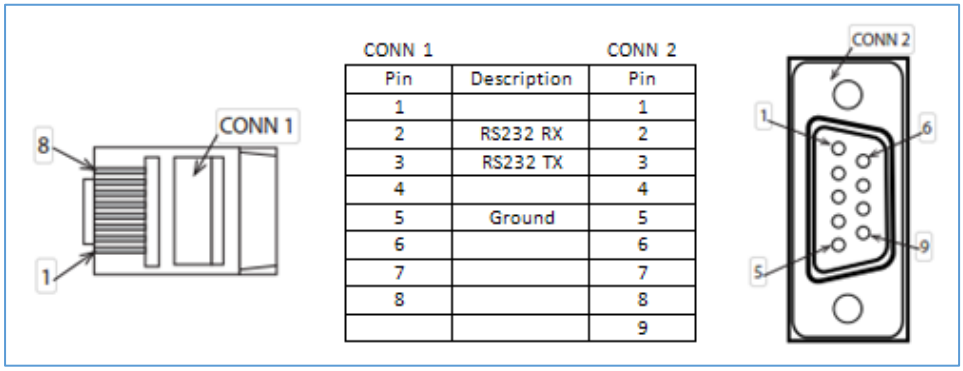


Figure 112: Serial Cable Pinout

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	Query or set system's date.	Panduit>sys date SUCCESS Date:2025-02-25 Time:08:44:50
sys time	Query or set system's time.	Panduit> sys time SUCCESS Date:2025-02-25 Time:08:45:43
sys ntp (G6 Only)	Query the ntp status and servers configured.	Panduit>sys ntp SUCCESS Server1 : 162.159.200.1 Server2 : 0.0.0.0 NTP Status : ON
sys ntp [on/off] (G6 Only)	Sets the ntp status to ON/OFF	Panduit>sys ntp on SUCCESS Panduit>sys ntp off SUCCESS
sys ntp [server1] [server2] (G6 Only)	Set the primary and secondary IP	Panduit>sys ntp 162.159.200.1

Command	Description	Example
	address of the ntp server 1 and server 2	SUCCESS Panduit>sys ntp 95.216.144.226 162.159.200.55 SUCCESS NTP Status : ON
sys ntp gmtoffset (G6 Only)	Displays current the GMT offset set	Panduit>sys ntp gmtoffset SUCCESS GMT Name : Chennai, Kolkata, Mumbai, Delhi GMT Offset : UTC+05:30
sys ntp gmtoffset [UTCoffset] (G6 Only)	Sets the UTC code defined for every offset to the PDU for the specific region. The UTC code can be viewed by entering the NTP help string command.sys	Panduit>sys ntp gmtoffset +00:03 SUCCESS Reboot required for change to take effect System Reboot now, Are you sure?(Y/N):Y
sys ntp gmtoffset [help] (G6 Only)	Displays the GMT offset help reference for all regions	Panduit>sys ntp gmtoffset help SUCCESS | Offset | Name |UTC Code ---------- | UTC-12:00 | International Date Line West |-12:00 | UTC-11:00 | Samoa |-11:00 | UTC-10:00 | Hawaii |-10:00 | UTC-09:00 | Alaska |-09:00
sys ver	Query system's version information including firmware,	Panduit>sys ver SUCCESS Firmware Version : 5.2.5 Bootloader Version : 1.2 Language Version : 1.2.2

Command	Description	Example
	bootloader, and Web.	Web Version : 1.22
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 rst [pduid]	Reset system.	Panduit>sys rst 1 Reboot required for change to take effort. System Reboot now, Are you sure? (Y/N):Y
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 **NOTE:** There must be a valid file named conf.ini existing under directory/fw.
sys upd all	Update system's firmware with existing pdu bin f ile.	Panduit>sys upd all 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 log del event	Delete event log file.	Panduit>sys log del event SUCCESS

Command	Description	Example
sys log edit event [on/off] [interval]	Configure event log collection parameters	PANDUIT>sys log edit event on 1 SUCCESS PANDUIT>sys log edit event off 1 SUCCESS
sys log del data	Delete data log file.	Panduit>sys log del data SUCCESS
sys log edit data [on/off] [interval]	Configure data log collection parameters	PANDUIT>sys log edit data on 1 SUCCESS PANDUIT>sys log edit data off 1 SUCCESS
sys dualinput get	Gets the Region for the Dual rated PDUs Power Capacity.	Panduit> sys dualinput get SUCCESS EMEA rating is active Rating: 346-415V, 16A, 11.0kVA, 50/60Hz
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
sys cordtype [TYPE]	Displays the SKU/cord type information set User can select one of the available cord types. Command gives us the list of available SKU/cord types	Panduit> sys cordtype SUCCESS SKU : P36E50M_32A3WYE Panduit>sys cordtype 32A3WYE SUCCESS SKU : P36E50M_32A3WYE
sys updatehid [motor/rfid] [pduid] [0(hot)/ 1(cold)]	Updates the handle rfid or motor firmware	Panduit> sys updatehid motor 1 1 Updating HID motor firmware, please wait… Handle update is SUCCESS, PDU will reboot now

Command	Description	Example
		Panduit> sys updatehid rfid 1 1 Updating HID RFID firmware, please wait… Handle update is SUCCESS, PDU will reboot now
sys updatercm rcm (G6 Only) net	Updates the RCM firmware using the rcm.bin to the fw folder	Panduit> sys updatercm rcm Updating RCM firmware, please wait… Panduit> sys updatercm rcm Updating RCM firmware, please wait RCM update is SUCCESS, PDU will reboot now

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 telnet [on/off] (G6 Only)	Query or on/off telnet.	Panduit>net telnet SUCCESS telnet port: 23 Telnet server is running Panduit>net telnet on SUCCESS Reboot required for change to take effect System Reboot now, Are you sure?(Y/N)Y Panduit> net telnet off SUCCESS Reboot required for change to take effect System Reboot now, Are you sure?(Y/N):
net ftps	Query FTPs.	Panduit>net ftps SUCCESS FTPS Port: 21 Service is running

Command	Description	Example
		ls Ftps
net ftps [on/off]	Query or on/off FTPs.	Panduit>net ftps on Reboot required for change to take effect Ftps protocol is changed, Please reboot to validate System Reboot now, Are you sure?(Y/N):Y
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 WEB protocol is changed, Please reboot to validate System Reboot now, Are you sure? (Y/N):Y
net https [on/off]	Query or on/off net https.	Panduit>net https SUCCESS HTTPS Port: 443 Status: ON Panduit>net https on Reboot required for change to take effect HTTPS protocol is being turned on, Please reboot to validate System Reboot now, Are you sure?(Y/N): Panduit>net https off Reboot required for change to take effect HTTPS protocol is being turned off, Please reboot to validate System Reboot now, Are you sure?(Y/N):
net redfish	Query or on/off net https.	Panduit> net redfish SUCCESS Status: OFF Panduit>net redfish on net redfish on SUCCESS Panduit>net redfish off SUCCESS

Command	Description	Example
net redirect [on/off] (G6 Only)	Query or on/off net redirect.	Panduit> net redirect SUCCESS Redirection Port: 443 Status: OFF Panduit>net redirect on SUCCESS Panduit>net redirect off SUCCESS
net telnet port [portnumber] (G6 Only)	Sets the port number for TELNET.	Panduit>net telnet port 23 Reboot required for change to take effect Telnet port is changed, Please reboot to validate System Reboot now, Are you sure?(Y/N):Y
net snmp	Query SNMP status.	Panduit>net snmp SUCCESS v1v2c: ON v3: ON trap: ON
net snmp [v1v2c/v3] [on/off]	Sets SNMP On or Off.	Panduit>net snmp v1v2c on / net snmp v3 on SUCCESS Panduit>net snmp v1v2c off / net snmp v3 off SUCCESS
net snmp trap [on/off/port]	Query the snmp trap port number or turns off/on the snmp trap.	Panduit>net snmp trap on SUCCESS Panduit>net snmp trap port SUCCESS SNMP Trap Port: 162
net snmp port [portnumber]	Sets SNMP port number.	Panduit>net snmp port 162 Reboot required for change to take effect SNMP port is changed, Please reboot to validate system Reboot now, Are you sure? (Y/N): Y
net snmp v1v2c <index> <IPaddress> <Read_community>	Configure the SNMP v1/v2c manager.	Panduit>net snmp v1v2c 1 10.20.14.238 public private enable SUCCESS

Command	Description	Example
<Write_community> <Enable/Disable>		
net snmp v3 <index> <username> <securitylevel[AP/ANP/NANP]> <Auth_password> <Auth_algo[MD5/SHA]> <Priv_key> <Priv_algo[AES128/AES192/AES256]> <Enable/Disable>	Configure the SNMP v3 manager.	Panduit>net snmp v3 1 admin AP 123456789 SHA 123456789 AES128 enable SUCCESS
net [mac/tcpip]	Displays the MAC address Displays the TCPIP address	Panduit>net mac SUCCESS MAC Addr: C8-45-44-3B-5D-28 MAC Addr: C8-45-44-D3-33-B7 Panduit>net tcpip SUCCESS eth0 IPv4 Addr: 10.20.15.16 eth0 IPv6 Link Local Addr: fe80::f680:fcc3:de2e:2131 eth0 IPv6 DHCP Addr: 2001:1111:1111:1121:f606:f2da:29ed:feba eth1 IPv4 Addr: 0.0.0.0 eth1 IPv6 Link Local Addr: 0.0.0.0 eth1 IPv6 DHCP Addr: 0.0.0.0
net tcpip [eth0dhcp/eth1dhcp/eth0static/eth1static ip nm gw] (G6 Only)	Changes the eth0 or eth1 to DHCP or Static mode.	Panduit>net tcpip SUCCESS eth0 IPv4 Addr: 10.20.15.16 eth0 IPv6 Link Local Addr: fe80::f680:fcc3:de2e:2131 eth0 IPv6 DHCP Addr: 2001:1111:1111:1121:f606:f2da:29ed:feba eth1 IPv4 Addr: 0.0.0.0 eth1 IPv6 Link Local Addr: 0.0.0.0 eth1 IPv6 DHCP Addr: 0.0.0.0 Panduit>net tcpip eth0static 10.20.15.16 255.255.255.128 10.20.15.1 Reboot required for change to take effect Network is reconfigured, Please reboot to validate

Command	Description	Example
		System Reboot now, Are you sure?(Y/N):Y
net tcpip [v6eth0dhcp/v6eth1dhcp/v6eth0static/v6eth1static ip pl gw] (G6 Only)	Changes the IPv6 network to DHCP or Static mode	Panduit>net tcpip v6eth0dhcp Reboot required for change to take effect Network is reconfigured, Please reboot to validate System Reboot now, Are you sure?(Y/N):Y Panduit>>net tcpip v6eth1static 2001:1111:1111:1121:f606:f2da:29ed:feba 64 fe80::9e66:97ff:fe76:f3fd%10 Reboot required for change to take effect Network is reconfigured, Please reboot to validate System Reboot now, Are you sure?(Y/N):Y
net scp (G6 Only)	Copies the event logs to the specified system	Panduit>net scp SUCCESS : scp enabled
net scp <full_localfilepath> <remoteuser>@ <remotehost> <full_remotefilepath> (G6 Only)	Copies the event logs to the specified system	Panduit>net scp /system/log/eventlog.txt buildserver@10.10.105.255/home/buildserver The authenticity of host '10.10.105.255 (10.10.105.255)' can't be established. ED25519 key fingerprint is SHA256:F+FVTej0G4bvsDzOnx9jSklo77LQcdu F1BCFCZFwuhM. This key is not known by any other names Are you sure you want to continue connecting (yes/no/[fingerprint])? Yes Warning: Permanently added '10.10.105.255' (ED25519) to the list of known hosts. buildserver@10.10.105.255's password: eventlog.txt 100% 11 KB 739.8 KB/s 00:00 File successfully uploaded.
net ip [v4] [v6] [v4v6]	Changes the mode between	Panduit>net ip v4 Reboot required for change to take effect IP protocol is changed, Please reboot to validate

Command	Description	Example
	DUAL, IPv4 or IPv6 Only	System Reboot now, Are you sure?(Y/N):Y Panduit>net ip v6 Reboot required for change to take effort IP protocol is changed, reboot to validate System Reboot now, Are you sure?(Y/N):Y
net phy	Query the set link speed	Panduit>net phy SUCCESS link speed : auto negotiation
net phy [auto/10100mbps/1gbps]	Set the link speed to auto negotiation/ 10100mbps/ 1gbps	Panduit>net phy SUCCESS link speed: auto negotiation Panduit>net phy 10100mbps Reboot required for change to take effort Phy speed is changed, reboot to validate System Reboot now, Are you sure?(Y/N):Y
net dns [-h <hostname> -d <domain> -s1 <server1> -s2 <server2>] (G6 Only)	Changes the DNS domain name, host name, primary and secondary server	Panduit>net dns -h admin -d test -s1 10.10.105.20 -s2 10.10.105.21 Reboot required for change to take effect IP protocol is changed, Please reboot to validate System Reboot now, Are you sure?(Y/N):Y
net dns [disable/enable] [dnsname/servername]] (G6 Only)	Enables/Disables the DNS server or host by name	Panduit>net dns enable dnsname Reboot required for change to take effect IP protocol is changed, Please reboot to validate System Reboot now, Are you sure?(Y/N):Y
net cert	Updates the certificate file	Panduit>net cert SUCCESS Custom certificate key file active, in /system/cert/cert.key Custom certificate cert file active, in /system/cert/cert.crt
net cert [def]	Updates the certificate file	Panduit>net cert def Removing custom certificate key file, in /cert/cert.key Removing custom certificate file, in /cert/cert.crt Reboot required for change to take effect Certificate Setting changed, reboot to validate System Reboot now, Are you sure?(Y/N):Y

Command	Description	Example
net eap (G6 Only)	Displays the current authentication information	Panduit>net eap SUCCESS ETH0 AUTH:EAP-TLS ETH0 IDENTITY :SmartPower ETH1 AUTH :EAP-TLS ETH1 IDENTITY :SmartPower
net eap [eth0/eth1] [enable/disable] outer TLS identity [Identity] passphrase [private key passphrase] (G6 Only)	Setting the an authentication information for EAP-TLS configuration to any specific ethernet port. Note – Upload CA Certificate, Client Key and Client Certificate via FTPS, before setting via CLI.	Panduit>net eap eth0 enable outer TLS identity system_bangalore_center01 passphrase smartpower SUCCESS Reboot required for change to take effect Network is reconfigured, Please reboot to validate System Reboot now, Are you sure?(Y/N):Y
net eap [eth0/eth1] [enable/disable] outer PEAP inner TLS identity [Identity] passphrase [private key passphrase] (G6 Only)	Setting the an authentication information for PEAP-TLS configuration to any specific ethernet port. Note – Upload CA Certificate,	Panduit>net eap eth0 enable outer PEAP inner TLS identity system_bangalore_center01 passphrase smartpower SUCCESS Reboot required for change to take effect Network is reconfigured, Please reboot to validate System Reboot now, Are you sure?(Y/N):Y

Command	Description	Example
	Client Key and Client Certificate via FTPS, before setting via CLI.	
net eap [eth0/eth1] [enable/disable] outer PEAP inner MSCHAP identity [Identity] password [password] (G6 Only)	Setting the an authentication information for PEAP-MSCHAPV2 configuration to any specific ethernet port. Note – Upload CA Certificate via FTPS, before setting via CLI.	Panduit>net eap eth1 enable outer PEAP inner MSCHAP identity system_bangalore_center01 passphrase smartpower SUCCESS Reboot required for change to take effect 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
usr login	Displays information about the user Logged in.	Panduit>usr login SUCCESS User: admin IPAddress: 10.19.58.216 ClientType: SSH
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.
usr options [interactive/non- interactive] [add/del/edit] [username] [password] [confirm_password] [role:admin/user/manager] (G6 Only)	Add Users and set credentials, define roles using interactive and non-interactive method.	Panduit>usr options interactive Enter command from List: add/del/edit add Enter user name User1 Enter Password 123456789 Re enter Password for confirmation 123456789 Enter role : admin | user | manager admin Enter temperature scale (C/F) C SUCCESS Panduit>usr options non-interactive add user2 123456789 123456789 admin f SUCCESS

Command	Description	Example
usr roleoptions [interactive/non- interactive] [add/del/edit] [rolename] [Admin Privilege required? : yes/no] [roledescription] (G6 Only)	Add Users and set credentials, define roles and privileges using interactive and non-interactive method.	Panduit> usr roleoptions interactive Enter command from List: add/del/edit add Enter role name Admin Bangalore Enter role description Admin in Bangalore Admin privilege required : yes/no yes SUCCESS Panduit>usr roleoptions non-interactive add AdminBangalore yes AdmininBangalore SUCCESS
usr rolelist (G6 Only)	Displays the rolelist with privilege and role descriptions .	Panduit>usr rolelist SUCCESS Role Privilege Role Description ========== admin admin admin operation user user user operation manager admin redfish user
usr pwdpolicy [interactive/non- interactive] [get/set] [pwd_age_interval : | 7 | 14 | 30 | 60 | 90 | 180 |365 |Never Expire] [min_len] [max_len] [at least 1 lower character must be in password: yes/no] [at least 1 upper character must be in password: yes/no] [at least 1 numerical character must be in password: yes/no] [at least 1 special character must be in password: yes/no] (G6 Only)	Get/Set data for the password fields as per user requirements in two approaches – interactive or non-interactive	Panduit>usr pwdpolicy interactive Enter command from List: get/set set Enter Password Aging Interval in days from List: | 7 | 14 | 30 | 60 | 90 | 180 | 365 | Never Expire Never Expire Enter Minimal length for Password : should be => 8 & < 32 8 Enter Maximum length for Password : should be > 8 & <= 32 12 Do You want to Enforce at least 1 lower case character policy in Password : yes | no no

Command	Description	Example
		Do You want to Enforce at least 1 Upper case character policy in Password : yes | no no Do You want to Enforce at least 1 Numerical character policy in Password : yes | no yes Do You want to Enforce at least 1 Special character policy in Password : yes | no no SUCCESS Panduit>usr pwdpolicy non-interactive get Password Policy details are: maxpwdlen = 12 minpwdlen=8 Password Aging Interval = Never Expire Enforce at least one lower case character : [no] Panduit> Enforce at least one upper case character : [no] Enforce at least one numeric character : [yes] Enforce at least one special character : [no] SUCCESS Panduit>useusr pwdpolicy non-interactive set NeverExpire 8 12 no no yes no SUCCESS
usr sessionmgmt [interactive/non- interactive] [get/set] [sign in retries allowed? : yes/no] [number_retry: 3 to 10] [sesssion_timeout from list: |	Get/Set data for the sessions management as per user requirements in two approaches – interactive	Panduit>usr sessionmgmt interactive Enter command from List: get/set get Session Management details are: chkuserblocking = 1 maxnumfailedlogins=3 blocktimeout=3 idletimeout=10

Command	Description	Example
1 | 10 | 20 | 30 | 60 | 120 | 240 | 360 | 720 | 1440 |] [lockout_time from list : | 1 | 2 | 3 | 4 | 5 | 10 | 15 | 20 | 30 | 60 | 120 | 240 | 360 | 720 | infinite |] (G6 Only)	or non-interactive	SUCCESS Panduit>usr sessionmgmt interactive Enter command from List: get/set set Do You want to allow Sign-In retries : yes | no yes Enter Number of Retries Allowed from count: [3] to [10] 3 Enter Session Timeout Value (in min) from List: | 1 | 10 | 20 | 30 | 60 | 120 | 240 | 360 | 720 | 1440 | 10 Enter Lockout Time Value (in min) from List: | 1 | 2 | 3 | 4 | 5 | 10 | 15 | 20 | 30 | 60 | 120 | 240 | 360 | 720 | infinite | 10 SUCCESS Panduit>usr sessionmgmt non-interactive get Session Management details are: chkuserblocking = 1 maxnumfailedlogins=3 blocktimeout=10 idletimeout=10 SUCCESS Panduit> usr sessionmgmt non-interactive set yes 3 10 10 SUCCESS
INTERACTIVE APPROACH* When the user selects an Interactive Approach, user will be prompted for each parameter/option to perform the respective action. NON-INTERACTIVE APPROACH** When the user selects a Non-Interactive Approach, user needs to enter all the parameters as per the syntax in a single line.		

Device Commands

Command	Description	Example
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 daisy chain.	Panduit>dev daisy rna init SUCCESS System Reboot now, Are you sure? (Y/N):N
dev daisy [rna/qna] [create]	Creating daisy chain	Panduit>dev daisy rna init create SUCCESS System Reboot now, Are you sure? (Y/N):N
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] [controlstatus]	Query or set specified PDUID and outlet-	Panduit> dev outlet 1 controlstatus SUCCESS Relay Outlet

Command	Description	Example
	index's outlet control status.	S.No: Name : Status : OnDelay : OffDelay : RebootDelay : PowerOnState | 1 : OUTLET 1 : Open : 0 : 0 : 5 : ON | 2 : OUTLET 2 : Open : 0 : 0 : 5 : ON | 3 : OUTLET 3 : Open : 0 : 0 : 5 : ON
dev outlet [pduID] [outletindex/outletname] [get] [status]	Query the specified PDUID and outlet-index's or outlet name's outlet control get status.	Panduit> dev outlet 1 OUTLET10 get status SUCCESS Relay Outlet Name : Status : OnDelay : OffDelay : RebootDelay : PowerOnState |10 : OUTLET10 : Open : 0 : 0 : 5 : ON
dev outlet [pduID] [outletindexdev/outletname] [set] [outletname/poweronstate/ondelay/offdelay/rebootdelay]	Displays the status of the PDU Outlets with reference to outlet index, outlet name, power state, on delay, off delay and reboot delay	Panduit>dev outlet 1 outlet42 set outletname OUTLET42OUTLET42 SUCCESS Panduit>dev outlet 1 outlet42 set poweronstate on SUCCESS Panduit>dev outlet 1 outlet42 set poweronstate off SUCCESS Panduit>dev outlet 1 outlet42 set poweronstate lastknown SUCCESS Panduit>dev outlet 1 42 set ondelay 7200 SUCCESS Panduit>dev outlet 1 42 set offdelay 7200 SUCCESS Panduit>dev outlet 1 42 set rebootdelay 60 SUCCESS

Command	Description	Example
dev outlet [pduID] [outletindex/outletname] [on/off/ondelay/offdelay/rebootdelay/reboot]	Command to Turn on/off/off delay/ ondelay/r ebootdelay the outlet power	Panduit>dev outlet 1 1 on SUCCESS Panduit>dev outlet 1 1 rebootdelay SUCCESS
dev usb [on|off]	Query or on/off USB.	Panduit> dev usb SUCCESS USB is open Panduit> dev usb on SUCCESS Panduit> dev usb off SUCCESS
dev sensor	List all sensors equipped.	Panduit> dev sensor SUCCESS Sensor count 4 ---------- Name Type, SN Value ---------- T1,TEMP 012345678 27.5 T3,TEMP 012345678 27.2 T2,TEMP 012345678 27.3 RH HUMI 012345678 44
dev sensor unit [pduid] (G6 Only)	List all sensors equipped for a pdu	Panduit> dev sensor unit 1 SUCCESS Sensor count 1 ---------- Name Type, SN Value ---------- T1,TEMP 012345678 27.5
dev statusled [pduid/all] [on/off] (G6 Only)	Turn the status led on and off for pdu/pdus	Panduit>dev statusled 1 on SUCCESS
dev ledstrip [on/off]	Turns on/off the ledstrip	Panduit>dev ledstrip on SUCCESS

Command	Description	Example
dev powershare	Displays the status of PDU power share	Panduit> dev power share SUCCESS PDU 1: Downstream: 0 Upstream: 1 Mains: 1 PDU 2: Downstream: 1 Upstream: 1 Mains: 1 PDU 3: Downstream: 1 Upstream: 1 Mains: 1
dev powershare [pduID] func [on/off]	Displays the status of PDU power share	Panduit> dev powershare 1 SUCCESS pdu 1 support POWER SHARE pdu 1 POWER SHARE is ON pdu 1 is on Main Power pdu 1 Upstream Power Status ON pdu 1 POWER SHARE output is ON Panduit>devdev powershare 1 func on SUCCESS Panduit>devdev powershare 1 func off SUCCESS
dev handle [pduID] [cold/hot] [lock/unlock]	Enables handle function	Panduit>dev handle 1 hot lock SUCCESS
dev tempscale get (G6 Only)	Display information about the Temperatur e scale and temperature scale unit	Panduit>dev tempscale get SUCCESS Temperature Scale : Celsius
dev tempscale global [c/f] (G6 Only)	Display information about the	Panduit>dev tempscale global c SUCCESS Panduit>

Command	Description	Example
	global set Temperature scale and scale unit	dev tempscale global f SUCCESS
dev tempscale user [c/f/default] (G6 Only)	Display information about the User set Temperature scale and scale unit	Panduit>dev tempscale user c SUCCESS Panduit> dev tempscale user f SUCCESS
dev rcm [PDUID] [status/fwver/hwver/selftest [start/result]] (G6 Only)	Set the FW/HW/Self test start or display the result.	Panduit>dev rcm 1 status RCM support is enabled for PDU 1 RCM Communication status is OK SUCCESS Panduit>dev rcm 1 fwver RCM Firmware version :53 SUCCESS Panduit>dev rcm 1 hwver RCM Hardware version :16 SUCCESS Panduit>dev rcm 1 selftest start RCM self test initiated successfully for PDU 1 SUCCESS Panduit>dev rcm 1 selftest result Last Self Test has Passed SUCCESS

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
pwr outlet [pduid] [idx]	Query specified outlet's electric information.	Panduit>pwr outlet 1 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.
pwr phase [pduid] [idx]	Query specified phase's electric information.	Panduit> pwr phase 1 1 SUCCESS PDU ID 1 : PHASE 1 power Feature VoltageMeasType : Phase 1 to N frequency : 0Hz voltage : 227.0V current : 0.0A activepower : 0.0W apparentpower : 0.0VA powerfactor : 1.00 energy : 0.000kWh

Command	Description	Example
pwr cb [pduid] [idx]	Query specified circuit breaker's Electric information.	Panduit>pwr cb 1 1 SUCCESS PDU ID 1 : CB 1 power Feature frequency : 50Hz voltage : 227.0V current : 0.0A activepower : 0.0W apparentpower : 0.0VA powerfactor : 1.00 energy : 0.000kWh
pwr rcm [pduid] (G6 Only)	Display RCM Current for the PDU	Panduit>pwr rcm 1 RCM CURRENT:3 mA

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 G6 Accessories

Accessory P/N	Accessory Description
EA001	Panduit G6 Temperature Sensor
EB001	Panduit G6 Temperature + Humidity Sensor
EC001	Panduit G6 (3) Temperature + Humidity Sensor
ED001	Panduit G6 Liquid Rope Sensor
EE001	Panduit G6 Liquid Spot Sensor
EF001	Panduit G6 (3) Sensor Hub
EG001	Panduit G6 Liquid Rope Extension
ACA01	Panduit G6 Door Switch (magnetic 2 piece)
ACC01	Panduit G6 Dry Contact Input
ACD01	Panduit G6 USB Light Strip
ACF05	Intelligent Rack Security Handle with Integral Humidity Sensor
ACF06	Intelligent Rack Security Handle with Integral Humidity Sensor and Keypad
ACF10	Temperature and Door Sensor; connects to Intelligent Rack Security Handle. (Rear)
ACF11	(3) Temperature and Door Sensor, connects to Intelligent Rack Security Handle (Front)
ACF20	Intelligent Rack Security Handle Patch Cord (JST to RJ45 Male)
MA030	Intelligent Rack 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	Intelligent Rack Security Handle HID CARDS 125 KHZ (10 PACK)
CRD-03-10PK	Intelligent Rack 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 G6 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.

For additional details on the Redfish API – please refer to "*G6 PDU Redfish Manual v1.0 FW5.x.pdf*"

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