PANDUIT®
infrastructure for a connected world

Panduit EL2P PDU

User Manual

Version 1.3

Table of Contents

Table of Figures

Section 1 – System Overview

PDU Controller

The hot swappable EL2P PDU controller features a touch screen and an accelerometer. The accelerometer auto rotates the display to accommodate both top fed and bottom fed power orientations. This centralized piece of intelligent hardware receives an IP address, contains a Graphical Web Interface and is addressable over the network. This user's manual also refers to the PDU controller as a Network Management Card (NMC).

The PDU controller can be configured from the Web GUI under System Management

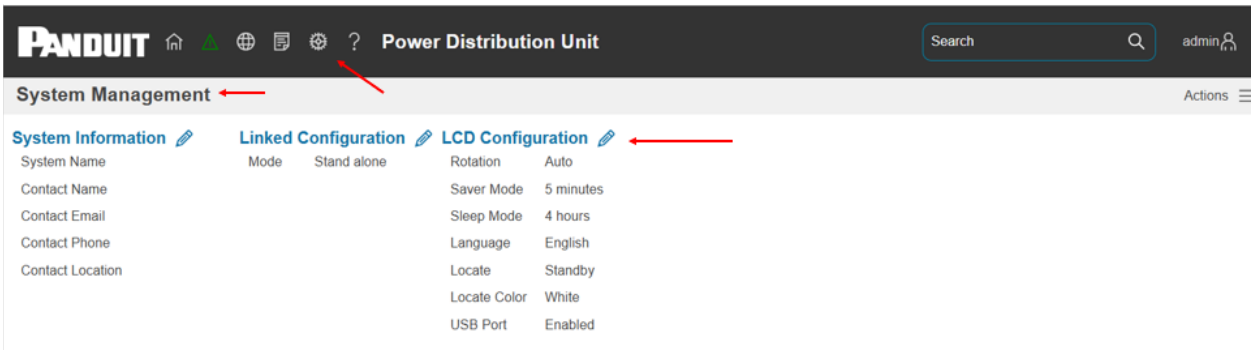


Figure 1: LCD Configuration

Connecting the NMC via Ethernet Port

Connecting the NMC 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 Network port on the NMC (see Figure 1).
2. Connect the other end of the cable to the Network port on the router (or another LAN device).

Figure 2: Ethernet Port for Network Connection

From the factory the NMC defaults to DHCP and HTTP**S** connection. If you are connected to a network with a DHCP server, the NMC automatically receives an IP address. If there is no DHCP server, the NMC will assign an IP (Auto IP). The Auto IP address will be a link-local IP address, and it can be obtained using the instructions in Appendix C: Direct connect via Ethernet without Bonjour. The NMC supports mDNS to discover the DHCP IP or the Auto IP. The mDNS address format is “pdu-<macaddress>.local”. For example, the mDNS address for Figure 1 corresponds to “pdu-000f9c03000b.local” The address is a unique address based on the NMC MAC address.

Connecting the NMC via Wi-Fi (PN: CNT06 Required)

The Wi-Fi feature is only available by swapping the standard NMC with replacement part number CNT06. Wi-Fi runs on the 2.4 GHz frequency.

Mobile devices can access the NMC via Wi-Fi.

1. Connect the NMC from a mobile device. Network id is pdu-<MAC_ADDRESS> and the default login SSID password is: adminadmin

   Note: Wireless access is only available for 10 minutes by default. User can switch this to ‘always on’ by going to the Wi-Fi Settings menu in the Web GUI

2. If the mobile device prompts with the Wi-Fi connection page, open the page. Otherwise, open mobile web browser and connect to https://192.168.5.1
3. Refer to Web Connection in Section 2 for accessing the web page.
4. Navigate to Identification page to examine the Ethernet IP address.

5. Navigate to Wi-Fi Settings page to set up Wi-Fi network

Connecting the NMC to a Computer Serial Port

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

To discover the network setting, perform the following steps:

1. Connect PC to the NMC serial port. See Figure 3: Serial In Port.
2. Using a Terminal emulator program, send read CLI command
    - Refer to Appendix D: Command Line Interface for CLI configuration and password change
3. Enter “read status.netStatus.*”

Figure 3: Serial In Port

v

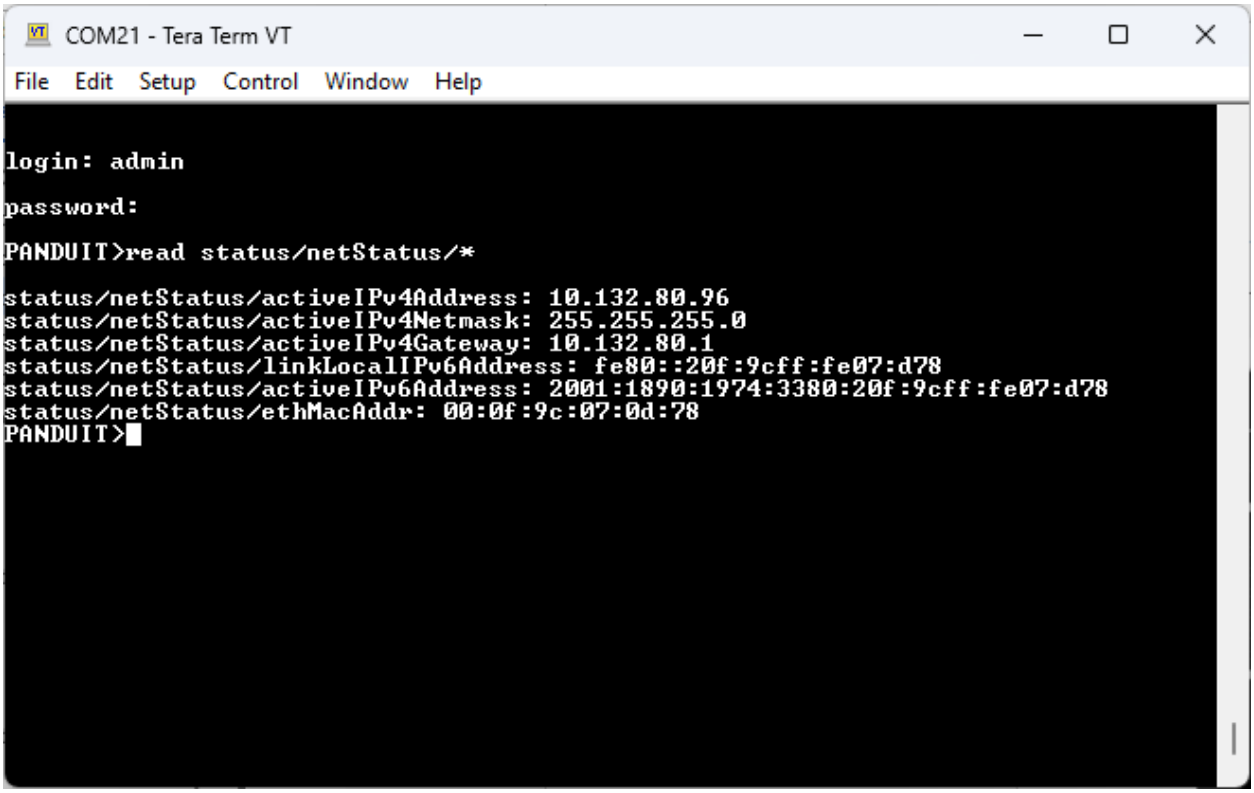


Figure 4: Network information from +

Section 2 – Web Graphical User Interface (GUI)

Internet Protocol (IP) Addressing

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

Web Connection

Supported Web Browsers

The supported Web browsers are Google Chrome (mobile and desktop), Mozilla Firefox, Microsoft Edge and Apple Safari (mobile and desktop).

Logging in to the Web Interface

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

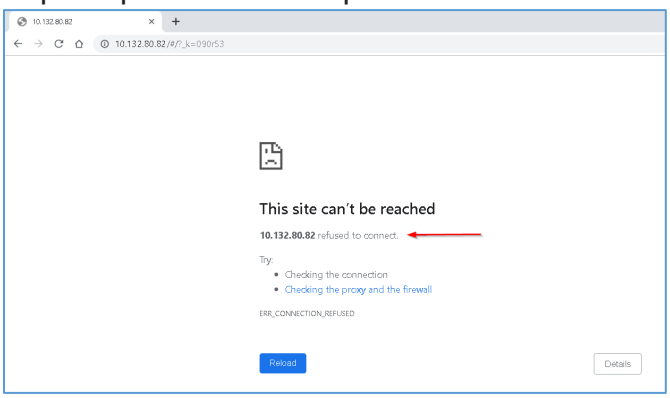


Figure 5: Refused Connection Example

- By default, the Web Interface uses a self-signed certificate. Until a CA signed certificate / key is installed, browsers will display a security error. In Chrome browser, click advanced, then click the “Proceed to” link.

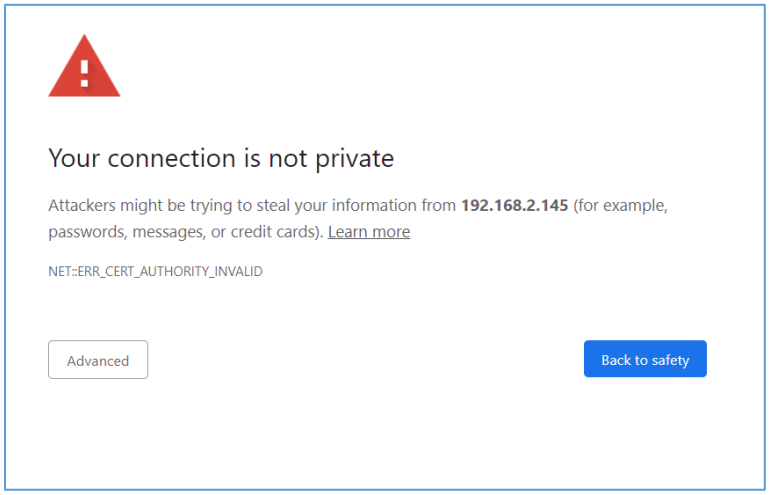


Figure 6: Certificate Warning

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

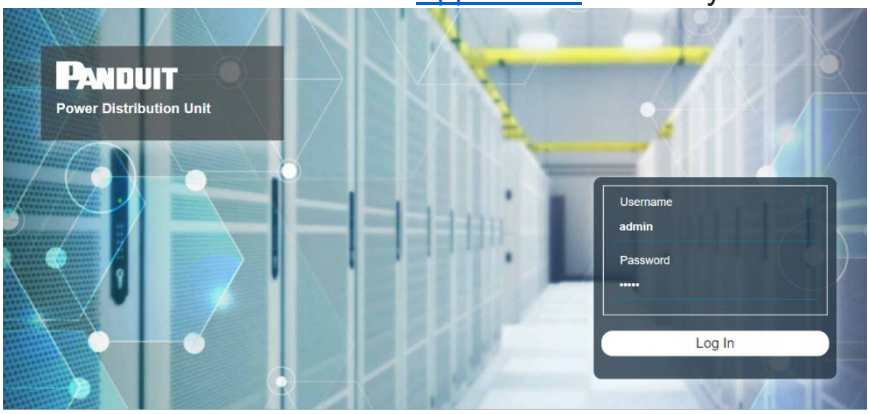


Figure 7: Login Page

Changing Your Password

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

1. Enter the username, current password, and new password twice to confirm. The passwords must be between 8 and 40 characters and follow three of the following four rules:
    a. Contain at least one lowercase character.
    b. Contain at least one uppercase character.
    c. Contain at least one number.

d. Contain at least one special character.

2. Click **Log In** to complete the password change.

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

1. Click on the username and select **Change Password**.

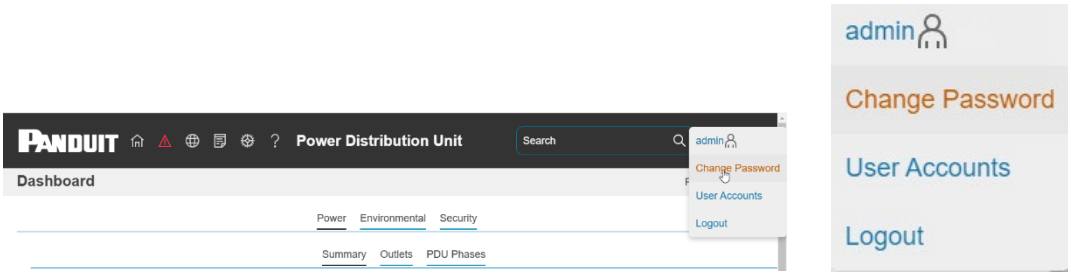


Figure 8: After Login

2. The **Change Password** window opens.
3. Follow the previous instructions in **Changing Your Password**

Introduction to the Web GUI

***Remember**: https:// must be used (for initial login)*

Landing Page/Dashboard

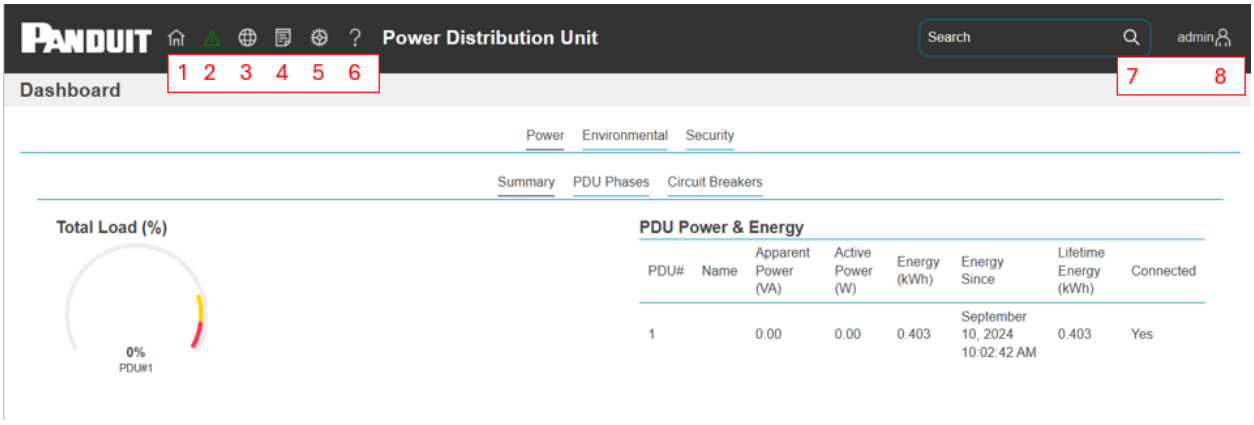
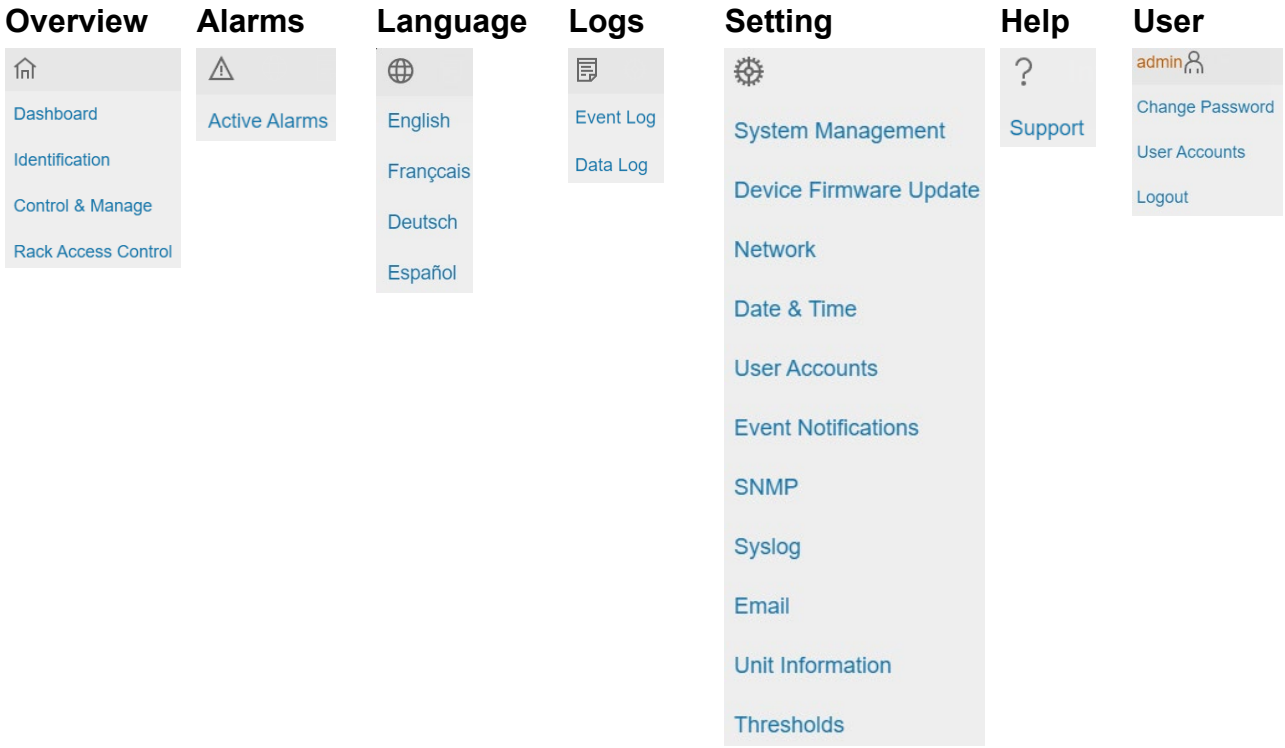


Figure 9: Landing Page/Dashboard

Number	Icon	Description
1		The home icon provides an overview of the PDU with access to the Dashboard, Identification, Control & Manage and Rack Access Control.
2		The Alarm icon provides details of the active alarms.
3		This icon lets you select a Language. There are seven languages available to choose from: English, French, German, and Spanish
4		This icon provides the logs of the PDU, which can be viewed and downloaded.
5		The settings icon allows a user to set up the Network Settings, System Management, SNMP, Email Setup, Trap Receiver, User Accounts and Thresholds.
6		Help and Support about the PDU can be found using this icon. MIB and User's manual are under this icon.
7		The search icon allows you to input key words and search for the related results.
8		This icon shows who is logged in (user or admin). Account passwords can be changed, and user accounts managed through this page.

Menu Dropdowns



Introduction to the Dashboard

Power Summary Page

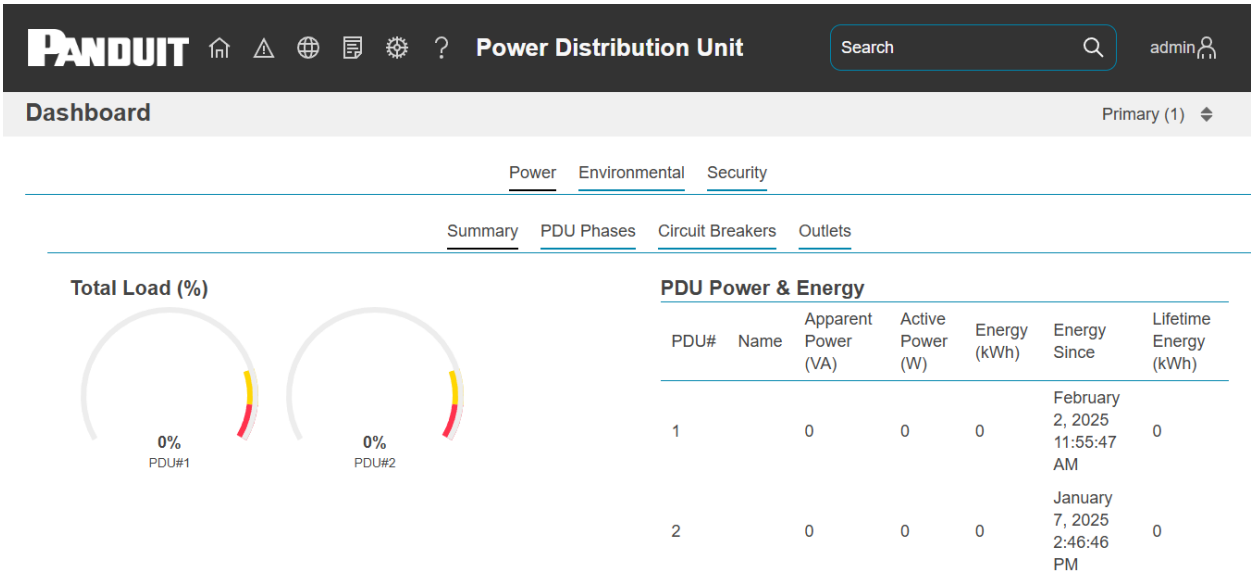


Figure 10: Power Summary Page

Power Outlets Page

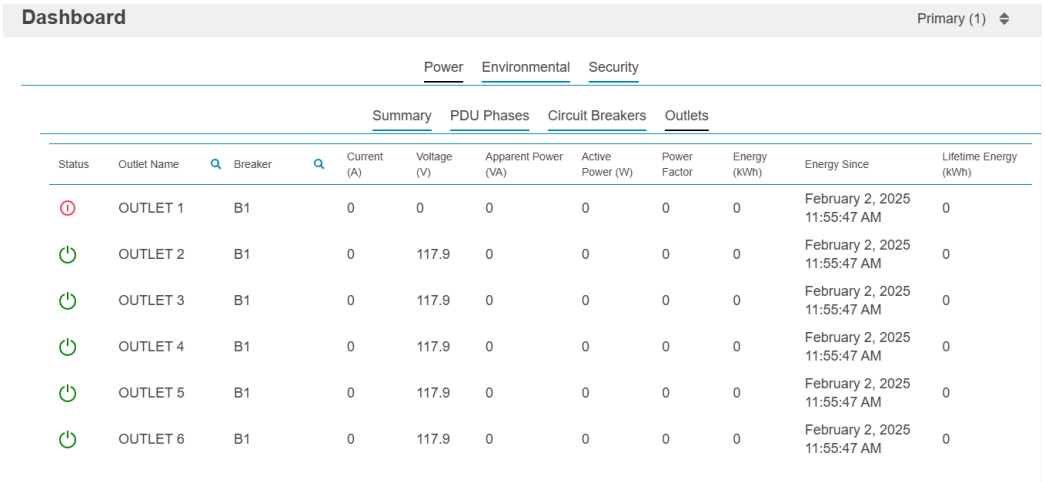


Figure 11: Power Outlets Page

Environmental Monitoring Page

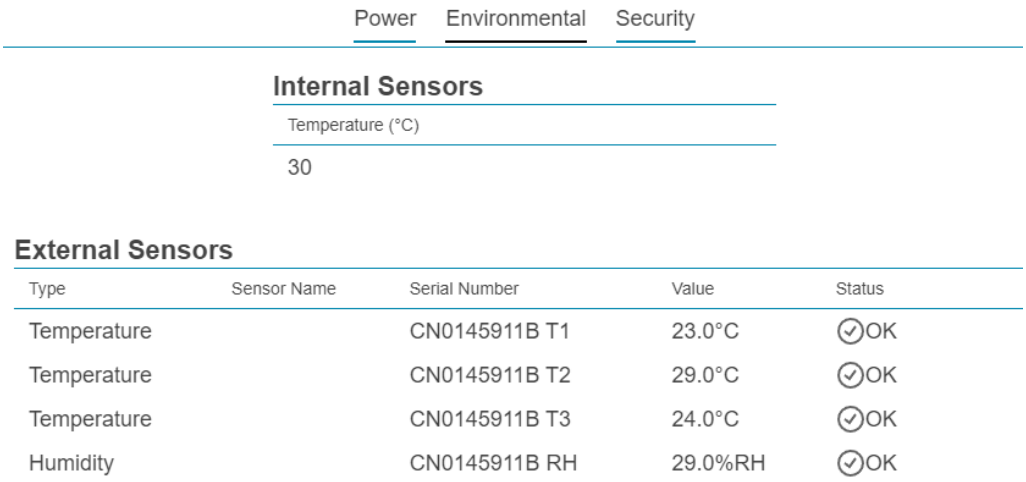


Figure 12: Environmental Monitoring Page

PARAMETER	DESCRIPTION
Type	Temperature, Humidity, Spot, Rope
Sensor Name	User configurable sensor name
Serial Number	Sensor Serial number
Value	Sensor reading
Status	Normal, Exceeds Thresholds, Alarms

Security Monitoring Page

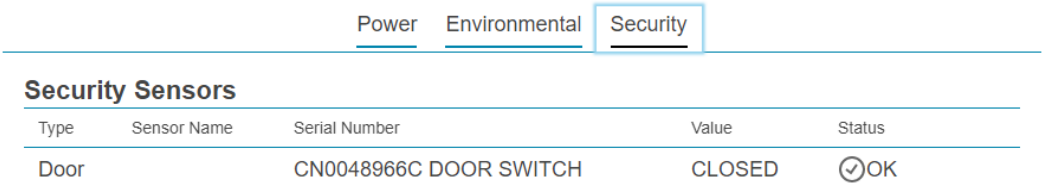


Figure 13: Security Monitoring Page

Note: See Section 8 for complete details on configuring PDU Security Settings.

System Management Information

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

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

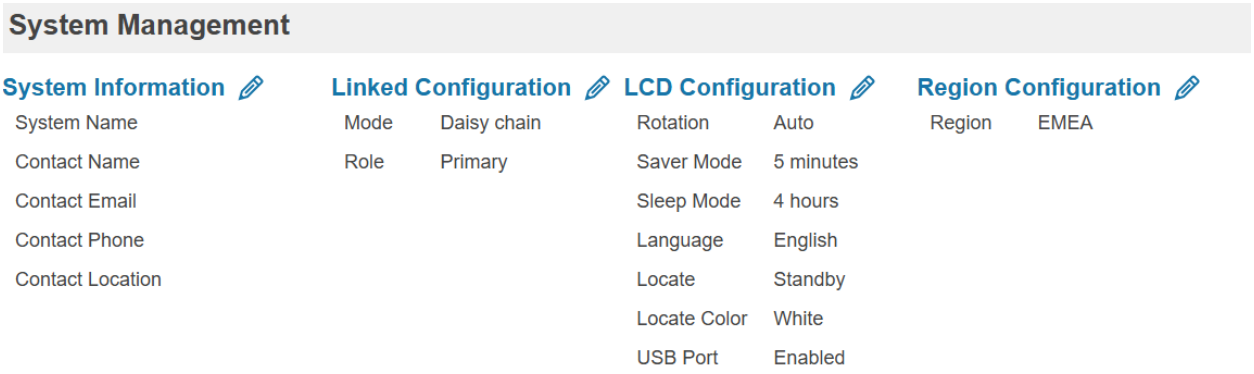


Figure 14: System Management

System Information

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

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

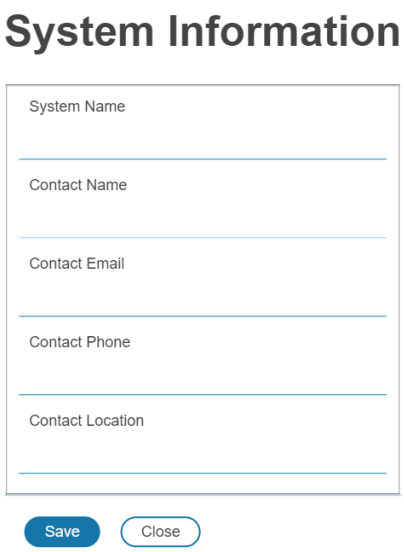


Figure 15: System Information Configuration

2. Enter the **System Name**
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**.

LCD Configuration

The LCD Configuration allows customization of LCD settings.

1. System Management → LCD Configuration

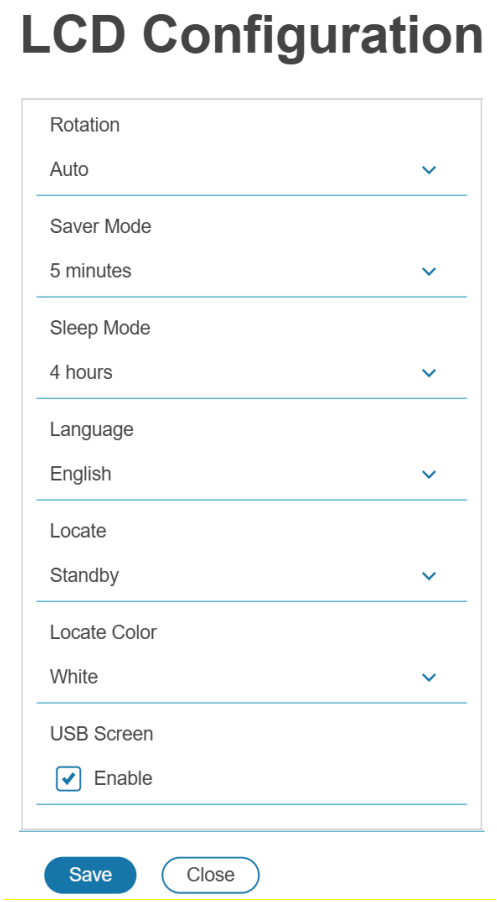


Figure 16: LCD Configuration

2. Select the **pencil** icon next to **LCD Configuration.**
3. Choose Rotation: Auto uses an accelerometer to automatically choose the rotation. Most installations should use Auto, otherwise select the rotation of the screen in degrees.

4. Choose Saver Mode: Select the time before LCD rotates between summary screens or disabled to disable summary screens.
5. Choose Sleep Mode: Select time before LCD screen is turned off or disabled to prevent the LCD from turning off. A shorter time reduces power usage and extends LCD life.
6. Choose Language: Select the language used on the LCD.
7. Press **Save**.

PDU Locate

Provides a method of locating a specific PDU by flashing the LCD screen with the chosen color.

1. Select the pencil icon next to LCD Configuration.
2. Change Locate to Locate On.
3. Choose color of LCD screen flash.

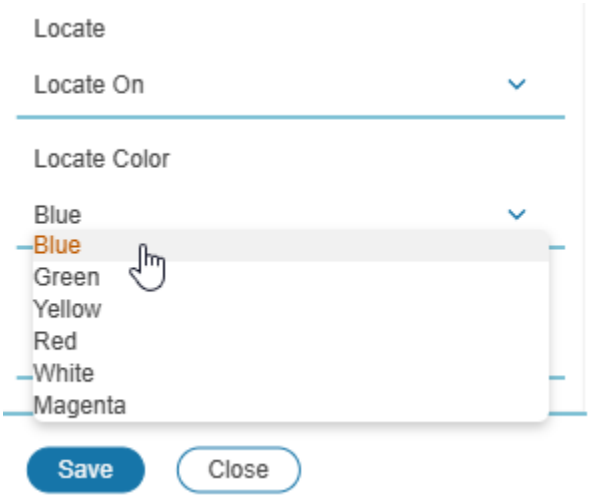


Figure 17: PDU Locate

4. Press Save.

To stop the PDU from flashing Restore Locate setting to Standby in Web UI.

Region Configuration

If the PDU is a dual rated PDU, the region can be changed between North America and EMEA to get the correct PDU ratings.

1. Select the pencil icon next to Region Configuration.
2. Choose Region.

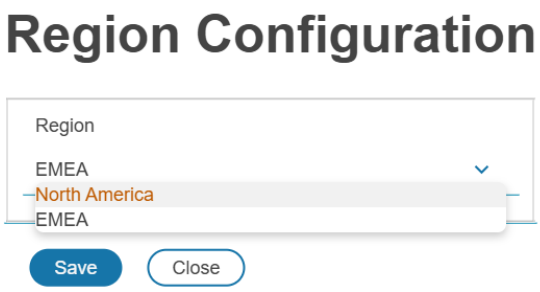


Figure 18: PDU Region

3. Press Save.

Network Settings

Network Settings allow management of IP Configuration, DNS, Web Access, SSH Configuration and other network settings.

Ethernet Interface Configuration:

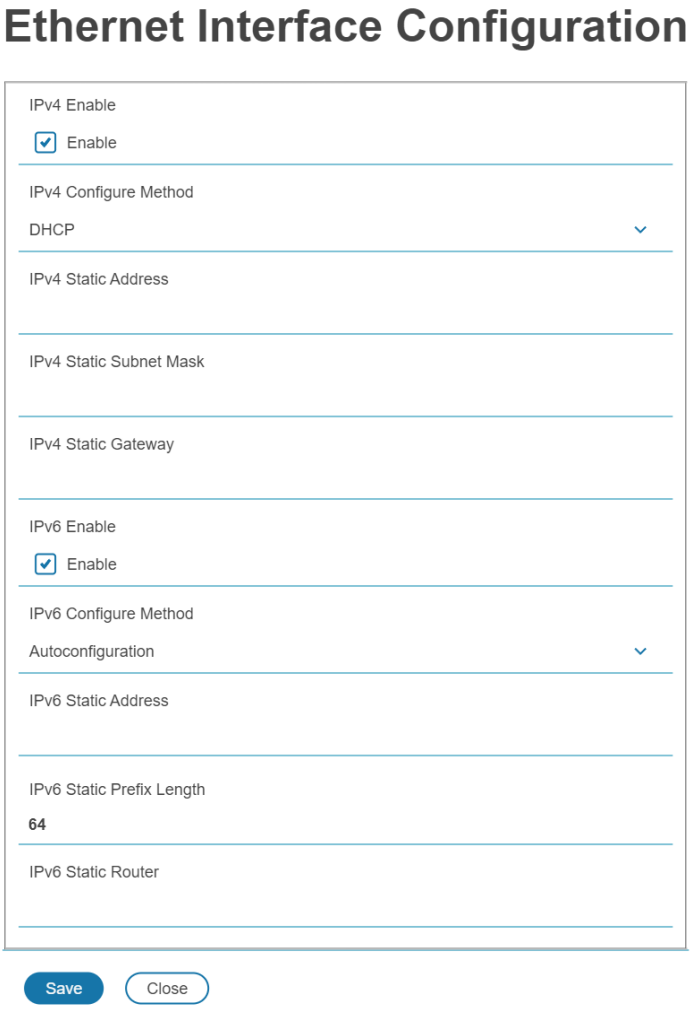


Figure 19: Ethernet Interface Configuration

DNS configuration:

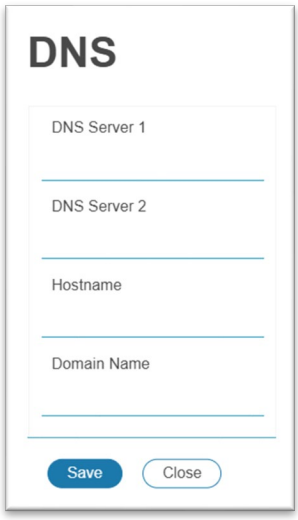


Figure 20: DNS Configuration

Web Access Configuration

Web Access Configuration is used to set HTTP and HTTPS. Also, this section will be used to upload HTTPS Certificates.

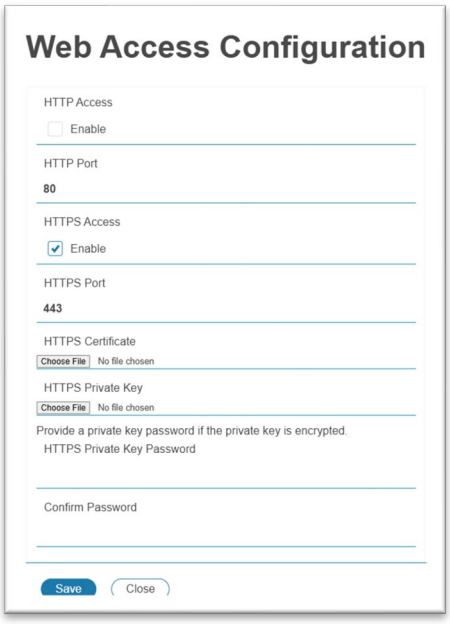


Figure 21: Web Access Configuration

Uploading Custom TLS certificate.

The product comes with a default RSA 2048-bit private key and certificate. It is recommended that a user uploads their custom TLS certificate for improved security.

1. Select the **Network Setting** folder from the Settings icon.

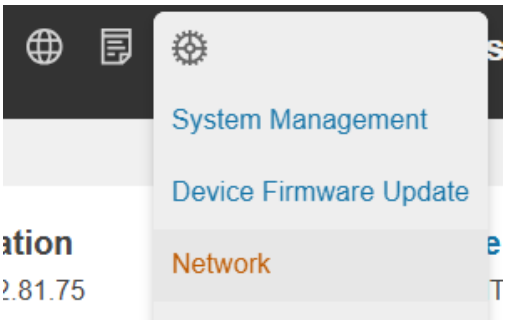


Figure 22: Network Settings

2. Select the pencil on the **Web Access Configuration**

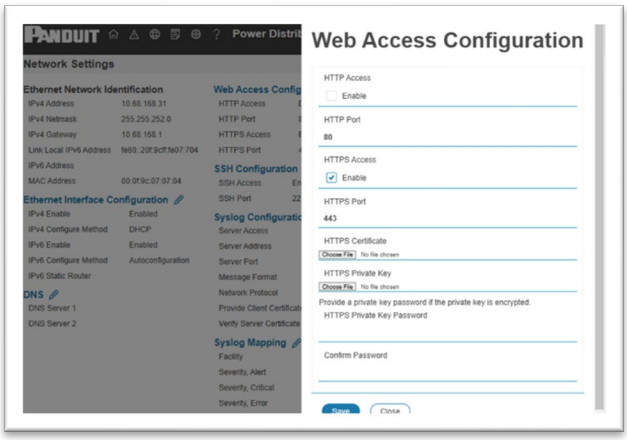


Figure 23: Web Access Configuration

3. Select the **Choose File** button to select the SSL Certificate and the SSL Certificate Key.

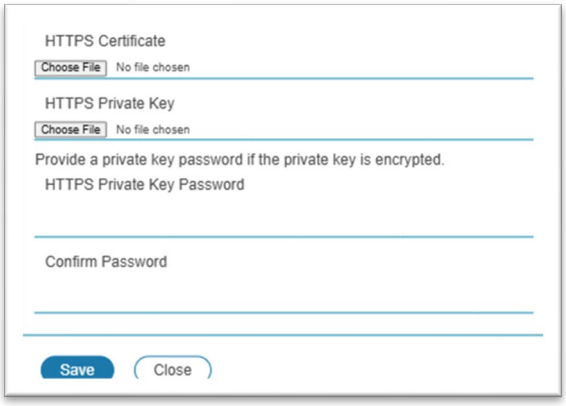


Figure 24: Upload Certificates

4. If the certificate is encrypted with a passcode, enter the **Passcode** and then confirm the passcode in the **Passcode** filed
5. Select **Save** to upload the certificate and key.

SSH Configuration:

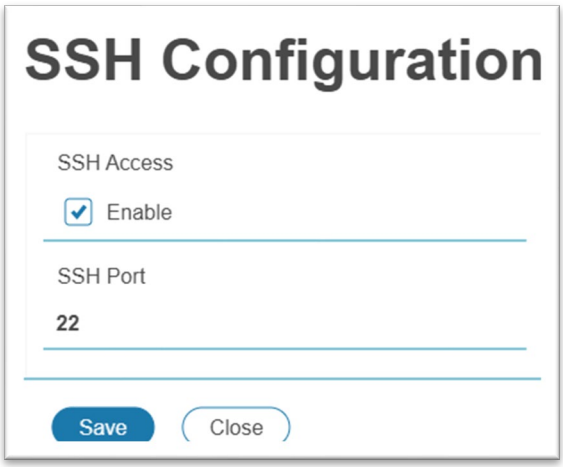


Figure 25: SSH Configuration

IEEE 802.1X Configuration:

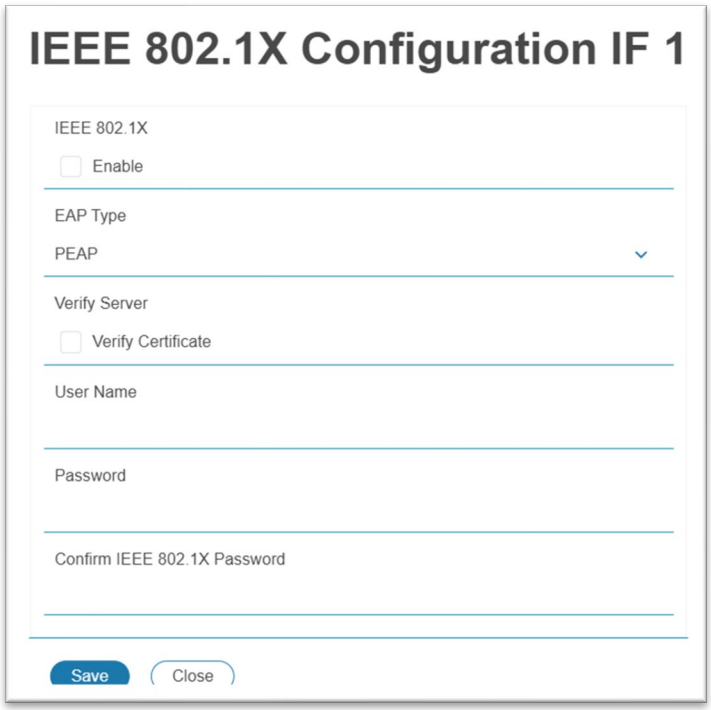


Figure 26: IEEE 802.1X Configuration

Unit Information

The unit information is a way to distinguish each individual PDU in the system and location inside the data center.

To configure the system management information, select **Unit Information** under the **gear** icon.

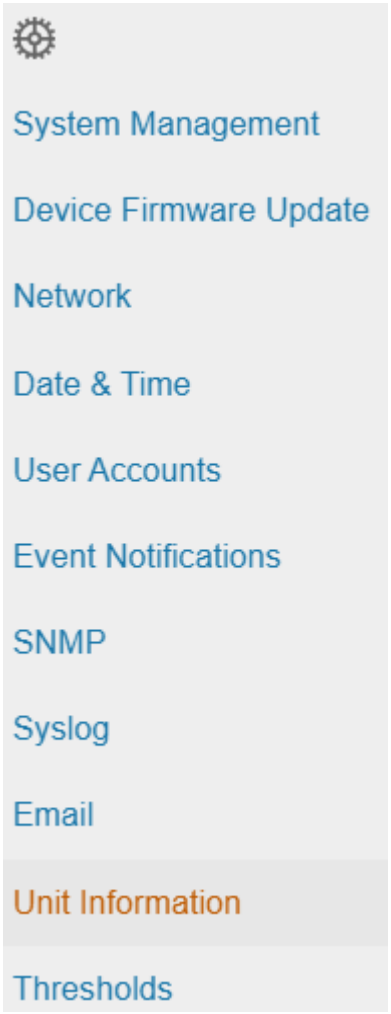
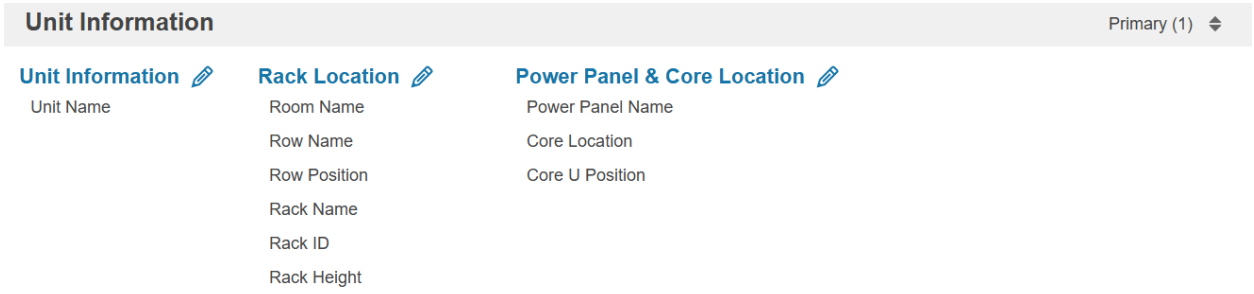


Figure 27: Unit Information

Choose the PDU in a daisy chain you wish to configure with the using the dropdown menu located on the right side of the screen. If the PDU is configured for Stand alone mode, the dropdown menu will not be present.



Unit Information

The Unit Name in the Unit Information tab will identify the name of the specific PDU

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.**

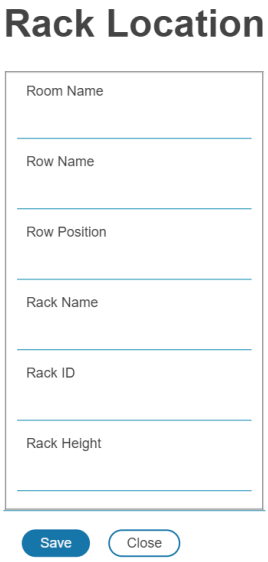


Figure 28: Rack Location Configuration

2. Enter the room location of the rack or cabinet that contains the PDU 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 what the power source each PDU is connected to. 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**.

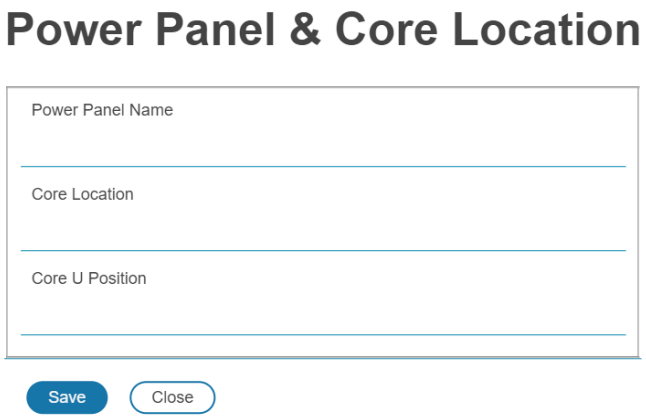


Figure 29: Power Panel & Core Location

2. Enter the name of the Power Source 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 NMCs are installed. For vertical PDUs, they are typically installed in the back.
4. Enter the rack unit (RU) location into the **Core U Position**. Vertical PDUs are usually installed in the 0 RU space.
5. Press **Save**.

Setting Time and Date on the NMC

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 **Time & Date** and select **Date/Time Configuration**.

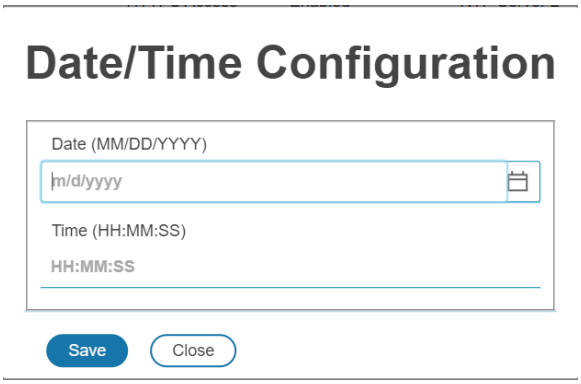


Figure 30: Setting the Date and Time

2. Enter the date using the MM/DD/YYYY 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**.

Configure Network Time Protocol (NTP)

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

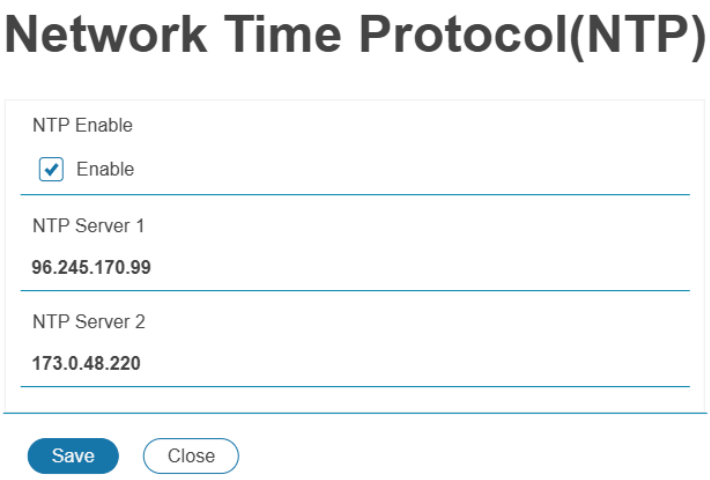


Figure 31: NTP Configuration

2. Click **Enable** to enable NTP.
3. Enter the hostname or IP address of the primary NTP server in the **Primary NTP Server** field.

4. Enter the hostname IP address of the primary NTP server in the **Secondary NTP Server** field.
5. Press **Save**.

Time Zone Configuration

1. Go to **Time & Date** and select **Time Zone Configuration**.

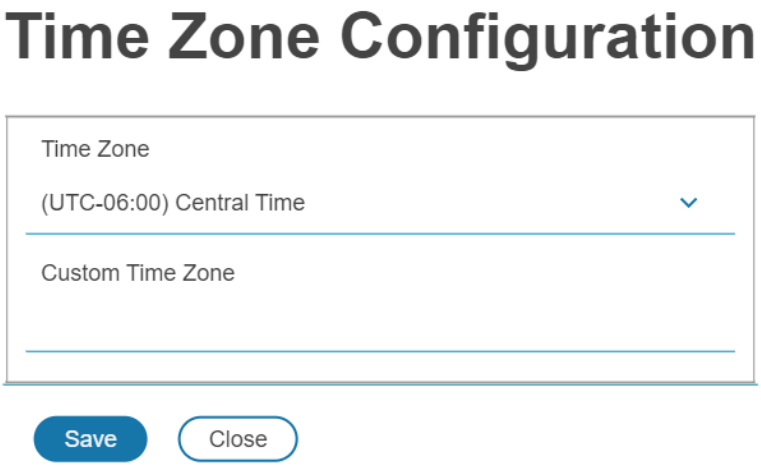


Figure 32: Daylight Saving Time Zone Configuration

2. Select a predefined time zone from the pull-down menu.
3. If the desired time zone is not in pull down menu, enter the TZ identifier from the IANA time zone database (https://www.iana.org/time-zones) in the **Custom Time Zone**:

   A list of time zones can also be found in https://en.wikipedia.org/wiki/List_of_tz_database_time_zones.

Network Time Protocol (NTP) Test

The Network Time Protocol Test allows the user to verify the connectivity to the NTP server. To verify the connection, follow these steps.

1. Click on the pencil next to the Network Time Protocol (NTP) Test.
2. Select Start Test and click save

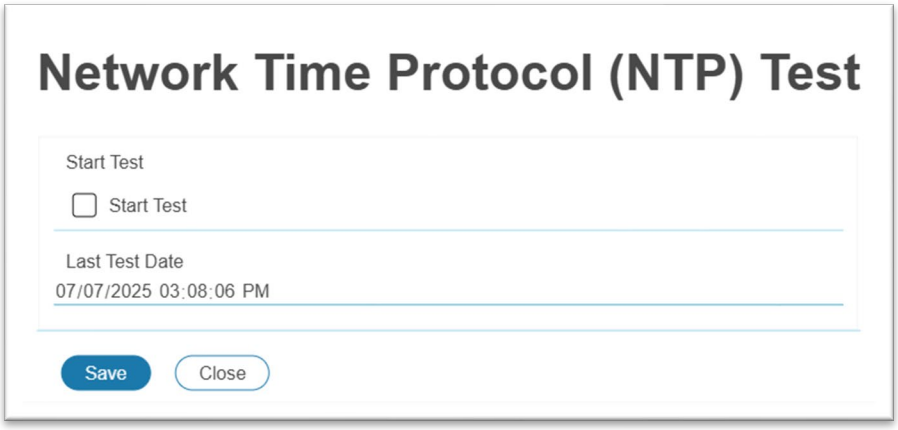


Figure 33: Starting NTP Test

3. Wait for the test to be completed.
4. The statue will be displayed under the Network Time Protocol (NTP) Test section.

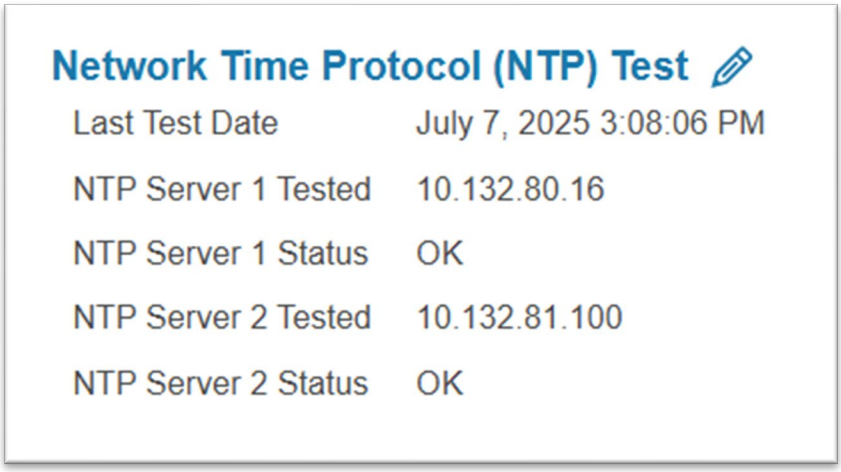


Figure 34: Status of NTP Test

Control & Manage

The Control and Manage section of the Web GUI is where the user is able to perform operations based on the PDUs functionality. You can control the outlets, reset PDU Energy and per-outlet Energy meters. The EL2P series of PDUs introduces outlet sequencing feature. This feature enables the user to control the sequence order of when the outlets are powered on.

To access the control & manage section select **Control & Manage** from the Home Icon.

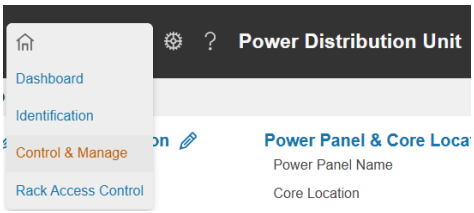


Figure 35: Control & Manage

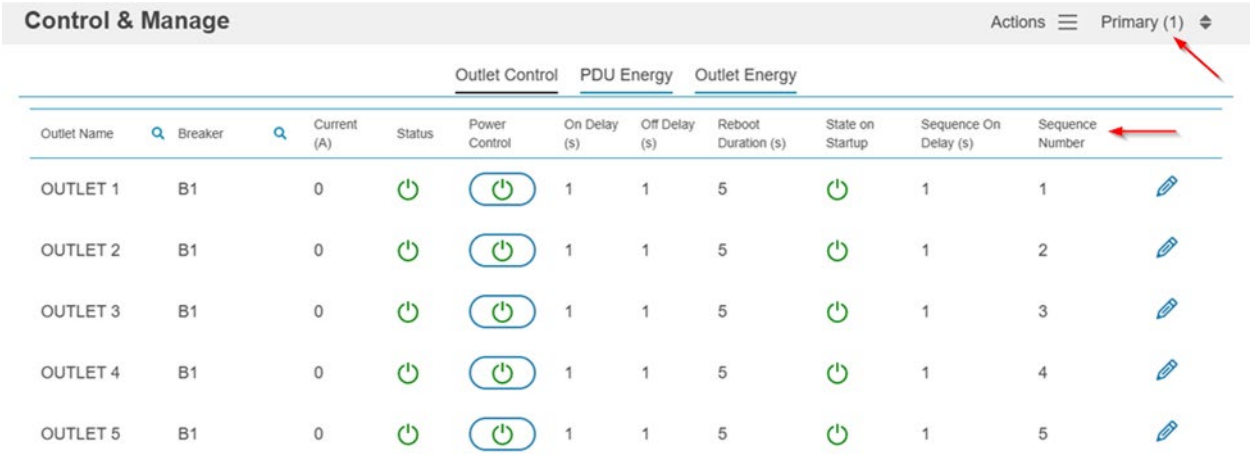


Figure 36: Control & Manage default page view

Outlet Power Management

Outlet Status

For Panduit PDUs with outlet level control the **Status** of the outlet represents the state of the outlet.

Note: The user must select the PDU they wish to control from the dropdown menu (refer to Figure 37).

On: Outlet is on

Off: Outlet is off

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. On the Control & Manage page, expand the **Outlet Control tab.**

2. Open the **Outlet Configuration** dialog for the by clicking the pencil icon on the same line as the outlet to name.
3. In the dialog, select the value field for the Outlet Name.
4. Delete the default name and type the new name.
5. Press **Enter**.

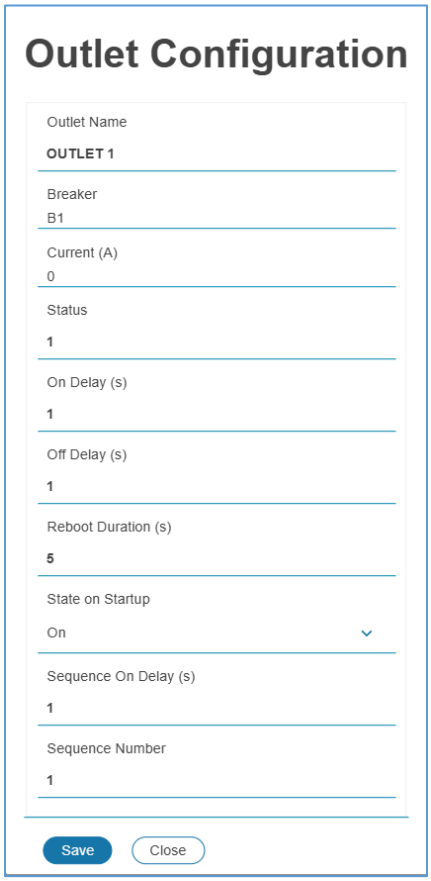


Figure 37: Outlet Naming, Time Delay, State on Startup or Reboot

*Note: When **Status** is 1, the outlet relay is on. When **Status** is 0, the outlet relay is off.*

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 Control** tab from the **Control & Manage** tab.
2. In the **Outlet Configuration** dialog, 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** menu item from the **Home** icon.
2. In the **Power Control** column, click the button for the outlet that must be switched on, switched off, or rebooted.
3. Select the desired **Power Control** from the dropdown menu.
    a. **Cancel** will stop delayed operations and retain the current outlet state.
    b. **Off** will immediately turn off outlet power.
    c. **Off Delayed** will wait the outlet's **Off Delay (s)** seconds and then turn off outlet power.
    d. **Reboot Delayed** will immediately turn off outlet power, wait **Reboot Delay (s)** seconds and then turn on outlet power.
    e. **Reboot Immediately** will immediately turn off outlet power, wait approximately ½ second and then turn on outlet power.
    f. **On** will immediately turn on outlet power.
    g. **On Delayed** will wait the outlet's **On Delay (s)** seconds and then turn on outlet power.

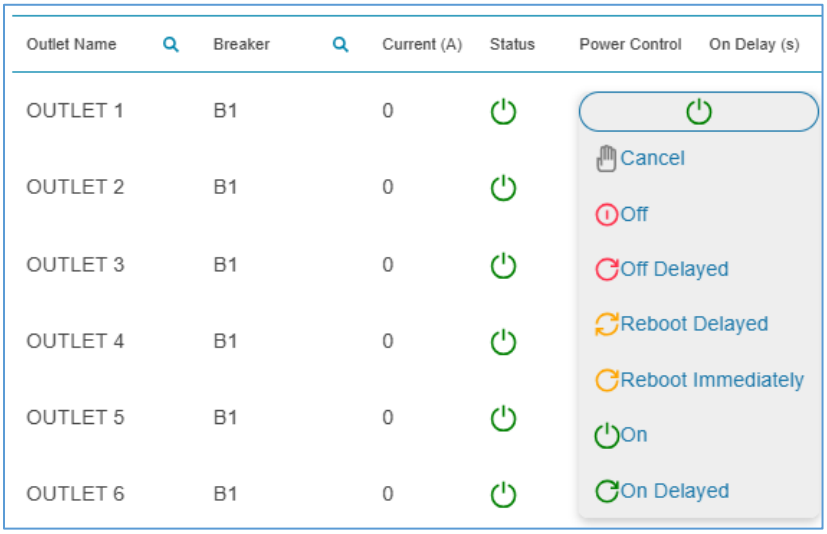


Figure 38: Outlet Control

4. A confirmation dialog is displayed.

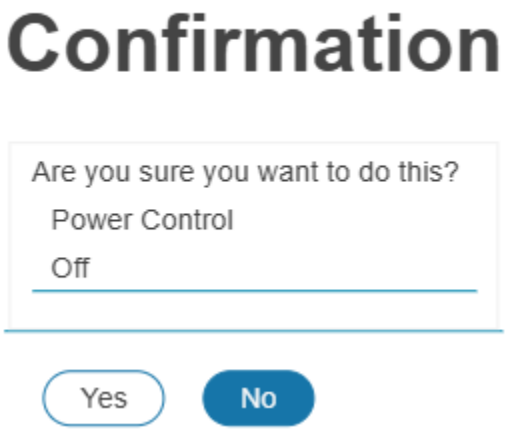


Figure 39: Outlet Control

Select Yes to apply the change. Select No to not apply the change.

Setting the Outlet Power On/Off/Reboot Delays for Panduit PDUs

This is only applicable to outlet-switched PDUs.

1. Select the **Home** Icon then **Control & Manage** from the drop-down menu in the Web UI.
2. Select the outlet for which to set a delay by clicking on the pencil icon.
3. Configure the length of the delay. Delay settings are described in the section *Switching an Outlet On or Off.*
    a. Note: a delay of 0 seconds will result in the delay being approximately as fast as the system can process the requested operation.
4. Select **Save.**

Outlet Control Enable/Disable

The **Outlet Control** Enable/Disable feature allows/prevents all user interfaces from changing the **Power Control** state for all outlets. Note: **Power On State** will still be applied appropriately.

1. Select the **Home** Icon then **Control & Manage** from the drop-down menu in the Web UI.
2. Select the **Outlet Control** menu from the **Actions** menu.

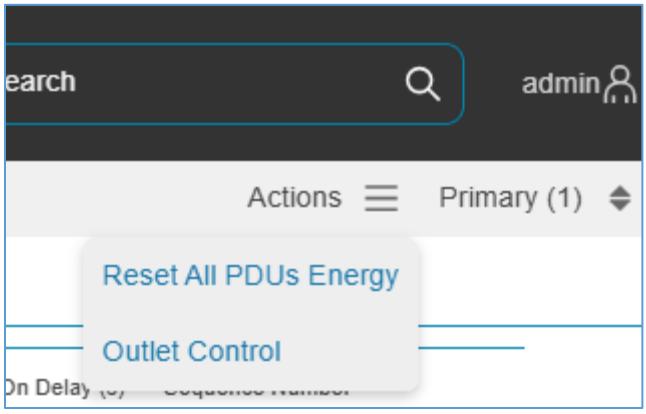


Figure 40: Outlet Control menu item

3. Select the Outlet Control Enabled/Disabled state.

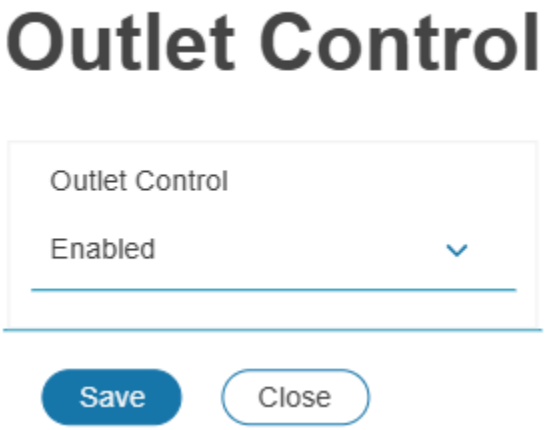


Figure 41: Outlet Control enable/disable dialog

4. Select **Save** to apply the change.

Outlet Power Sequence Setup

The outlets can be programmed to have a pre-determined on delay based on the PDU selected. (E.g. **Sequence 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.) By default, the “Sequence On Delay” and “Sequence Number” are 1 for all outlets. This provides a 1 second delay between turning on each outlet in sequence from the lowest numbered outlet to the highest numbered outlet.

When power is restored after a power loss, the outlet relay state is restored based on the “State on Startup” setting. The lowest “Sequence Number” is adjusted first. If outlets

share the same Sequence Number, the lowest indexed number state is applied first. If the State on Startup will turn on the outlet power and it is transitioning from off to on the outlet waits the “Sequence On Delay” seconds before turning on.

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

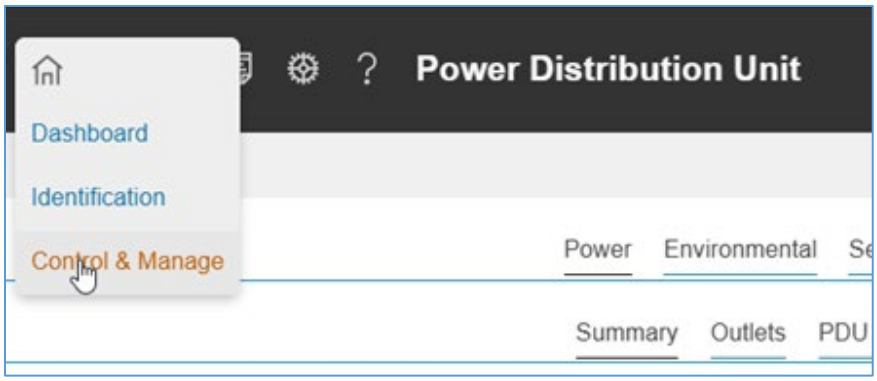


Figure 42: Control & Manage PDU

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

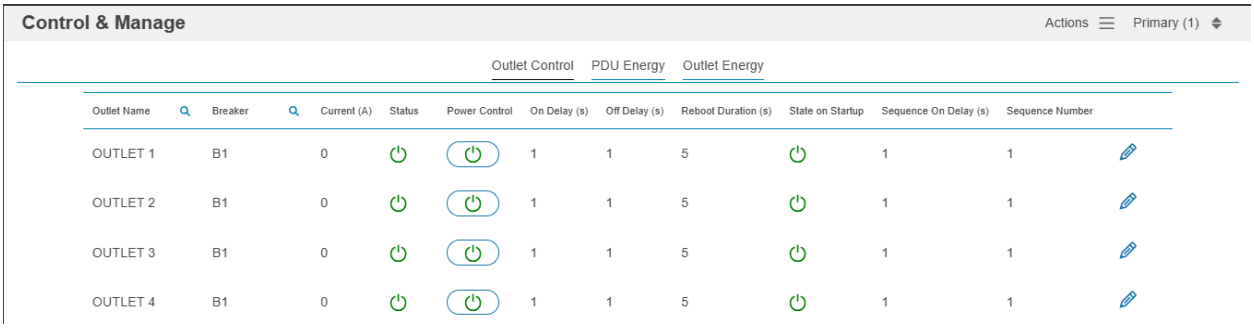


Figure 43: Edit Outlets

3. In the Edit Outlet window enter the **Sequence On-Delay (s)** time (0-7200 seconds) then select **Save**.
    a. Note: a delay of 0 seconds will result in the delay being approximately as fast as the system can process the requested operation.

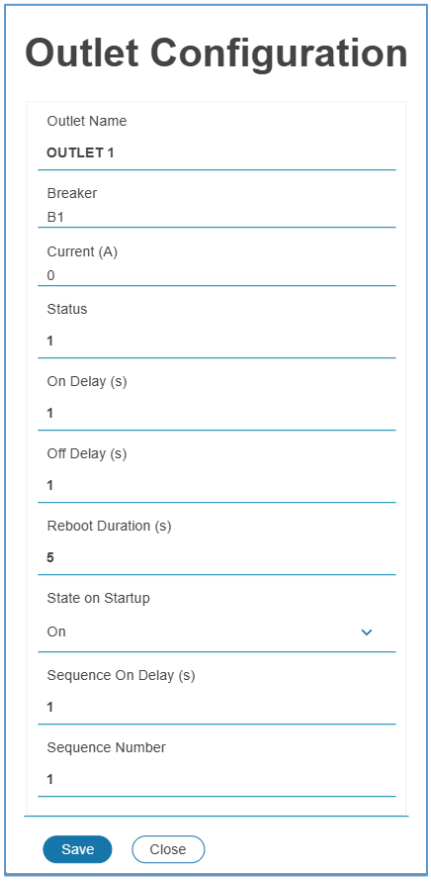


Figure 44: Sequence On-Delay Time

4. The Outlet Power Sequence has been set. Another option in the EL2P PDU is to simply set the sequence number with the sequence on delay.

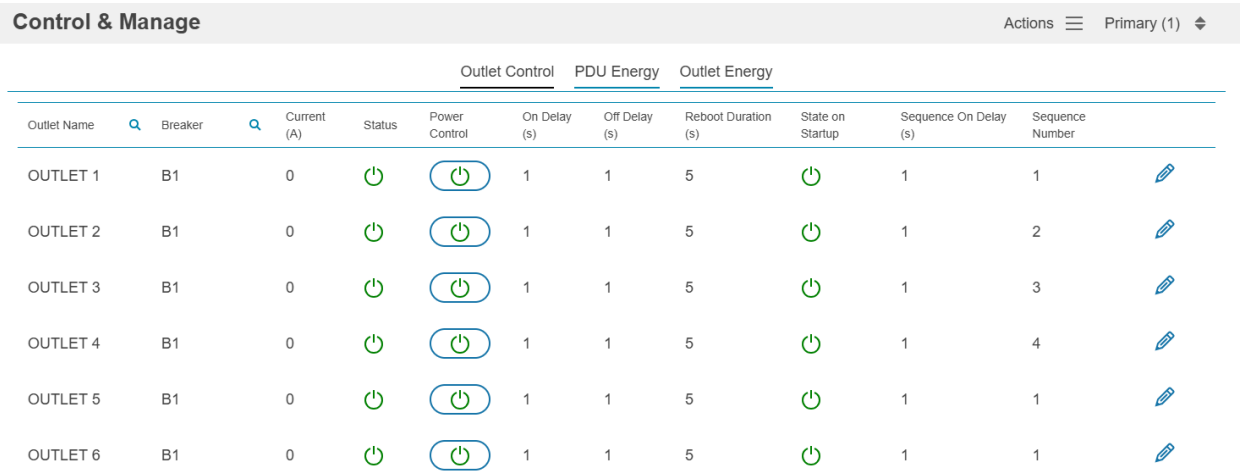


Figure 45: Saved Sequence

In this figure, when power is restored, outlets are turned on with 1 second between them in this order: 1, 5, 6, 2, 3, 4.

Reset All PDUs Energy

PDUs with energy monitoring accumulate energy since the energy meters were last reset. Every resettable PDU Energy meter can be reset at the same time. This includes input and per-outlet Lifetime Energy meters.

1. Select the **Home** Icon then **Control & Manage** from the drop-down menu in the Web UI.
2. Select the **Outlet Control** menu item from the **Actions** menu.

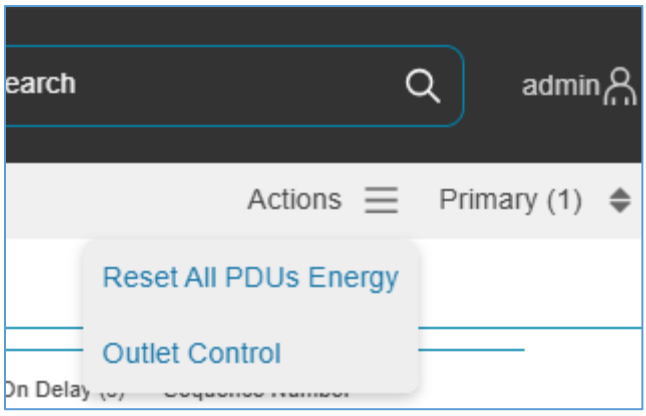


Figure 46: Reset All PDUs Energy menu item

3. Select Yes to reset all PDUs Energy.

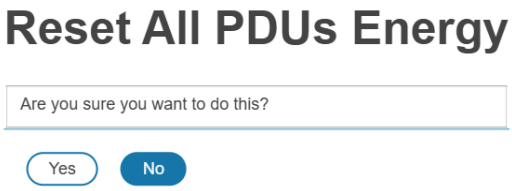


Figure 47: Reset All PDUs Energy dialog

4. If **Yes** was chosen, **Energy Since** will be set to the current date/time and the associated **Lifetime Energy** measurements will reset to zero.

PDU Energy

PDUs with input energy monitoring will show the **Lifetime Energy** accumulated since the **Energy Since** date/time.

1. Select the **Home** Icon then **Control & Manage** from the drop-down menu in the Web UI.
2. Select the **PDU Energy** tab.

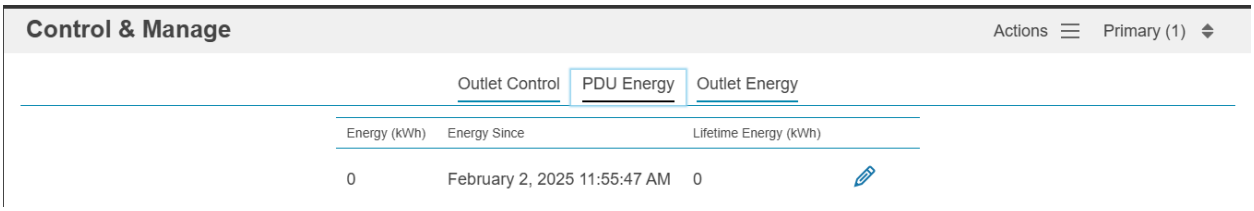


Figure 48: PDU Energy

Reset PDU Energy meter

Individual **PDU Energy** monitors can be reset.

1. Select the pencil icon next to an energy meter to display the **PDU Energy Configuration** dialog.

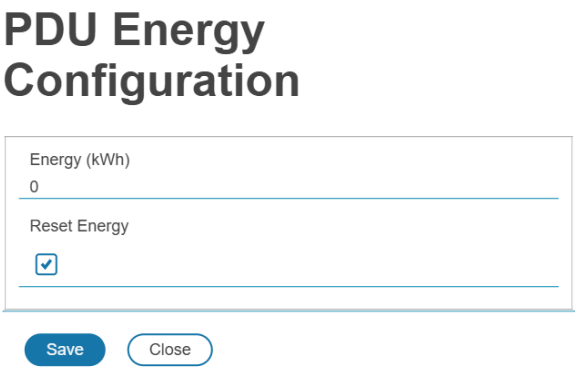


Figure 49: PDU Energy Configuration

2. Select the checkbox under **Reset Energy**.
    a. Select **Save** to reset the Lifetime Energy measurements for that meter.
    b. Or select **Close** to not apply the change.

Outlet Energy

PDUs with per-outlet energy monitoring will show the **Lifetime Energy** accumulated since the **Energy Since** date/time for each outlet. Each outlet's energy meter can be reset.

1. Select the **Home** Icon then **Control & Manage** from the drop-down menu in the Web UI.
2. Select the **Outlet Energy** tab.

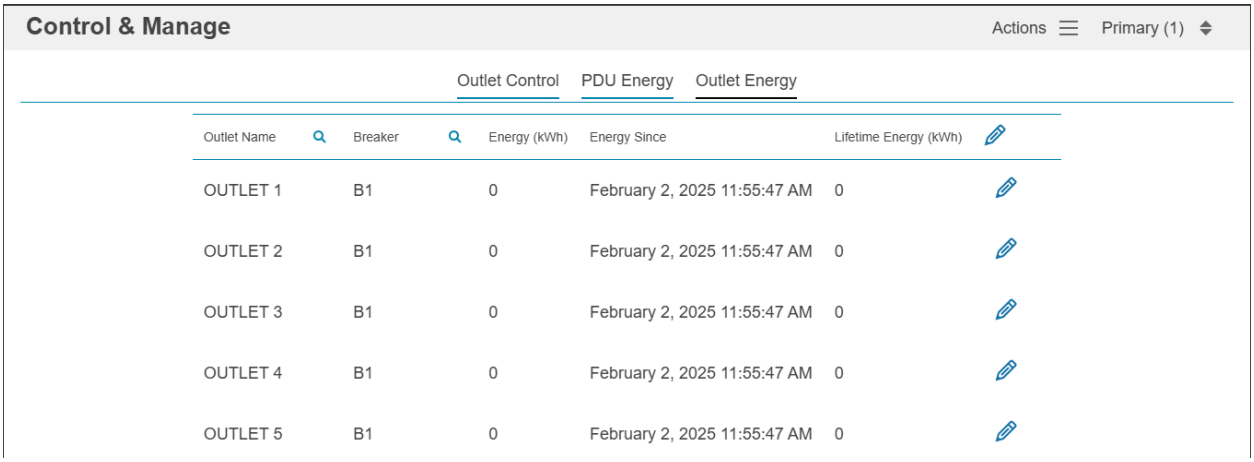


Figure 50: Outlet Energy

Reset Energy meter for all outlets on a PDU

1. Select the pencil icon next to **Lifetime Energy (kWh)** to show the Multiple **Outlet Energy Configuration** dialog.

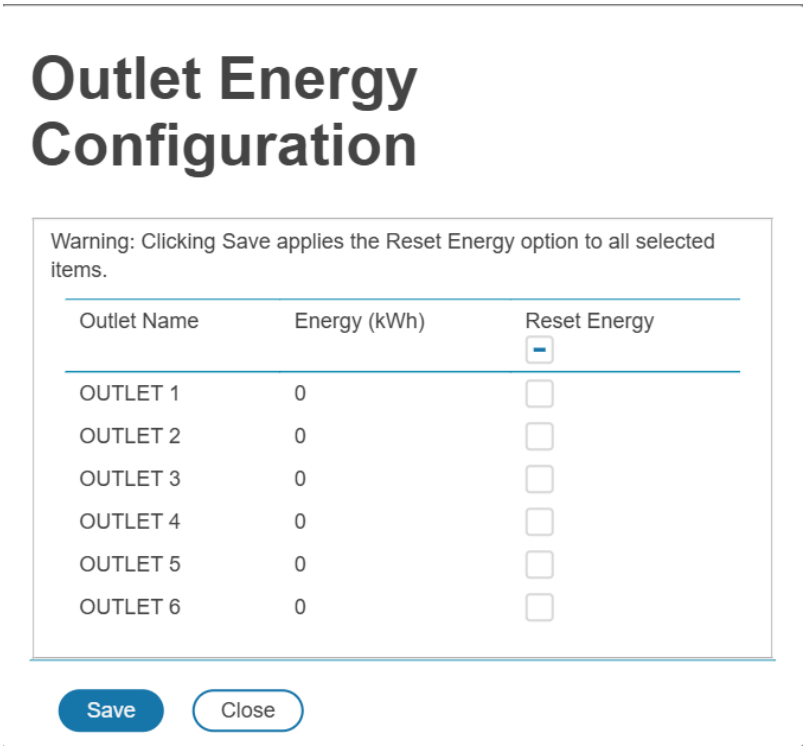


Figure 51: Multiple Outlet Energy Configuration dialog

2. Select the checkbox next to the individual outlets to be reset at the same time; or click the "-" checkbox under **Reset Energy** to quickly select all outlets or unselect them if all outlets are selected.

    a. Select **Save** to apply the changes.

    b. Select **Close** to not apply the change.

Reset Energy meter for one outlet

1. Select the pencil icon in each outlet row to show the per-outlet **Outlet Energy Configuration** dialog.

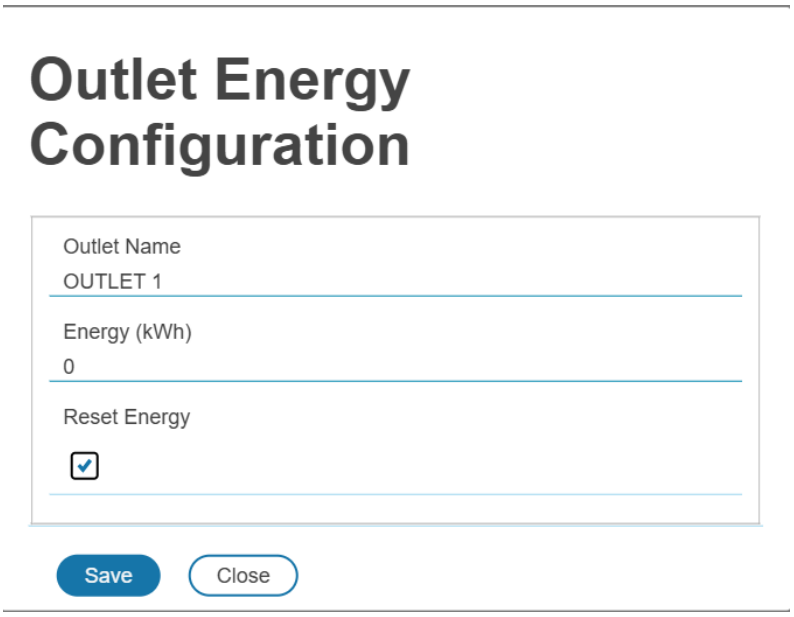


Figure 52: Outlet Energy Configuration

2. Select the checkbox under **Reset Energy**.
    a. Select **Save** to reset the Lifetime Energy measurements for that outlet.
    b. Select **Close** to not apply the change.

Setting Metering Thresholds

Threshold configuration can be found by selecting Thresholds in the Gear menu.

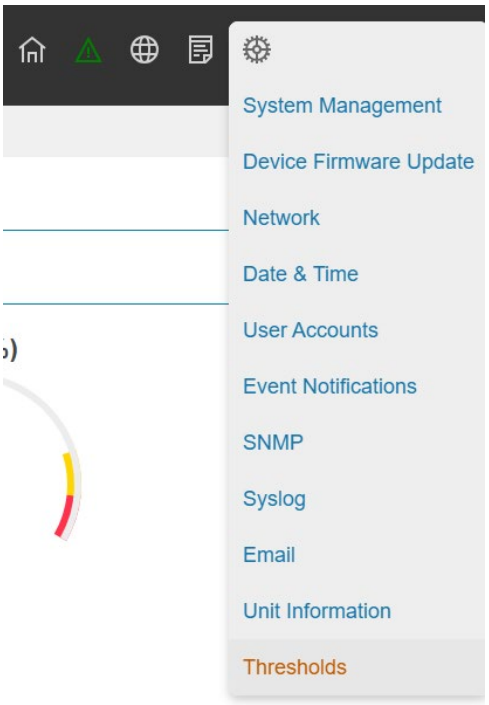


Figure 53: Threshold Settings

Thresholds are set individually for each PDU. Initial values are based on the characteristics of that specific model of PDU.

When viewing the threshold configuration, thresholds that are disabled are shown in gray with a strikethrough.

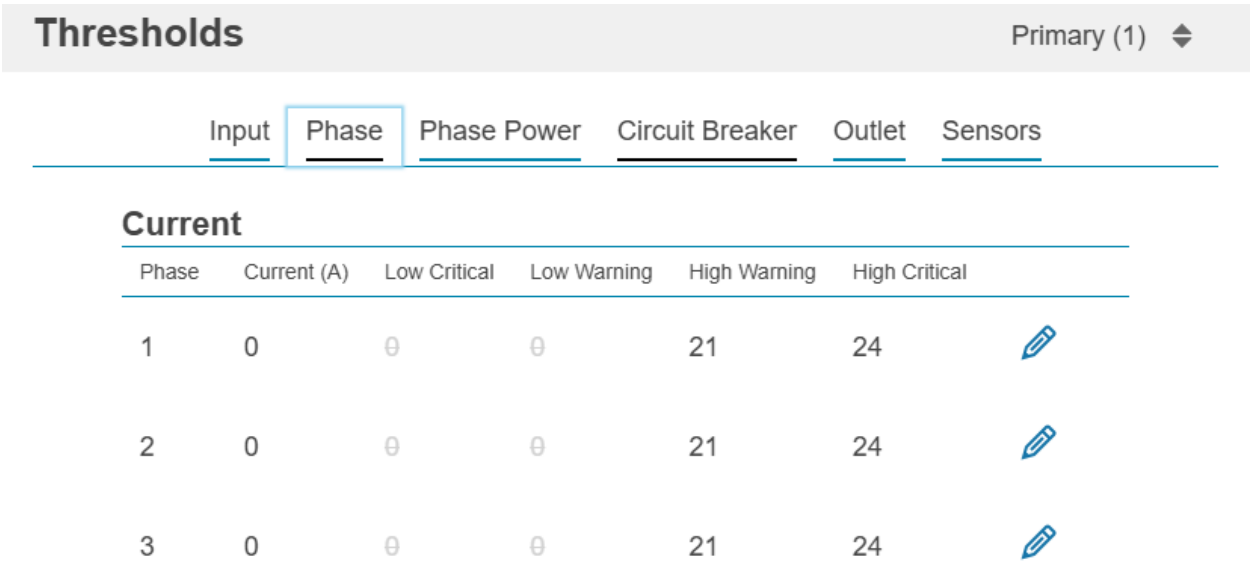


Figure 54: Threshold Configuration

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.

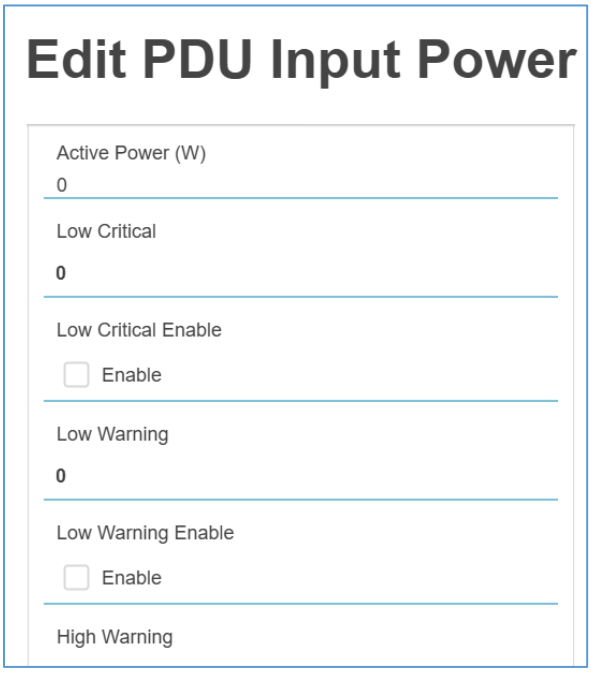


Figure 55: Power Threshold

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

   Low Critical (W)

   Low Warning (W)

   High Warning (W)

   High Critical (W)

4. Repeat steps 1 - 3 for all PDUs.

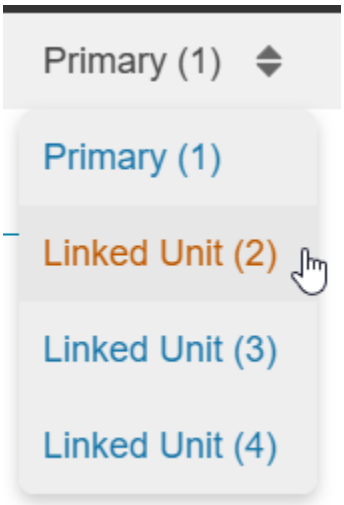


Figure 56: Selecting between Primary and Linked PDUs

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.

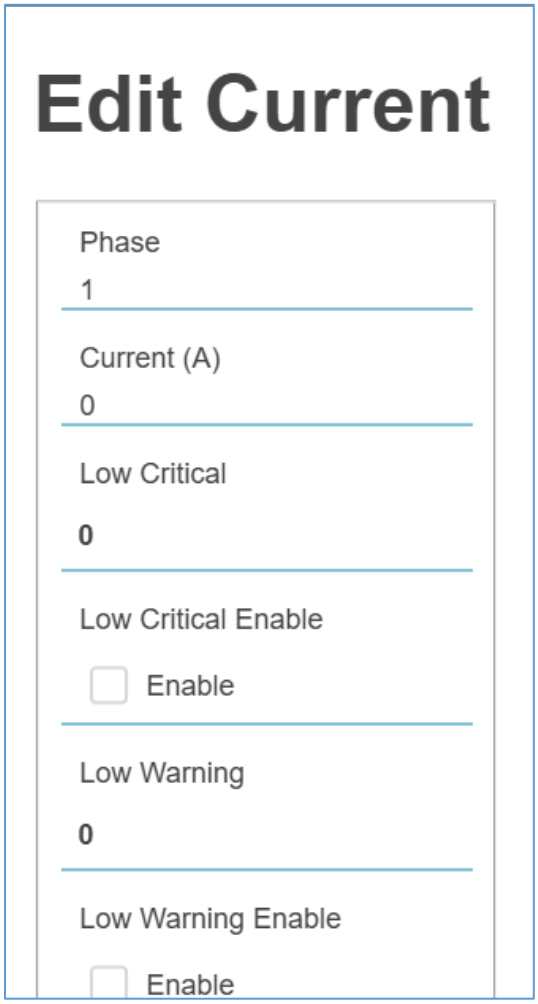


Figure 57: Phase Current Alarm

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

   Low Critical (A)

   Low Warning (A)

   High Warning (A)

   High Critical (A)

4. Repeat steps 1 - 3 for all phases and all PDUs.

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.

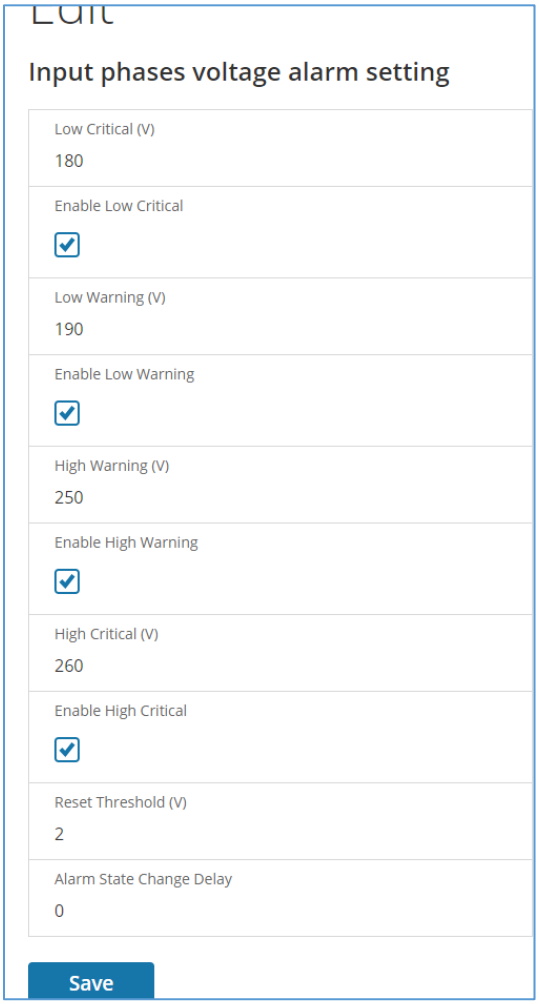


Figure 58: Phase Voltage Alarm

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

Lower Critical (V)

Lower Warning (V)

Upper Warning (V)

Upper Critical (V)

Reset Threshold (V)

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

Alarm State Change Delay (samples)

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

4. Repeat steps 1 - 3 for all phases.

Circuit Breaker Alarm Threshold

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

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

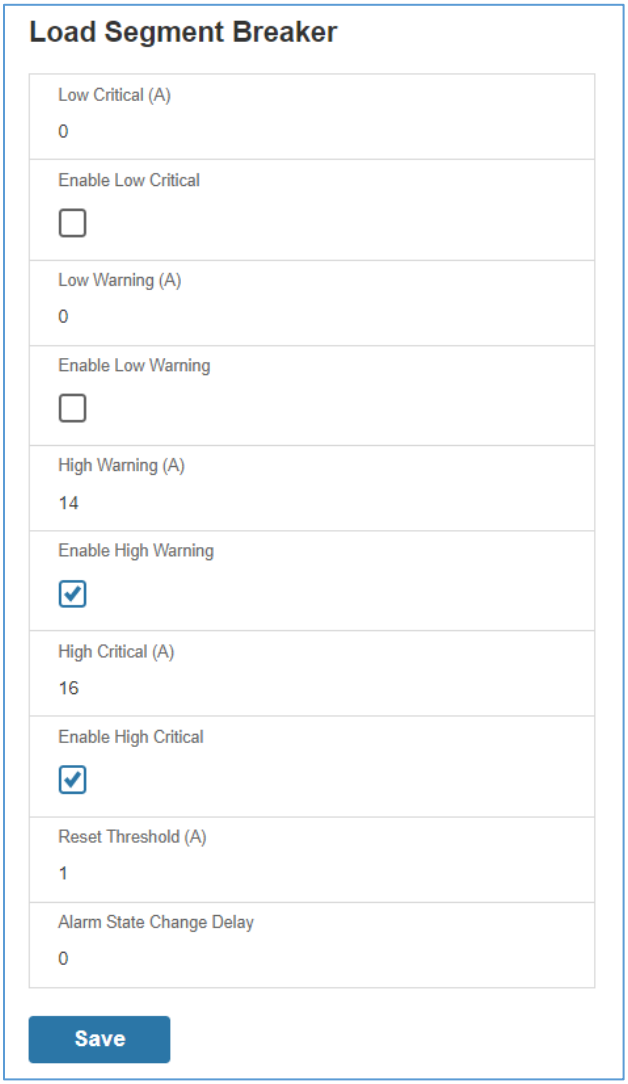


Figure 59: Load Segment Breaker

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

Lower Critical (A)

Lower Warning (A)

Upper Warning (A)

Upper Critical (A)

Reset Threshold (A)

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

Alarm State Change Delay (samples)

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

Repeat steps 1 - 3 for all circuit breakers.

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.

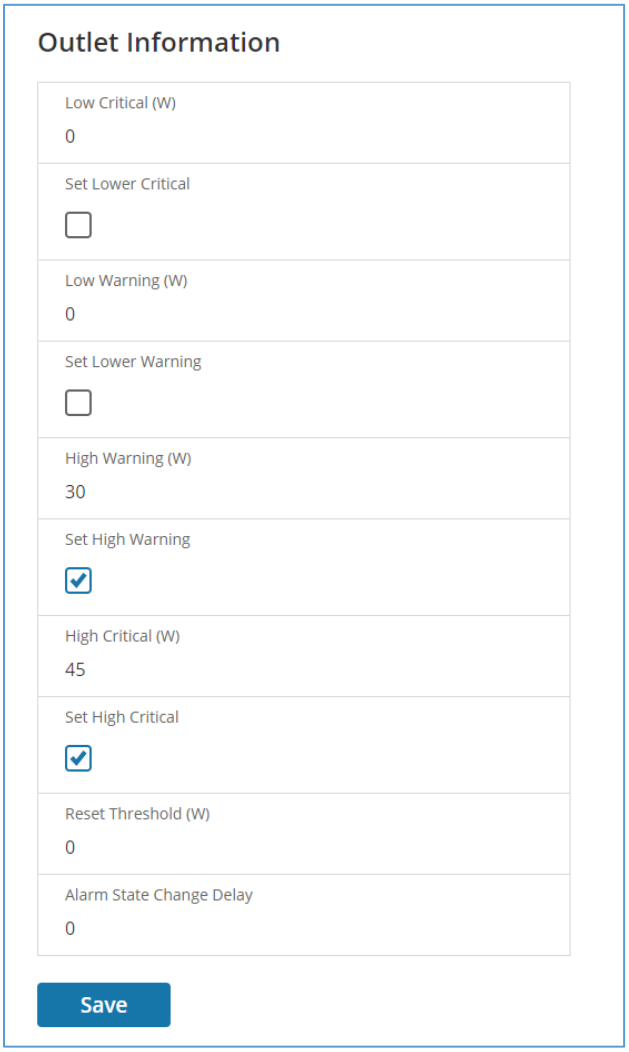


Figure 60: Outlet Information

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

Lower Critical (W)

Lower Warning (W)

Upper Warning (W)

Upper Critical (W)

Reset Threshold (W)

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

Alarm State Change Delay (samples)

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

Repeat steps 1 - 3 for all outlets.

Syslog Setup

The EL2P NMC can be configured to send syslog messages to a syslog server when an event occurs. To do this, the information about the Syslog server needs to be configured.

Syslog Server Configuration

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

Figure 61: Email Setup

2. Select the pencil icon next to **Syslog Configuration** and begin filling out the **Edit** screen.

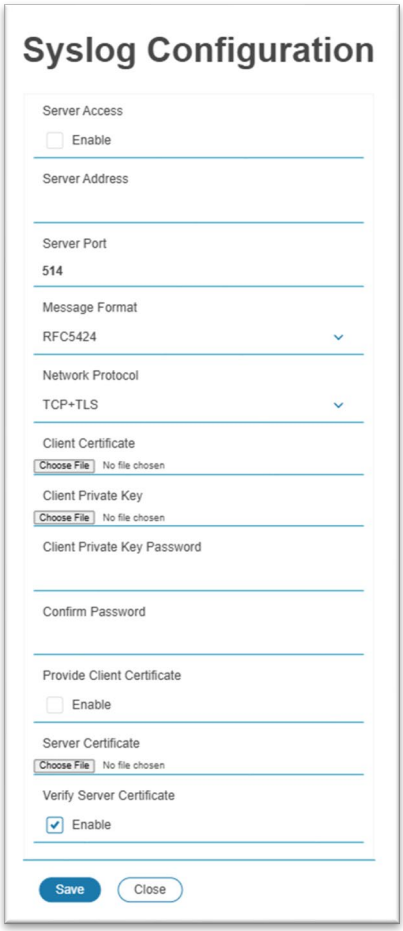


Figure 62: Syslog Configuration

- Set the **Server Address**. This is the address of the Syslog server that is going to accept the messages.
- Select the **Message Format.** It can be the RFC3164 format or the RFC5424 format.
- Configure the **Port** number. The port number is the communication endpoint on the server. The default is 514. Other common Syslog ports are 6514.
- Set the **Network Protocol.**
    - **UDP –** The message will be sent using the UDP protocol.
    - **TCP –** The message will be sent using the TCP protocol.

- **TCP+TLS** The message will be sent using the TCP protocol encrypted with TLS.

- If TCP+TLS is selected, Clients Private Key Password or Client Certificate can be entered.

3. Press **Save** when done.

Syslog Mapping

The Syslog Facility and Severity fields can be mapped to other values to allow for easier traceability on the Syslog sever. To edit the field

1. Select the pencil next to the Syslog Mapping.
2. Update the fields on the configuration menu.

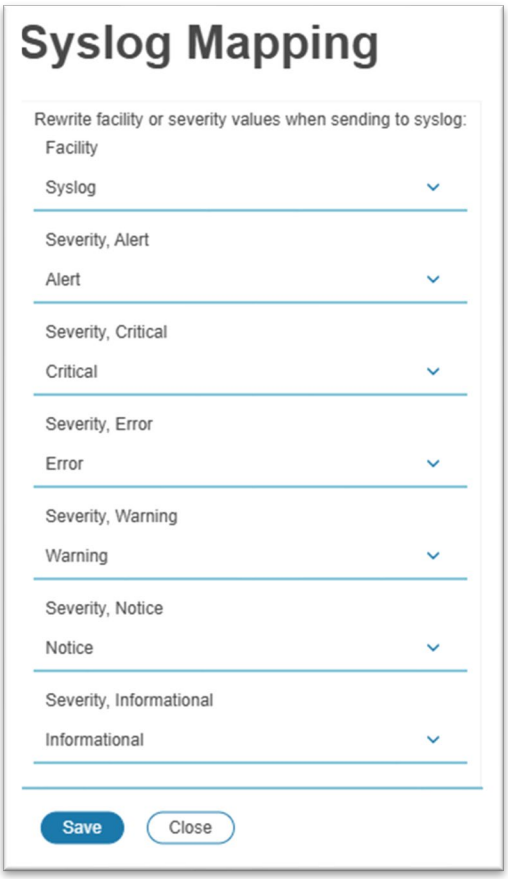


Figure 63: Syslog Mapping

3. Select save to apply the settings.

Email Setup

The Panduit NMC 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.

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

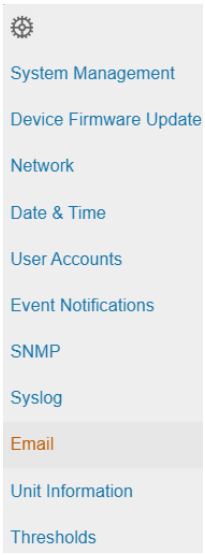


Figure 64: Email Setup

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

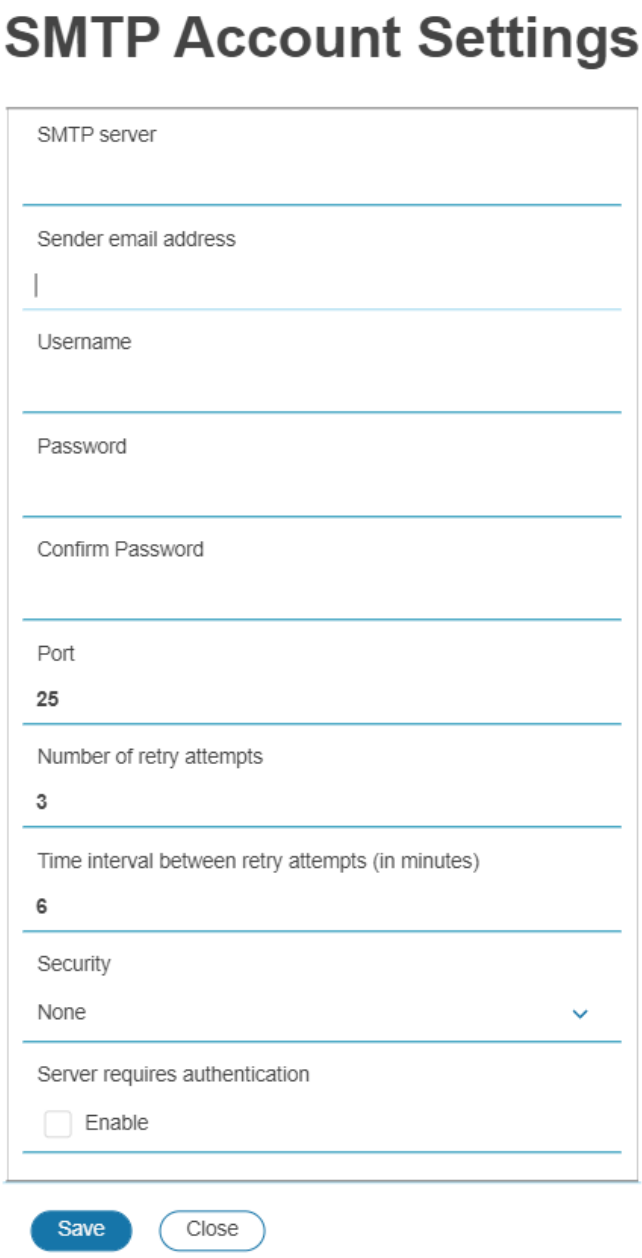


Figure 65: SMTP Account Settings

- Set the **SMTP server**. This is the address of the SMTP relay server that is going to accept the messages.
- Set the **Sender email address.** This is the email address from which the email is sent. You could use a unique email address on each PDU or the same email address across all PDUs.

- Configure the **Port** number. The port number is the communication endpoint on the server. The default is 25. Other common SMTP ports are 587 and 465.
- Set the transmission **Security.**
    - **None –** The connection is insecure.
    - **STARTTLS –** the client uses the STARTTLS command to upgrade a connection to an encrypted one
    - **TLS -** the client will establish a secure connection (also known as SMTPS.)
- 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.
- If the SMTP server requires authentication, enter the **Username** and **Password.** These will be determined by the configuration on the SMTP server.
- Set **Number of retry attempts.** This will be the number of times the PDU will attempt to resend a message if delivery fails. The default setting is 3.
- Set **Time interval between sending retries (in minutes).** This is the time, in minutes, the NMC will wait before retrying to send a failed message. The default setting is 6 minutes.

6. Press **Save** when done.

Next, fill out the **Email Recipients** list.

1. Select the pencil icon to display the **Edit Email Recipient** screen.

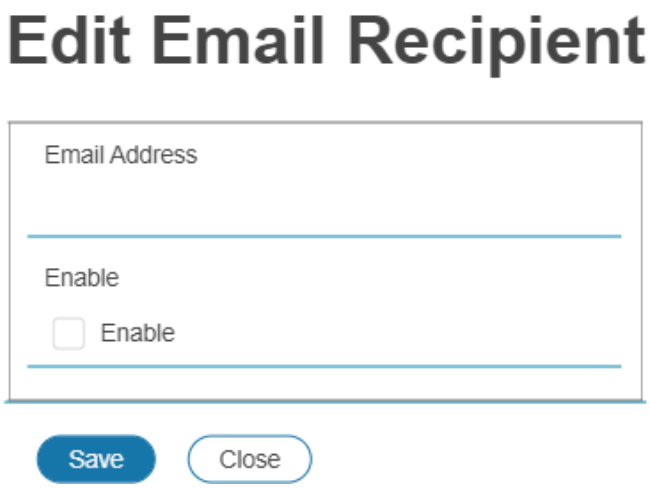


Figure 66: Email Recipient

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

Note: A maximum of 5 users can be registered as email alert recipients.

Event Log

NMC events or alarms are recorded in the event log. Syslog can also be configured to report this to remotely. All critical events are highlighted in red. All warning events are highlighted in yellow.

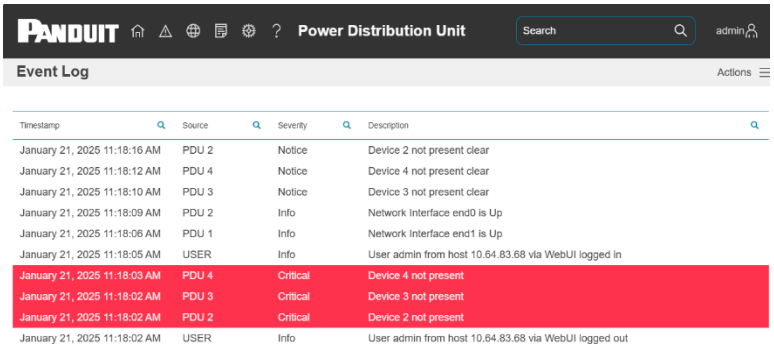


Figure 67: Event log

The event log can be downloaded or cleared from the Actions menu.

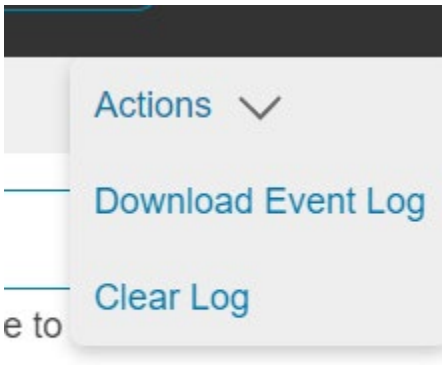


Figure 68: Event log Actions menu

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 60 minutes, the entire data log contains 1000 records with up to 41.67 days of data.) Once the data log reaches the maximum of 1000 records, the oldest entries are overwritten by the newer entries.

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

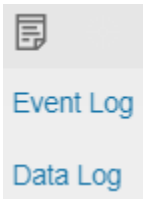


Figure 69: Data Log

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

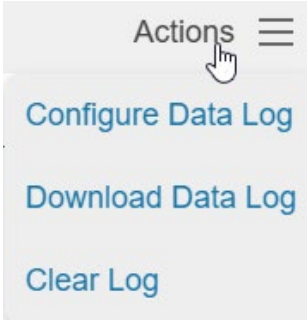


Figure 70: Data Log Configuration

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 60 minutes.)

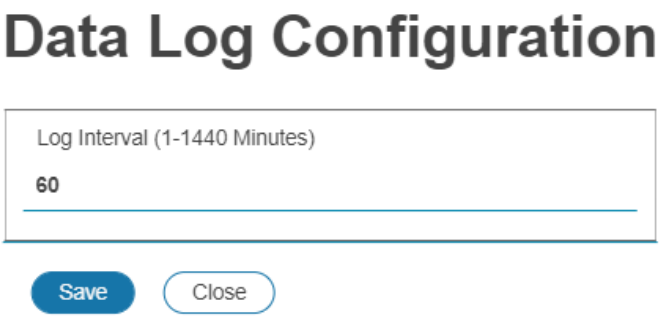


Figure 71: Data Log Configuration Panel

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

The PDU comes with an **Admin, Controller** and **Viewer** profile. The **Admin** role is typically the system administrator and has the Administrator Privileges with full operating permissions. The **Viewer** role is a Read Only profile. All other users must be added by a user with administrator privileges. The **Controller** role can control the PDU functionality, like outlet control, but cannot change the system settings.

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.
controller	Can control the PDU system but cannot change any configuration
viewer	Read-only permissions. Can monitor the system but cannot change any configuration

User Accounts

Add a user with the following steps:

1. Go to **Settings** and select **User Accounts**.
2. Click on the pencil next to empty username field to create a new user profile.
3. Use the Settings tab to enter the following information:
    - Username (required)
    - Role (required)
    - Password (required)
    - Confirm Password (required)
    - Select Enabled to activate user
    - Select Must Change Password at next Log In to force the user to update their password on the next login.

    NOTE: Passwords must be between 8 and 40 characters and follow three of the following four rules:

    a. Contain at least one lowercase character.

b. Contain at least one uppercase character.

c. Contain at least one number.

d. Contain at least one special character.

4. Select **Save** to save the new user profile.

Modify user profile:

1. Go to **Settings** and select **Users**.
2. Click on the pencil next to the user to modify.
3. Select **Edit**. Make changes to the user profile.
4. Select **Save**.

Delete user profile with the following steps:

1. Go to **Settings** and select **Users**.
2. Click on the pencil next to the user to modify.
3. Delete the username.
4. Select **Save.**

Setting Up the System for RADIUS Authentication

1. Go to **User Accounts** in the settings menu.

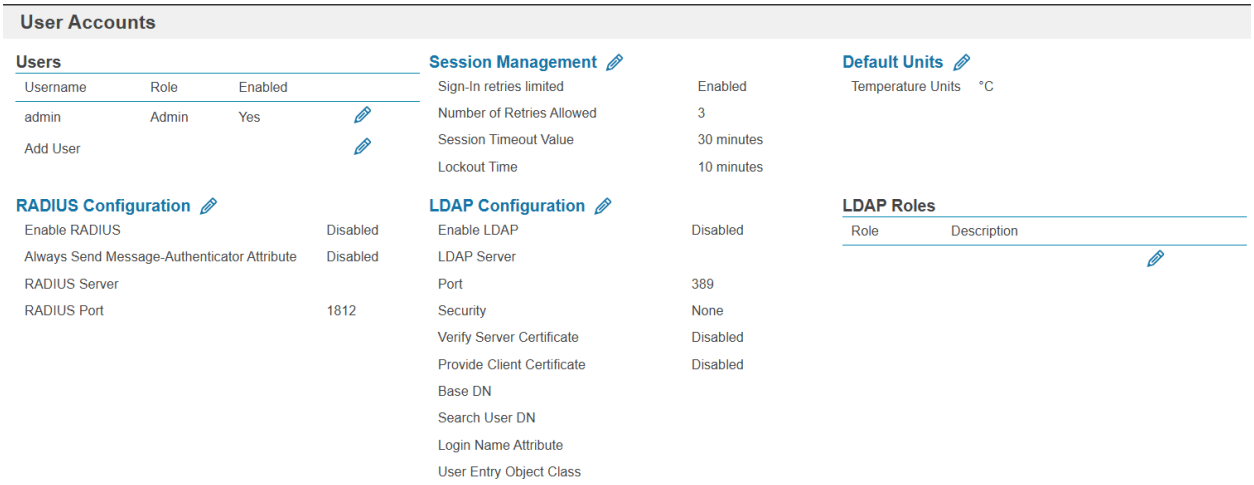


Figure 72: User Accounts

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

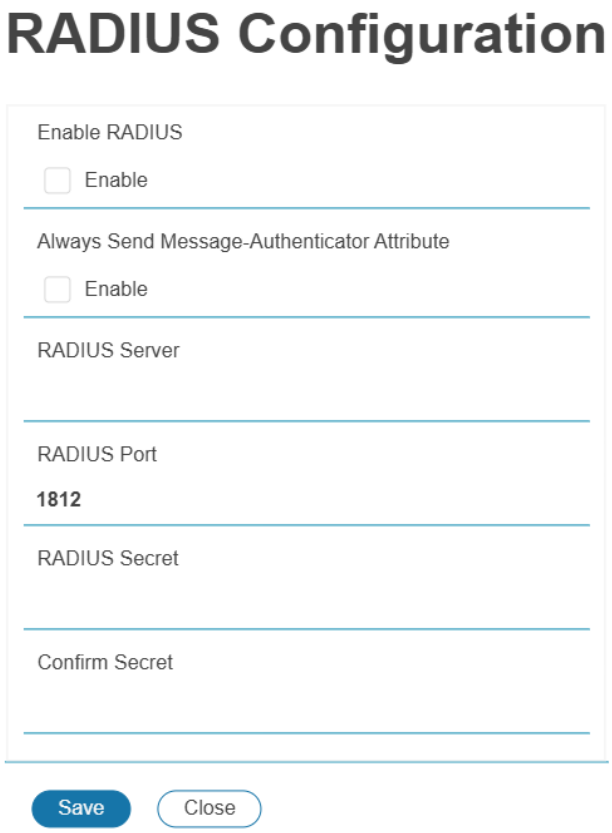


Figure 73: RADIUS Configuration

3. Select the **Enable** button.
4. Enter Server IP address field, Port number field, and Secret field.
5. (Optional) Select Always Send Message-Authentication Attributes to secure Radius messages
6. Click save and your Radius authentication is complete.

Note: By default, a RADIUS user will have the “viewer” 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) or Control(3). For complete details, see Appendix E: 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 NMC via the Web Interface:

1. Go to User Accounts (under the Settings) > 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.
   e.g. *192.168.1.101*
5. Enter a Port.
   Note: For Microsoft, this is typically 389.
6. Enter the Security. None for unencrypted transmission. StartTLS to upgrade the connection after connect to a TLS connection. TLS to start with TLS connection
7. In the Base DN field, enter in the account to be used to access AD.
   e.g. *CN=myuser,CN=Users,DC=EMEA,DC=mydomain,DC=com*
8. Enter the password in the Bind Password and Confirm Password fields.
9. In the Search User DN field:
   e.g. *DC=subdomain,DC=mydomain,DC=com*
10. In the Login Name Attribute field, enter **sAMAccountName** (typically).
11. In the User Entry Object Class field, enter **person**.

With these LDAP settings configured, the Bind is complete.

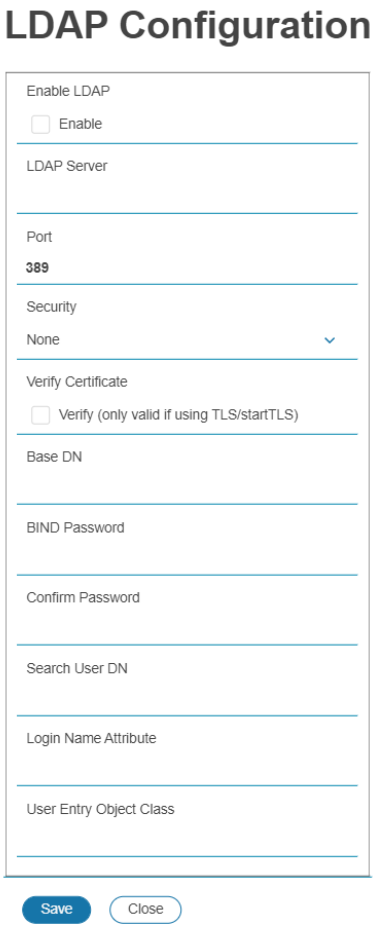


Figure 74: LDAP Configuration

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 NMC administrators. *i.e. admins*

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

2. Within the PDU Web GUI, go to **User Accounts** (under Setting) > **LDAP Roles**. Enter the **Role Name** that was created in AD. e.g. *admins*
3. Enable role privileges as needed (pictured below).

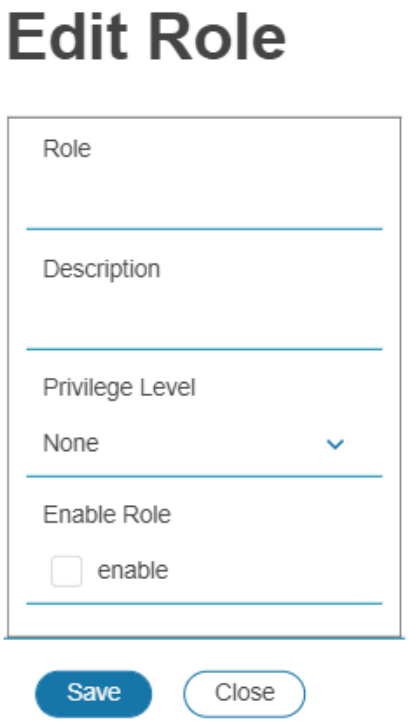


Figure 75: Enable Role Privileges

4. LDAP authentication is ready to use.

Wi-Fi Settings (PN: CNT06 Required)

The Wi-Fi feature is only available by swapping the standard NMC with replacement part number CNT06.

The CNT06 NMC can connect wirelessly to a Wi-Fi Network (using “Wi-Fi Network” mode). It can also act as a Wi-Fi access point (using “Direct Connect” mode) so that the user can connect a computer, mobile phone, or tablet directly to the NMC to monitor or configure it. Wi-Fi Settings can be accessed from the gear icon menu.

Note: Connecting both Wi-Fi network and Ethernet network simultaneously can result in unexpected network behavior. It is recommended to connect only one network.

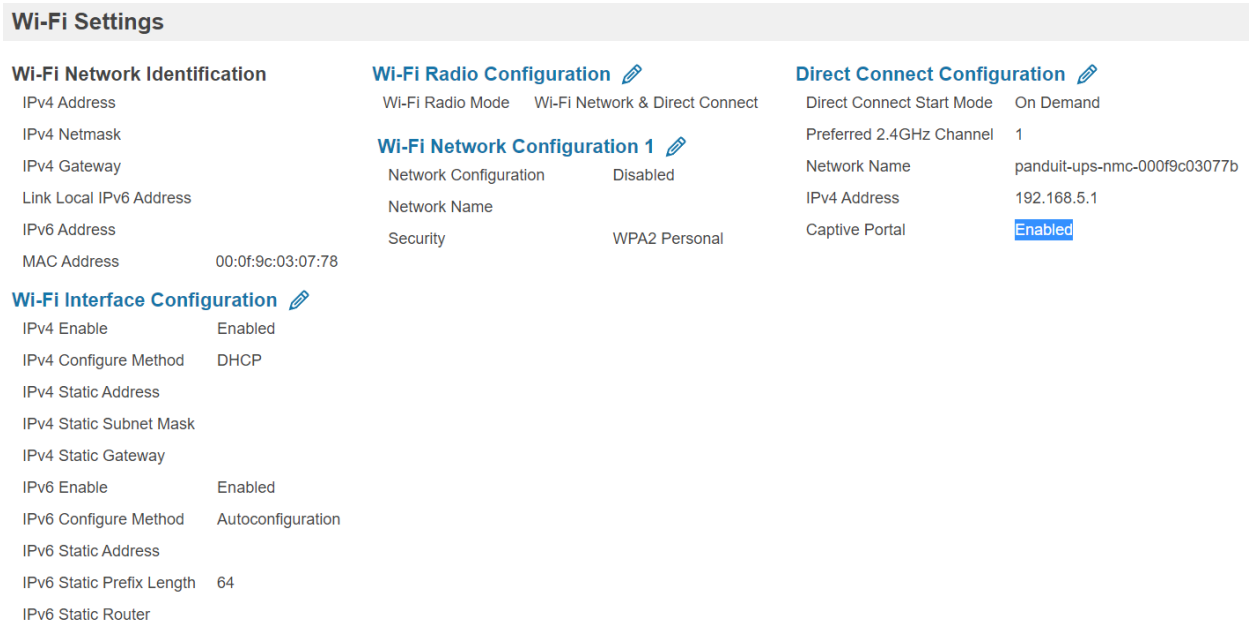


Figure 76: Wi-Fi Settings screen

Configuring Wi-Fi Radio mode

Click on the pencil icon next to the Wi-Fi Radio Configuration to change Wi-Fi radio mode.

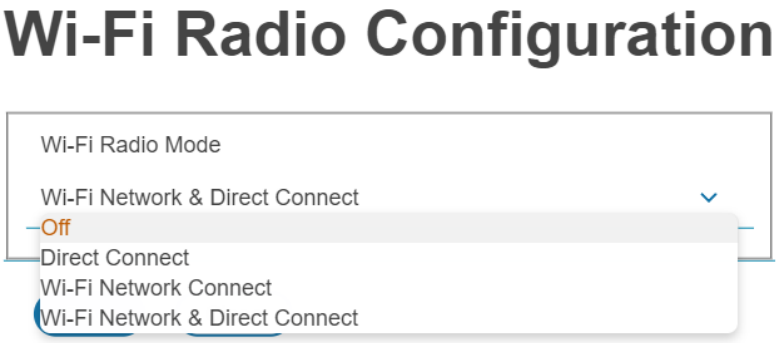


Figure 77: Wi-Fi Radio Configuration

1. Click on the drop-down menu from the mode option.
2. Select a desired mode.
    - Off: Turn Wi-Fi radio Off.
    - Direct Connect: Use only Direct Connect mode.
    - Wi-Fi Network Connect: Use only Wi-Fi Network connect mode.
    - Wi-Fi Network & Direct Connect: Use both Direct Connect and Wi-Fi Network Connect mode.

3. Click Save button

Configuring Direct Connect

Click on the pencil icon next to the Direct Connect Configuration to change Direct Connect settings. When the direct connect start mode is set to ‘On Demand’, push the reset button briefly to start the Wi-Fi direct connect.

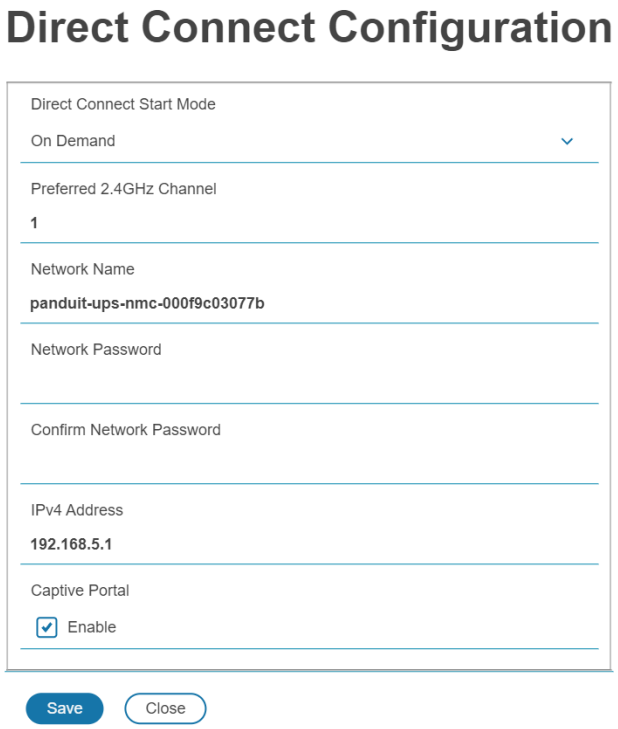


Figure 78: Wi-Fi Direct Connect Configuration

1. Select Start mode option
   - On Demand: Push the reset button to start the Direct Connect mode. It will be available for the following 10 minutes.
   - Always On: Direct Connect is always active.
2. Fill in desirable Direct Connect network settings that mobile devices will use.
3. Click Save button.

Configuring Wi-Fi Network

Click on the pencil icon next to the Wi-Fi Network Configuration to change the Wi-Fi network settings. The NMC provides four different security modes: WPA2 Personal, WPA3 Personal, WPA2 Enterprise, and WPA3 Enterprise. To connect to a Wi-Fi network, the Wi-Fi Network Configuration must match the configuration of the desired

Wi-Fi network.

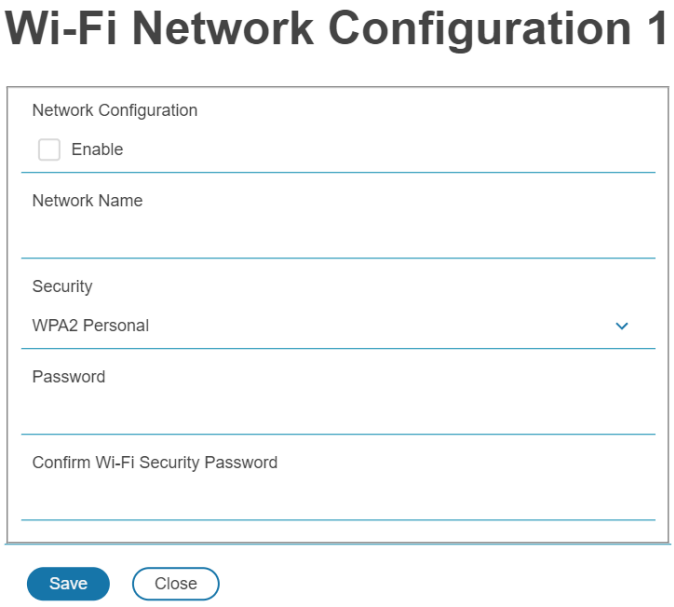


Figure 79: Wi-Fi Personal security Network configuration

1. Tick checkbox on **Enable.**
2. Fill in the Wi-Fi network configuration.
3. When Enterprise security is chosen, more configuration options will be required.
4. Click Save.

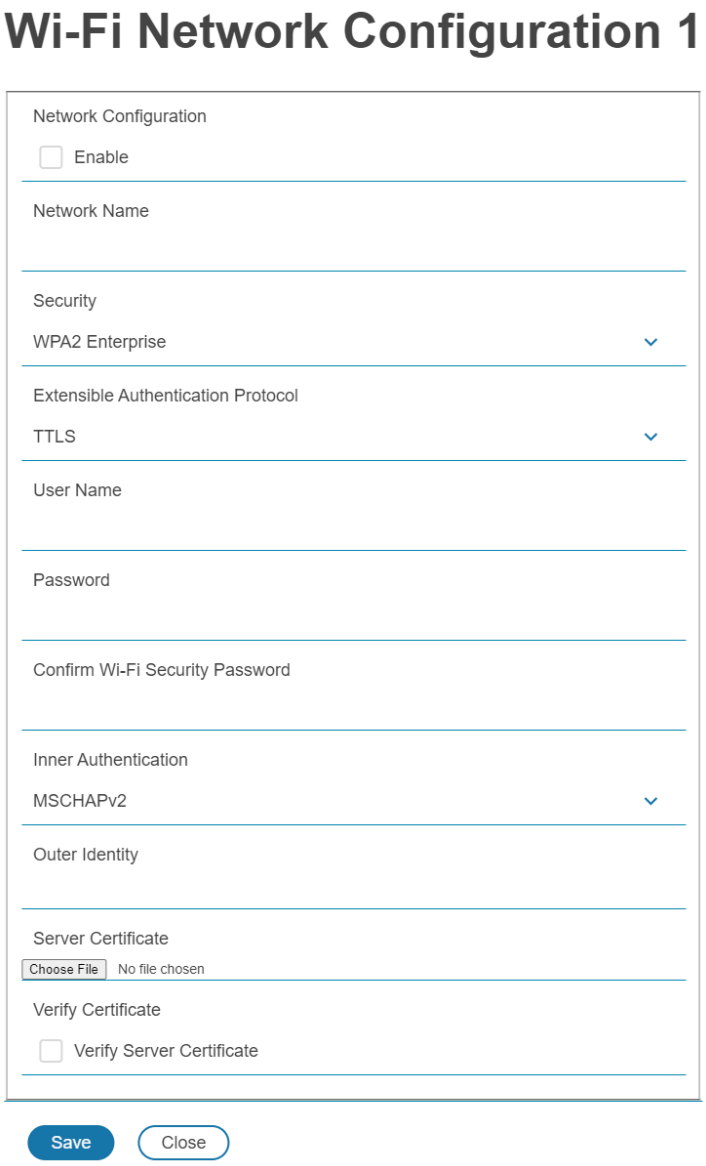


Figure 80: Wi-Fi Enterprise security Network configuration

Wi-Fi Enterprise security supports the PEAP, TLS, and TTLS protocols. The MSCHAPv2, MSCHAP, PAP, and CHAP inner authentication protocols are available with the TTLS protocol. Outer Identity must be filled. The server certificate validation is optional for WPA2 Enterprise.

Configuring Wi-Fi Interface

Click on the pencil icon next to the Wi-Fi Interface Configuration to change the Wi-Fi interface settings.

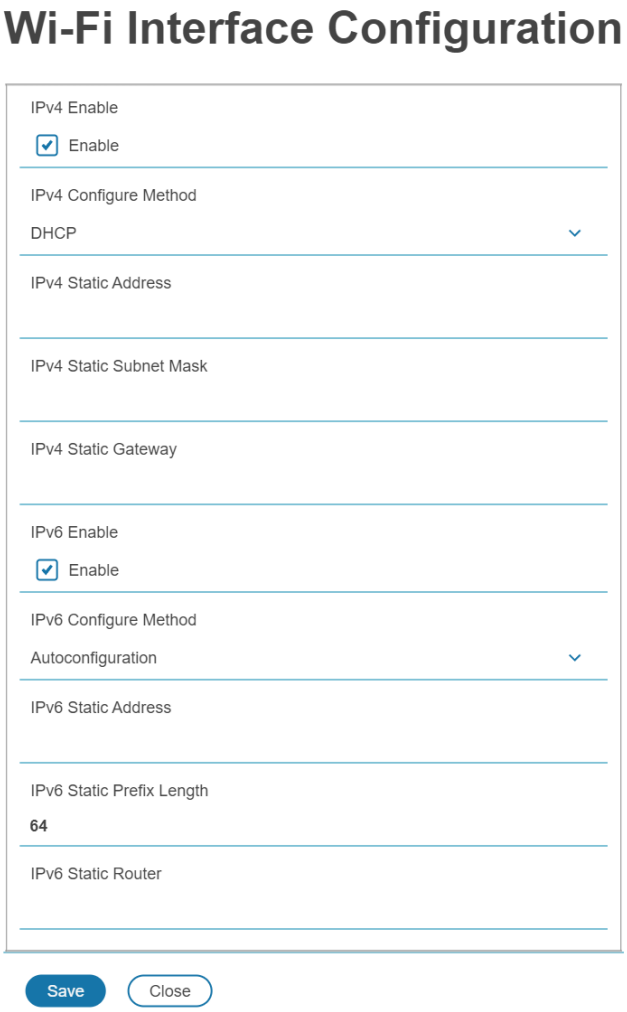


Figure 81: Wi-Fi Interface Configuration

Section 3 – Simple Network Management Protocol (SNMP)

SNMP Management Configuration

Setup SNMP

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

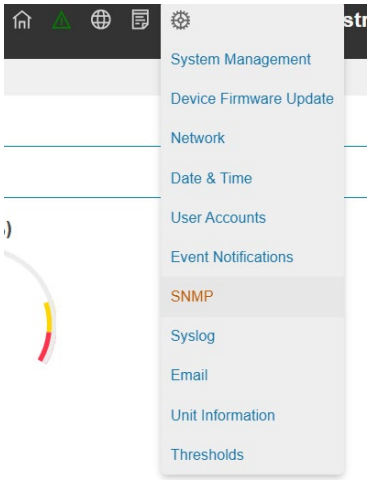


Figure 82: SNMP Configuration

3. The SNMP General includes SNMP Access and Version.

Figure 83: SNMP General

Setup SNMP Port

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

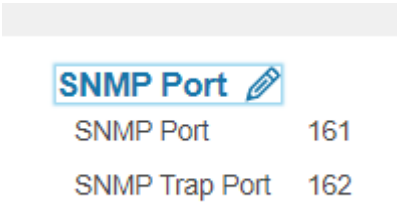


Figure 84: SNMP Port

3. Set up SNMP Port and SNMP Trap Port.

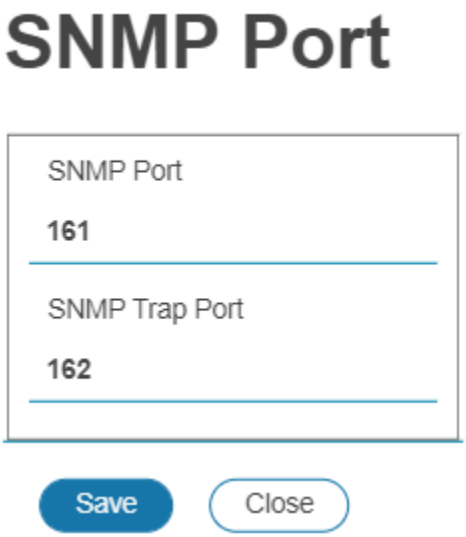


Figure 85: Setup SNMP Port and Trap Port

Configuring SNMP User

Configuring an SNMP user will allow a user to have access to the system over SNMP. To set up an SNMP USER, follow the following procedure:

Configuring Users for SNMP V1/V2c

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

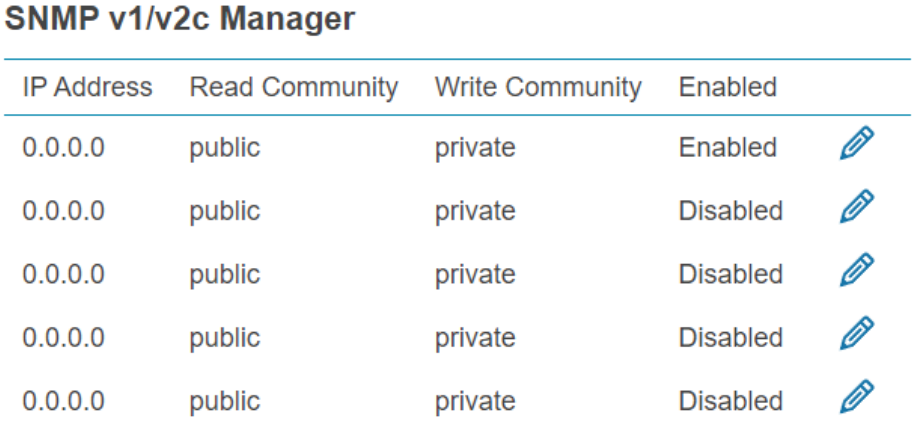


Figure 86: Define SNMP V1/V2c User

4. The **Edit** panel pop up displays.

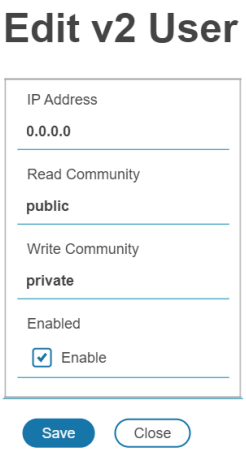


Figure 87: Edit V1/2c Manager

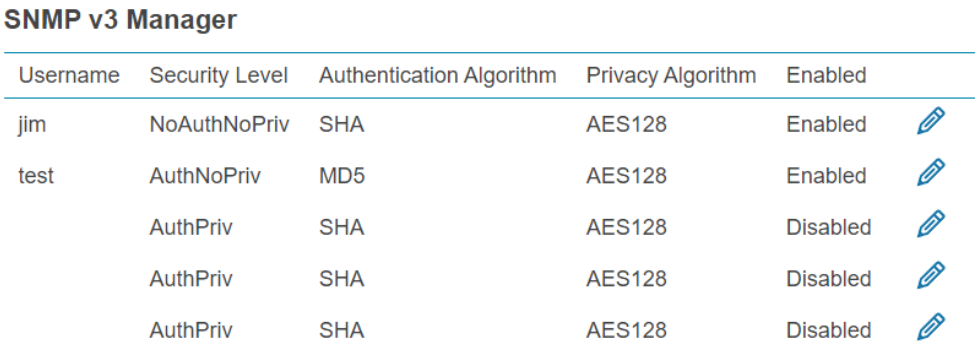
5. Set the following options:
   - IP Address: the IP address of the host for this SNMP V1/V2 manager. Only requests from this address will be acted upon.

     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 Settings, select **SNMP**.

3. In the **SNMP v3 Manager** panel, select the SNMP v3 manager to configure. Select the **pencil** icon in the last column.



SNMP v3 Manager

Username	Security Level	Authentication Algorithm	Privacy Algorithm	Enabled	
jim	NoAuthNoPriv	SHA	AES128	Enabled	
test	AuthNoPriv	MD5	AES128	Enabled	
	AuthPriv	SHA	AES128	Disabled	
	AuthPriv	SHA	AES128	Disabled	
	AuthPriv	SHA	AES128	Disabled	

Figure 88: SNMP v3 Manager

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

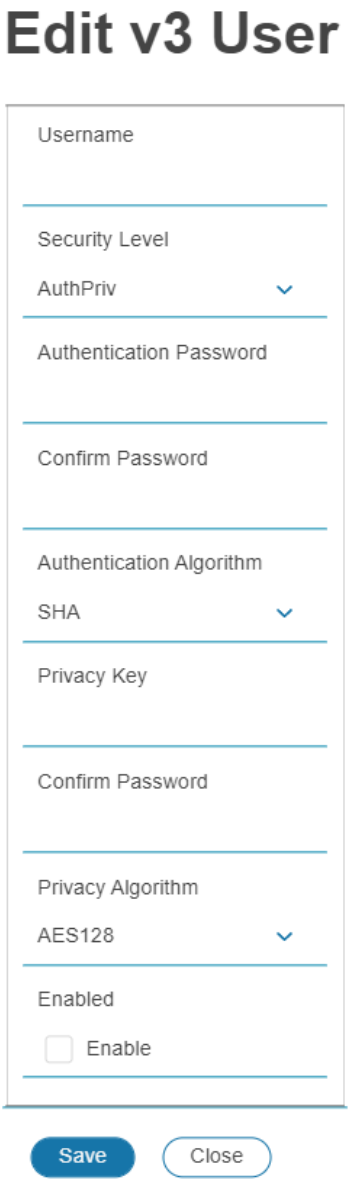


Figure 89: SNMP V3 Edit

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 **Authentication Password** to be used for authentication. Repeat the authentication password below it in **Confirm Password**.
8. Select the desired authentication algorithm.
   - MD5
   - SHA
9. Enter a new unique Privacy Key to be used with the privacy algorithm. Repeat the privacy key below it in **Confirm Password**.
10. Select the desired privacy algorithm.
    - AES-128
11. Click **Enable** and **Save**.

Configuring SNMP Traps

The NMC 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 NMC to send SNMP traps, follow the following procedure:

Configuring SNMP v1 Trap Settings

1. Go to Settings > SNMP
2. Click the pencil next to SNMPV2c Trap Receiver you want to update.

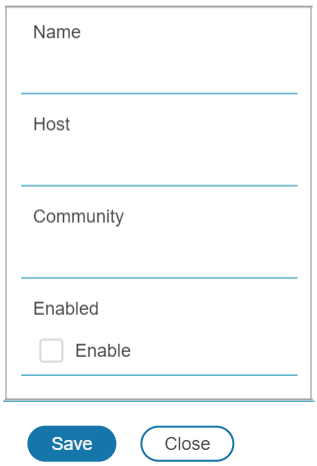


Figure 90: SNMPv2c Trap Receiver Configuration Information

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 Settings > SNMP
2. Click the pencil next to SNMPV3 Trap Server you want to update.

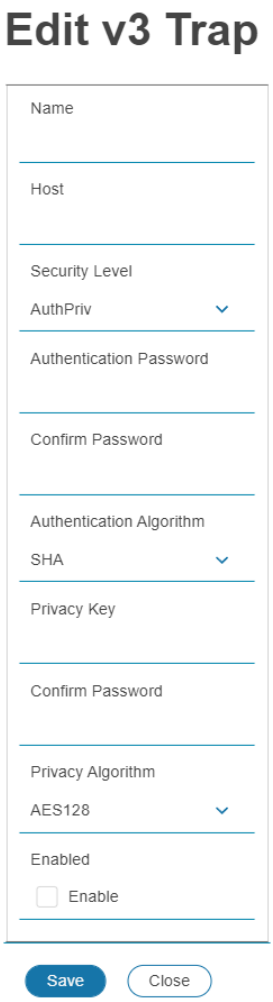


Figure 91: SNMPv3 Trap Server configuration Information.

3. Enter the **Name** and **Host** 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 **Authentication Password** from the SNMP Server to be used for authentication. Repeat the authentication password below it in **Confirm Password**.
6. Select the desired authentication algorithm.
    - MD5
    - SHA
7. Enter the **Privacy Key** from the SNMP Server for privacy algorithm. Repeat the privacy key below it in **Confirm Password**.
8. Select the desired privacy algorithm.
    - AES-128
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 touchscreen, graphical Network Controller panel.

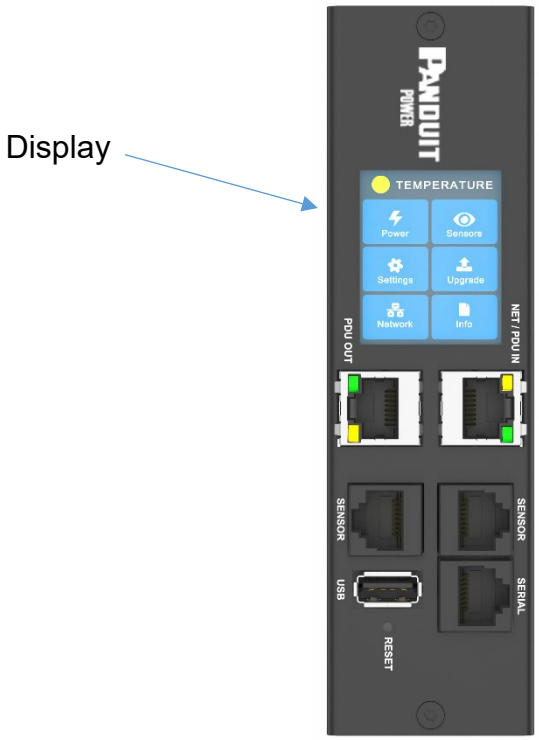


Figure 92: Network Controller

The Network Controller Display has three modes:

1. **Menu mode** (Network Controller Display main menu): When the PDU is powered up or when the screen is touched while in Standby Mode or Power Save mode.
2. **Standby mode**: This happens when a PDU is idle (no touch inputs) 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, touch the screen display.

Network Controller Menu Structure

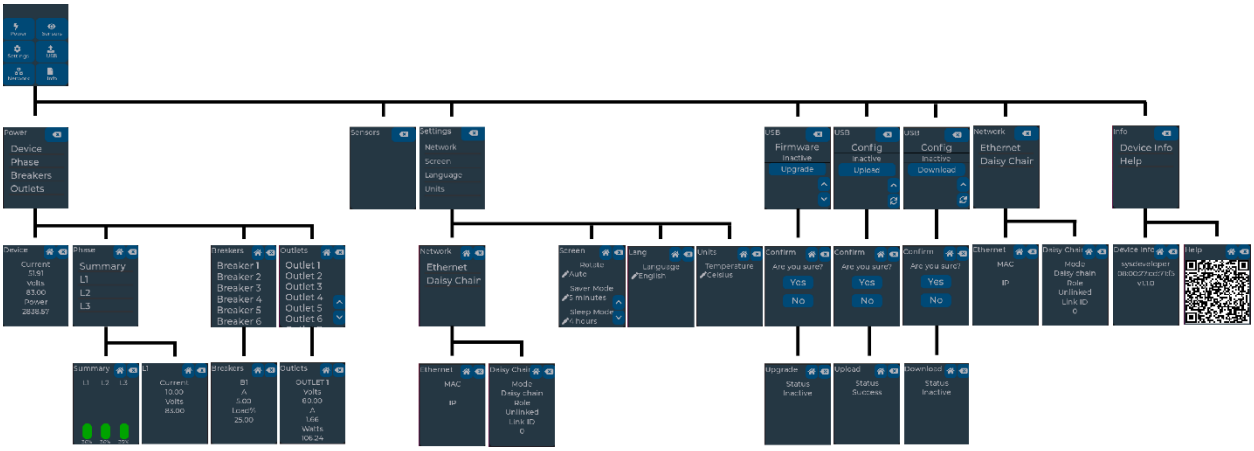


Figure 93: Network Controller Menu Structure

Main Menu Selections

The PDU menu selection hierarchy consists of Power, Sensors, Settings, USB, Network, and Info.

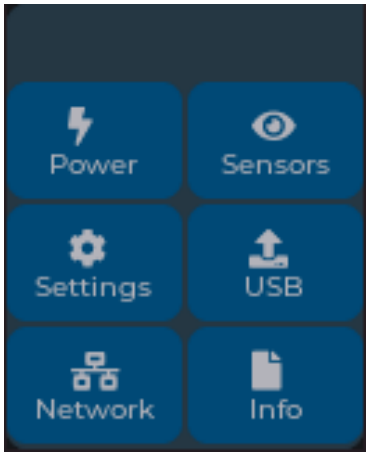


Figure 94: Main Menu Selections

Alarms Menu

The Alarms menu displays active alarms for the PDU. On the Main Menu, touch the alarm header to display the Alarm Screen. When you finish your review, press **Back** to return to the Main menu.

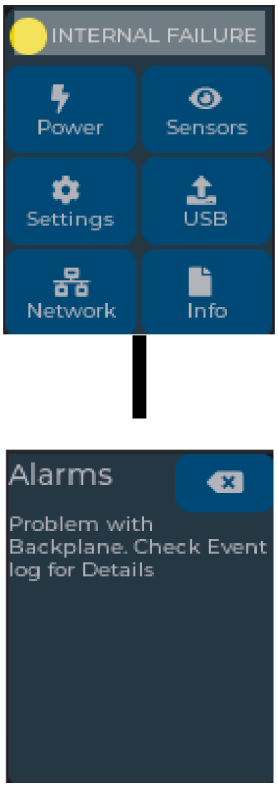


Figure 95: Alarms Menu

Power Menu

The Power menu manages Device, Phase, Breaker and Outlet. On the Main Menu, touch a menu option to display the submenu options. Press **Back** to return to the previous menu. Press **Home** to return to the Main menu.

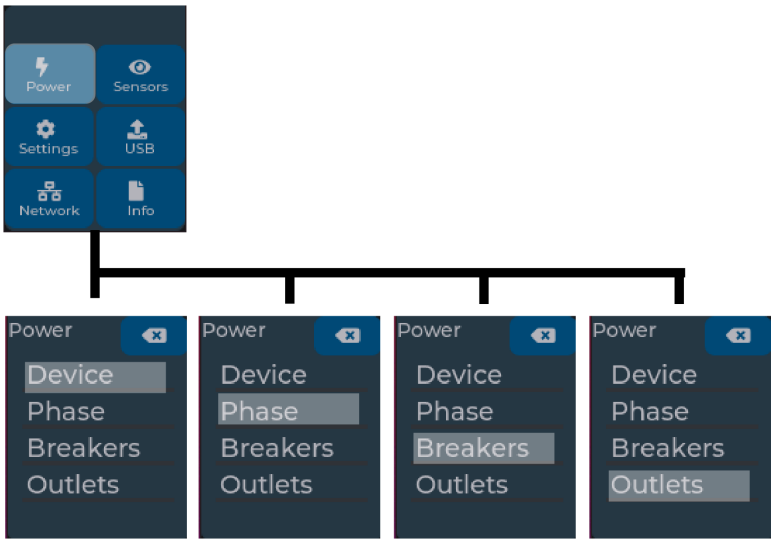


Figure 96: Power Menu

Device Submenu

The Device submenu is to display current, voltage and power. On the Power menu, touch Device to display the power values for the entire PDU. Press **Back** to return to the previous menu.

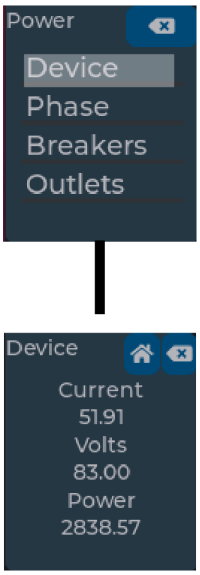


Figure 97: Device Submenu

Phase Submenu

The Phase submenu is to display the status of the phases On the Power menu, touch Phase to display the screens to set the values for the submenu. After you select the phase, touch the desired phase to display the values for that phase on the screen. Press **Back** to return to the previous menu.

Figure 98: Phase Submenu

Breaker Submenu

The Breaker submenu is to display power values for the breakers. On the Power Menu, touch Breakers to display a list of breakers. To display a breaker, touch the desired Breaker # to display values of a Breaker. Press **Back** to return to the previous menu.

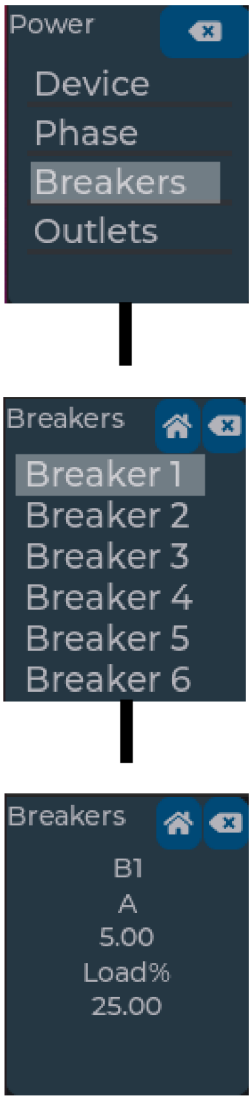


Figure 99: Breaker Submenu

Outlet Submenu

The Outlet submenu is to display voltage, current and power from outlet number 1 to number n. On the Power menu, touch Outlet. Touch the desired Outlet # to display values for an Outlet. Press **Back** to return to the previous menu.

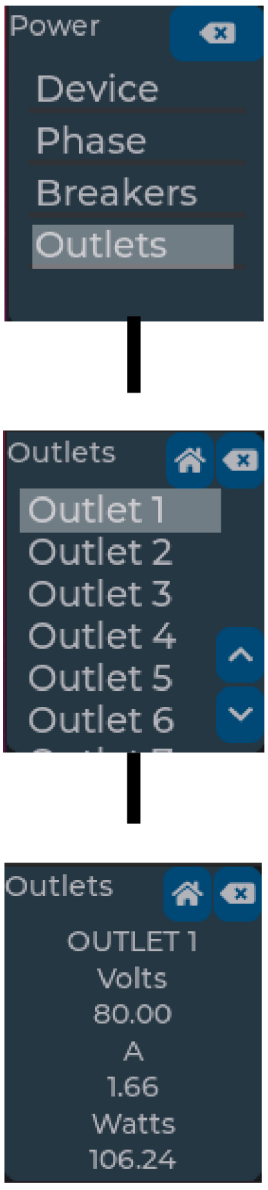


Figure 100: Outlet Submenu

Sensors Menu

The Sensor menu is to display temperature, humidity, door switch, fluid leak etc. On the Main Menu, touch Sensor to display a list of Sensors. Touch the desired Sensor # to display values for a Sensor. Press **Back** to return to the previous menu.

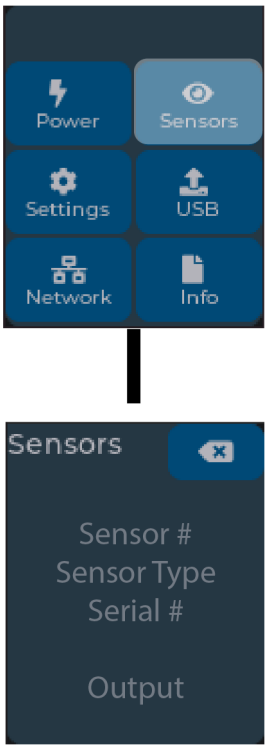


Figure 101: Sensors

Settings Menu

The Settings menu provides user configuration options including Network, Screen, Language, and Units. Press **Back** to return to the previous menu. Press **Home** to return to the Main menu.

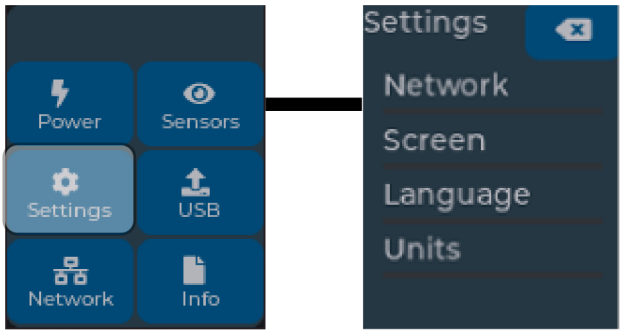


Figure 102: Setup Menu

Network Submenu

The Network submenu allows you to view device addresses and Daisy Chain configuration. On the Settings menu, touch Network to enter the Network Submenu. Touch Ethernet to display the screens that display the IP and MAC addresses. Touch Daisy Chain to display configuration options. Press **Back** to return to the previous menu.

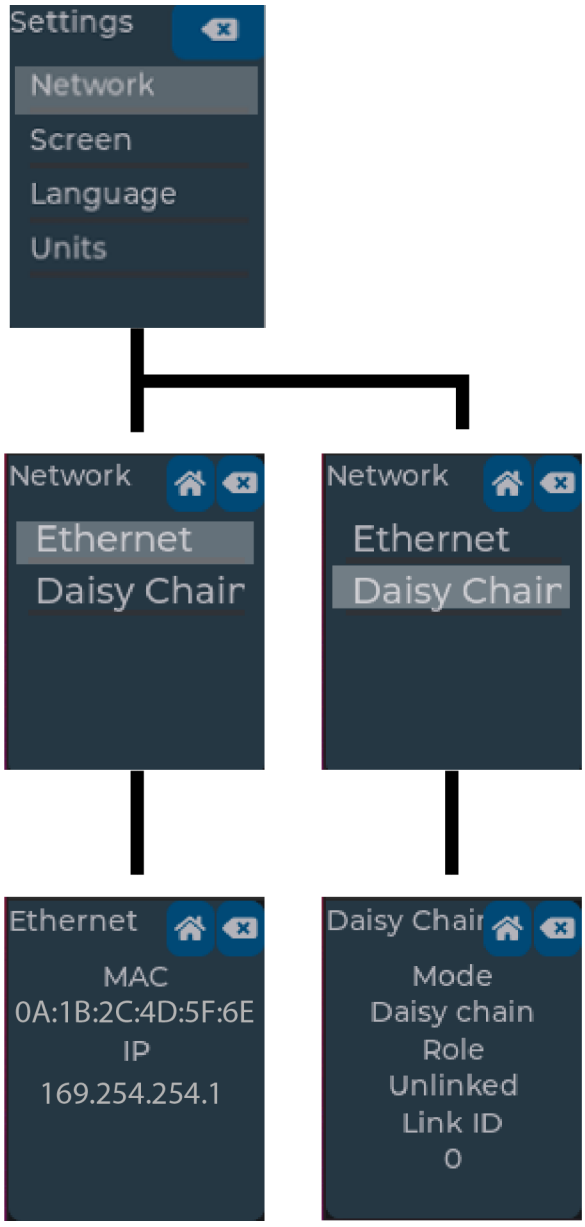


Figure 103: Network Submenu

Screen Submenu

The Screen submenu allows you to customize settings for Rotate, Saver Mode, and Sleep Mode. In the Settings menu, touch to select the submenu. After you select a option, touch the desired value on the screen to set. Press **Back** to return to the previous menu.

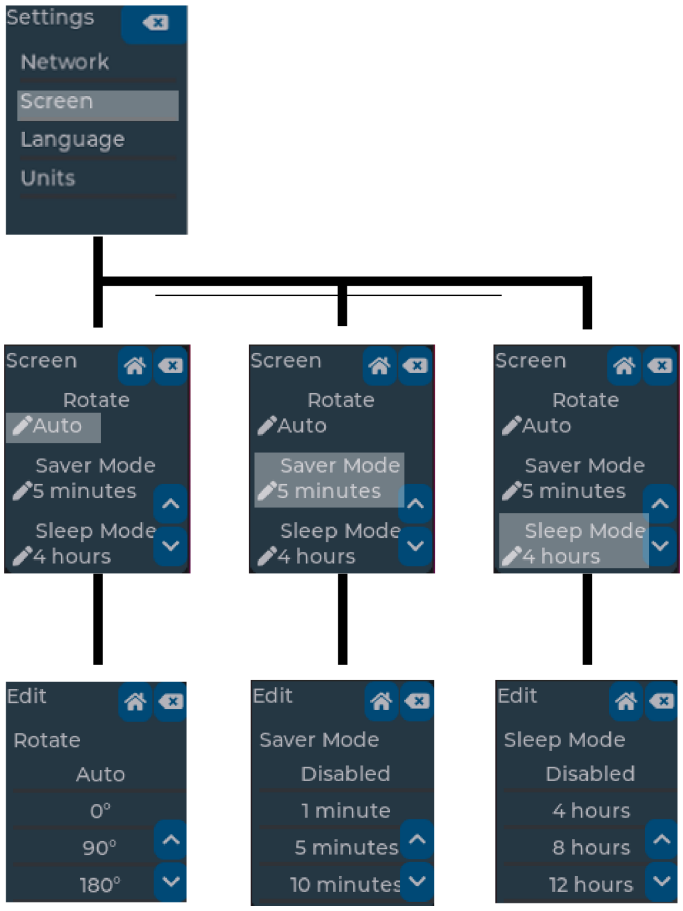


Figure 104: Screen Submenu

Language Submenu

The Language submenu allows you to select the language you need to use. In the Settings menu, touch Lang to display the screens to select the submenu. After you select Lang, touch the desired value on the screen to set. Press **Back** to return to the

previous menu.

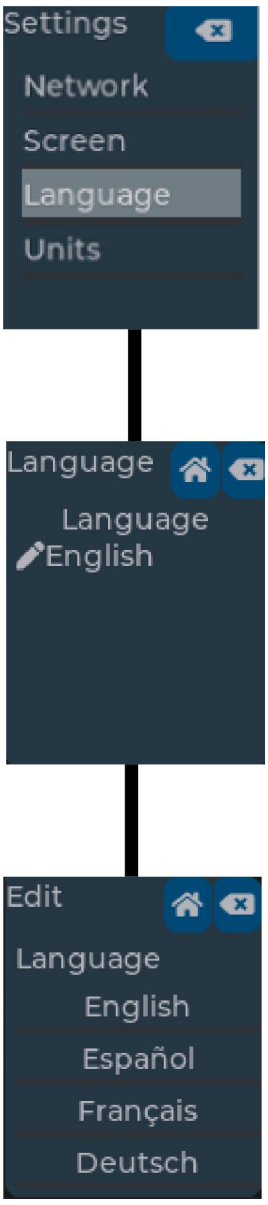


Figure 105: Language Submenu

Units Submenu

The Units submenu displays the temperature units. On the Settings menu touch the Units Submenu. In the Units Submenu touch the desired value to set. Press **Back** to return to the previous menu. Press **Home** to return to the Main Menu.

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

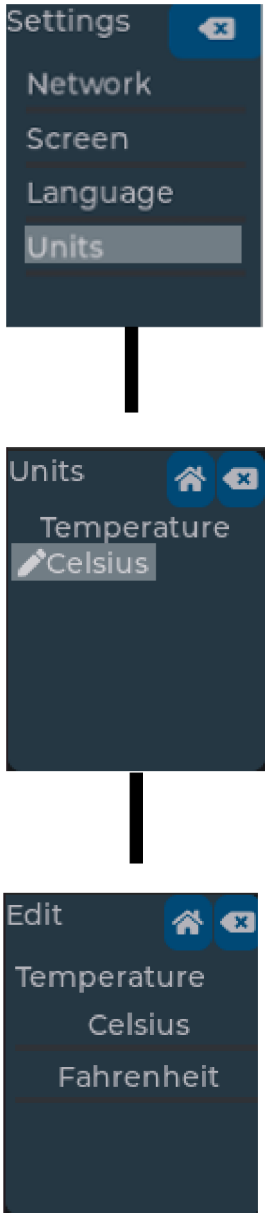


Figure 106: Units Submenu

USB Menu

The USB menu is used once an external USB drive is attached to the USB port. From this menu, users can upload firmware files. Only signed official firmware files are accepted by the device. The USB port can also be used to either upload a new configuration or download the current configuration to the attached external USB drive.

The USB port can be enabled or disabled from the Web UI (Settings → System Management).

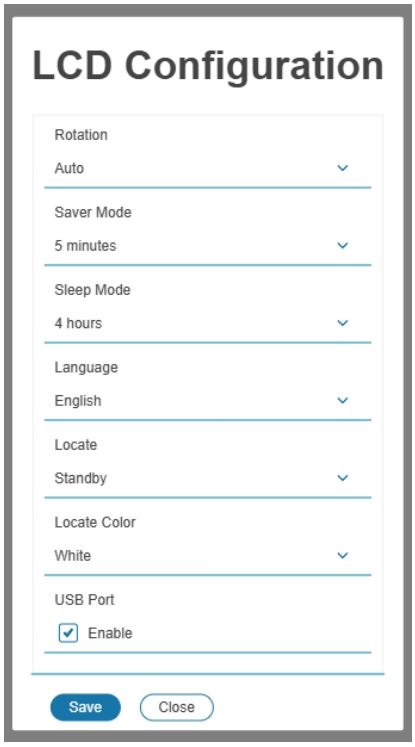


Figure 107: USB Enable

Firmware

To upgrade or downgrade firmware, insert a USB storage device containing a firmware file. Once inserted, the PDU will automatically detect and copy the firmware file. The status will update to "Copying" and then to "Available." When the status is "Available," the PDU is ready to load the new firmware file, and the USB device can be removed

from the PDU.

To start the firmware upgrade, touch "Upgrade" and then touch "Yes" to confirm. The firmware status page will appear, and the status will update from "Available" to "Uploading." Once finished uploading, the status will update from "Uploading" to "Activating." During the "Activating" phase, the PDU installs the firmware and performs any necessary cleanup.

Once "Activating" is completed, the device will reboot automatically (unless an identical version is already installed). Outlet states are not affected during the firmware upgrade or downgrade process.

Configuration

Upload: To upload a new configuration, insert a USB storage device containing a config*.json file. Once inserted, the PDU will automatically detect and copy the config file. The status will update from "Inactive" to "Copying" and then to "Available." When the status is "Available," the PDU is ready to load the new configuration, and the USB device can be removed from the PDU.

To start the config upload, touch "Upload" and then touch "Yes" to confirm. The Config Upload status page will appear, and the status will update from "Available" to "Uploading." During the "Uploading" phase, the PDU reads the configuration file and sets the appropriate values on the device. When uploading is complete, the status will indicate "Success" or "Fail." If any action fails, the status will revert to "Inactive," and the process can be tried again.

Download: To download the existing configuration, insert a USB storage device. To start the config download, touch "Download" and then touch "Yes" to confirm. The Config Download status page will appear, and the status will update from "Inactive" to "Downloading." During the "Downloading" phase, the PDU gathers all configuration data and creates a configuration file on the USB device. When downloading is complete, the status will indicate "Success" or "Fail." If any action fails, the status will revert to "Inactive," and the process can be tried again.

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

NOTE: If both a firmware and configuration file are on the USB device the PDU will prioritize copying the firmware first.

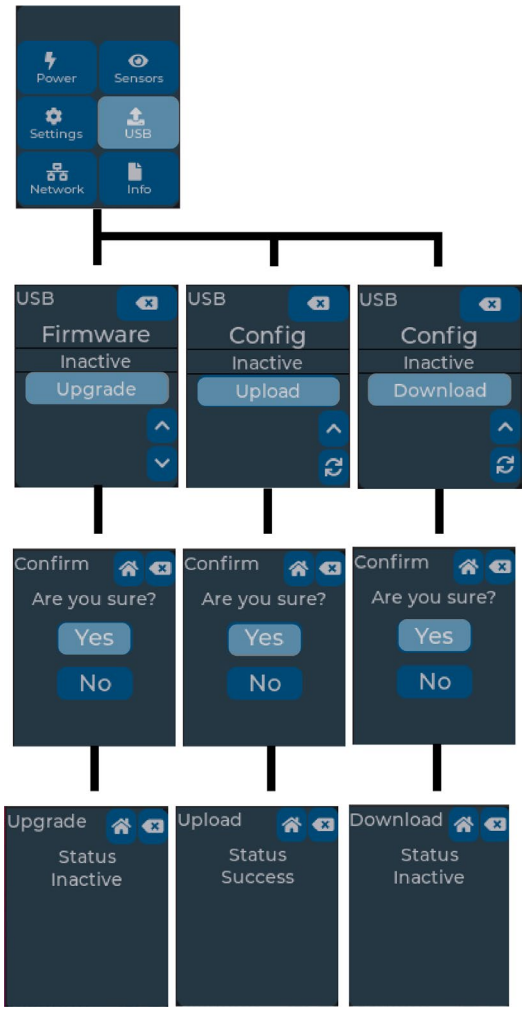


Figure 108: USB Submenu

Network Menu

The Network menu displays the temperature units. On the Settings 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 **Back** to return to the previous menu. Press **Home** to return to the Main menu.

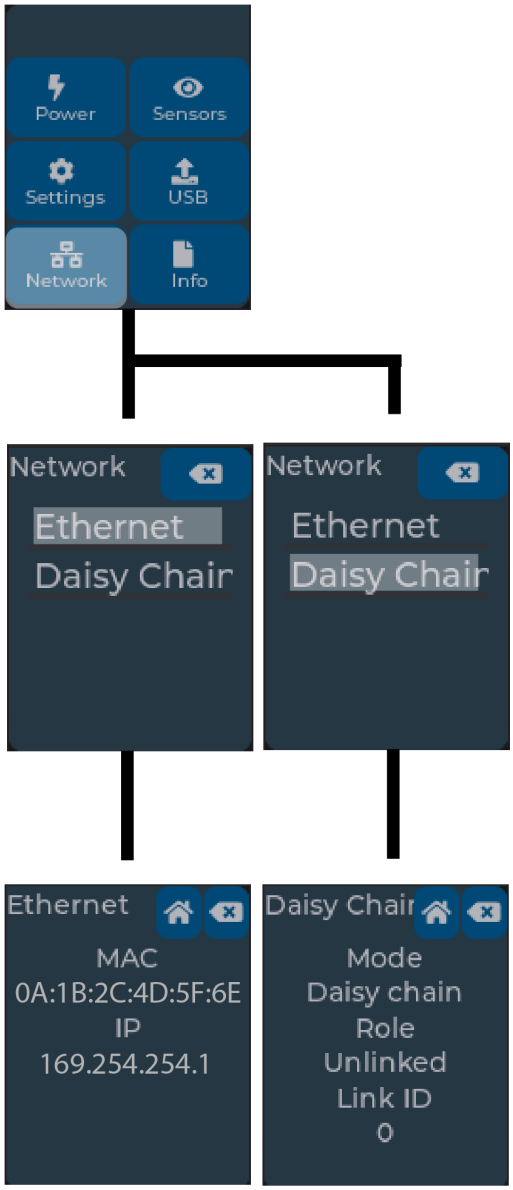


Figure 109: Network Menu

Info Menu

The Info menu displays the device information and a QR code that links to the product support page. In the Info menu, touch Device Info to display all relevant device information. Touch help to display a QR code which will redirect to the public product page. Press **Back** to return to the previous menu. Press **Home** to return to the Main menu.

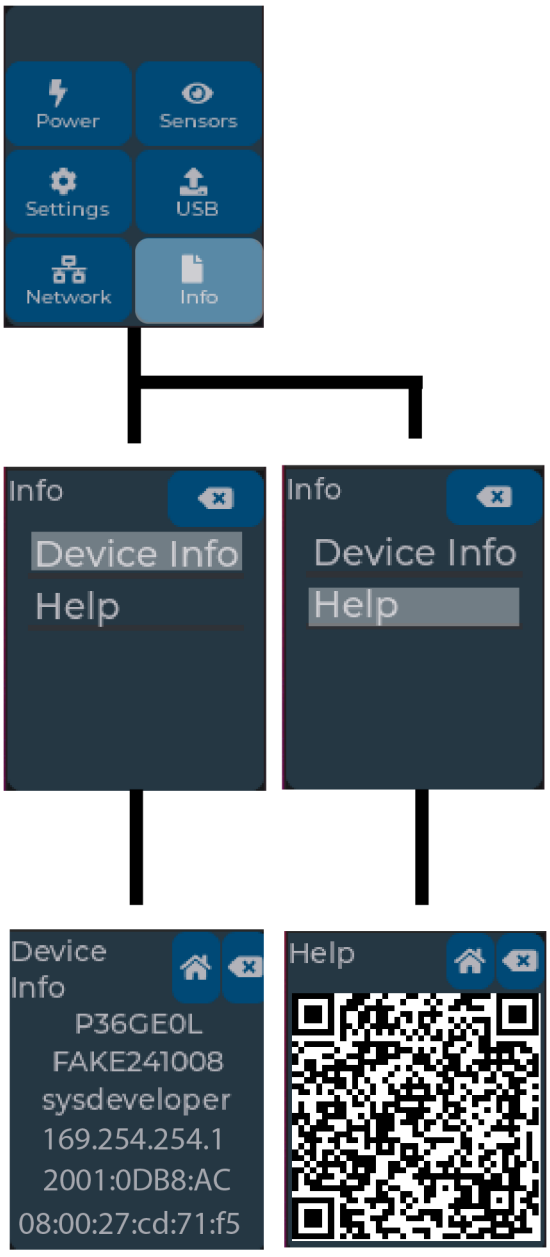


Figure 110: Info Menu

Help Menu

The help menu provides convenient access to user guide, device licenses as well as the SNMP MIB.

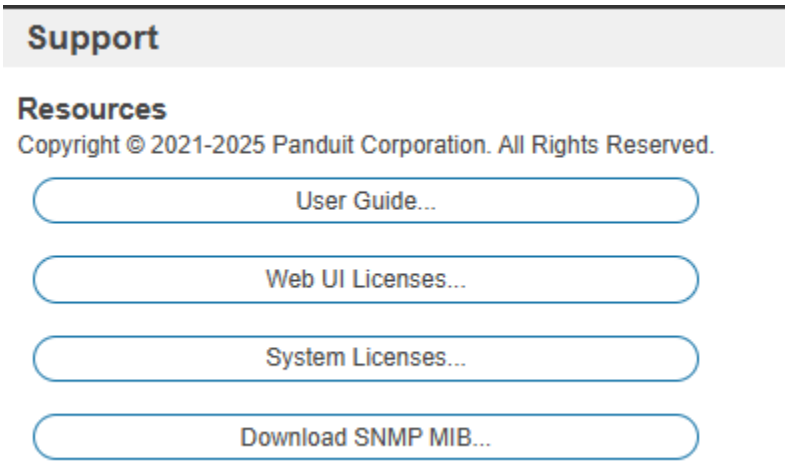


Figure 111: Help & Support

Search Box

The search box returns a list of keywords as they are typed in. This is a convenient option to quickly reach areas of the PDU. Once the desired area is displayed the user must mouse click over the topic to go directly to those respective pages.

Currently all headers are built in as keywords. Below are the keywords the search will react to:

0: "Home / Dashboard"

1: "Home / Identification"

2: "Home / Control & Manage"

3: "Alarms / Active Alarms"

4: "Languages / English"

5: "Languages / Français"

6: "Languages / Deutsch"

7: "Languages / Español"

8: "Logs / Event Log"

9: "Logs / Data Log"

10: "Settings / Network Settings"

11: "Settings / System Management"

12: "Settings / Unit Information"

13: "Settings / Device Firmware Update"

14: "Settings / Event Notifications"

15: "Settings / SNMP Manager"

16: "Settings / Email Setup"

17: "Settings / Trap Receiver"

18: "Settings / User Accounts"

19: "Settings / Thresholds"

20: "Settings / Wi-Fi Settings"

21: "Settings / Rack Access Control"

22: "Settings / Link Configuration"

23: "Help / Support"

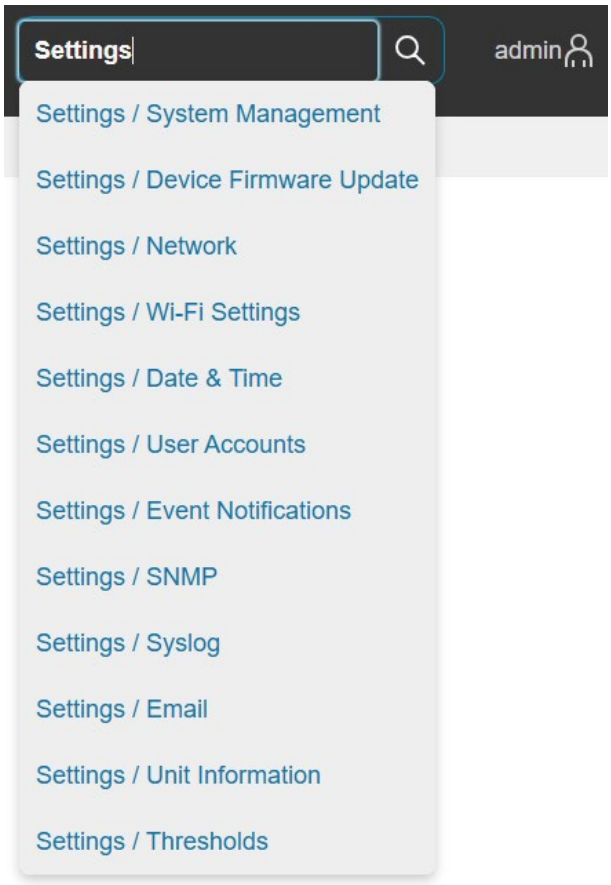


Figure 112: Example Search Box

Section 5 – Daisy Chain Configuration

The daisy chain PDU feature is disabled from the factory and must be enabled through the Web GUI under Settings → System Management.

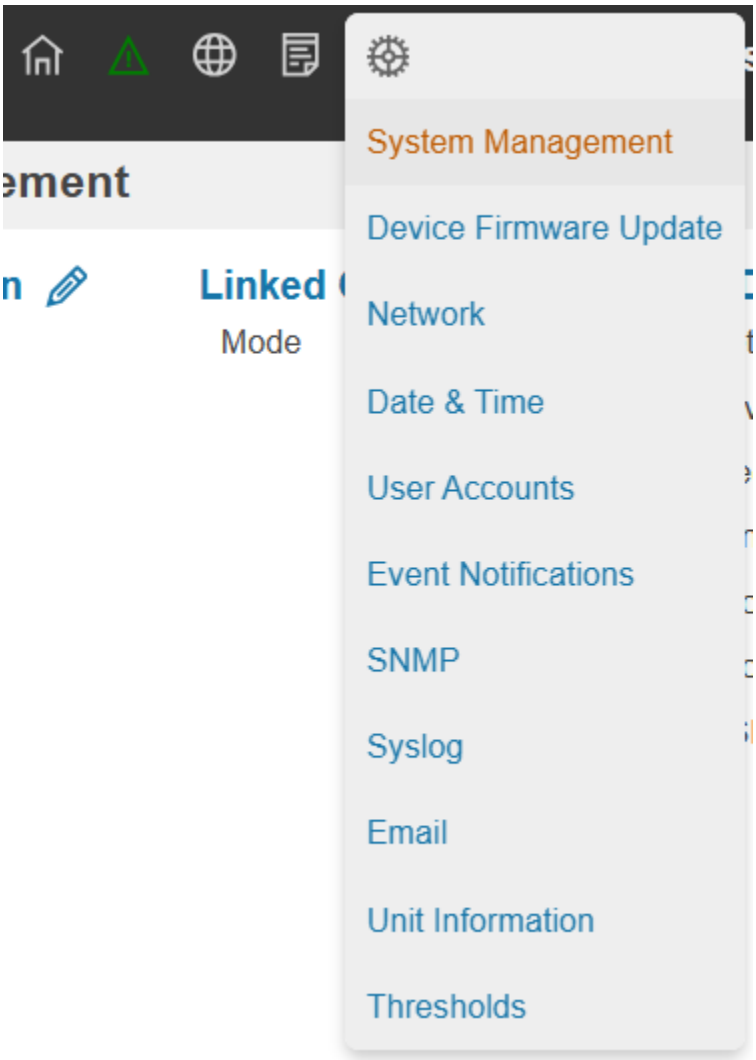


Figure 113: System Management

In **Link Configuration** user must select the '**Mode**' and the '**Role**' of the PDU.

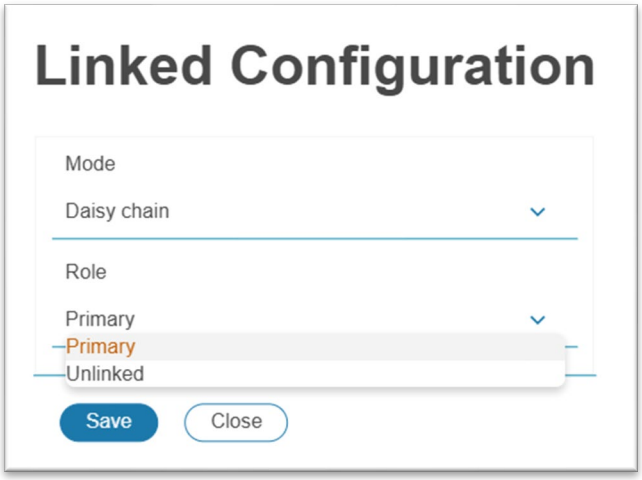


Figure 114: Linked Configuration

Daisy-Chain Overview

In daisy chain mode, up to (64) EL2P PDUs can be connected via one IP address. This allows users to gather information/data from, and to configure, all the daisy-chained PDUs from the main PDU. Daisy chain functionality reduces network cost for PDUs.

Daisy-Chain Setup

After the initial PDU is configured (Primary), 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.

Repeat connecting PDUs from the **PDU Out** port to the **Ethernet/PDU In** port.

Go to the Web interface (or management software) to manage and control the PDUs in the daisy chain.

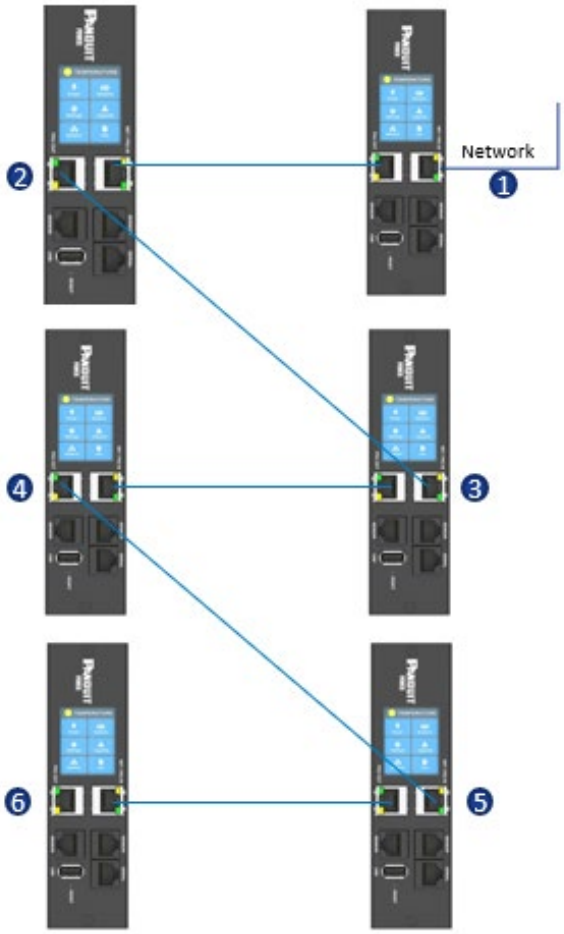


Figure 115: Connection Diagram 6 PDU Daisy Chain

Power Share

Power Share is designed to allow for continual sensor monitoring and electronic rack access if (1) of the (2) power feeds experiences an interruption. Due to limited available power from the Panduit iPDU Controller, power share was designed and tested under the following conditions:

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

ACF06L Panduit Security Handle, EHH01L (T+D), EHC01L (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 PDU controller has a maximum output power capacity of 600mA @ 5V = 3 watts;

600mA @ 12V = 7.2 watts. Based on this, DO NOT deploy the Automatic Light Bar (PN: ACD01L) when deploying solutions leveraging Power Share.

Section 6 – EL2P PDU Accessories

Hardware Overview

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.

The EL2P PDU accessories are specially designed to interoperate with the EL2P controller. Connecting unapproved sensors to the NMC controller or connecting EL2P PDU Sensors to 3rd party controllers may result in damage.

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

The following table lists available sensors as well as the accessories respective associated sensor count:

Sensor	Description	Sensor Count
Temperature Sensor (EA001, EA001L)	Monitors the temperature in the rack.	1
Temperature + Humidity Sensor (EB001, EB001L)	Monitors the temperature and relative humidity in the rack.	2
Three Temperature + Humidity Sensor (EC001, EC001L)	Monitors the temperature in three areas using three separate probes and the relative humidity using one probe.	4
Door Sensor (ACA01, ACA01L)	Monitors intrusion when a door on which the sensor is installed has been opened greater than 10 mm.	1
Liquid - Rope Sensor (ED00, ED001L)	Monitors leak detection of liquid with a resistivity of less than 2 megaohms (including distilled water).	1
Liquid – Spot Sensor (EE001, EE001L)	Monitors leak detection of liquid with a resistivity of less than 2 megaohms (including	1

Sensor	Description	Sensor Count
	distilled water) in the monitored area.	
Sensor Port Hub (EF001, EF001L)	Passive hub allowing for three additional sensors to be connected.	N/A
Leak Detection Sensor Extension (EG001, EG001L)	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
Dry Contact Sensor (ACC01, ACC01L)	Input to the PDU NMC and designed to monitor a change in contact state.	1

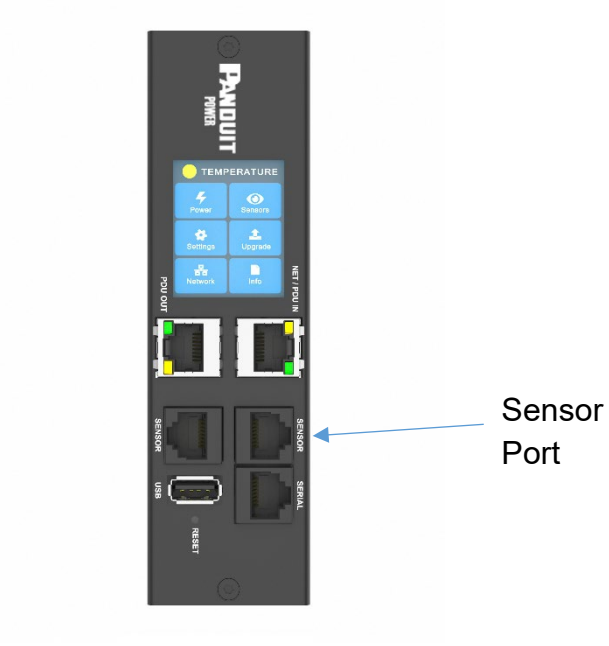


Figure 116: Sensor Port

Configuring Temperature Scale

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

1. Go to **User Accounts.**

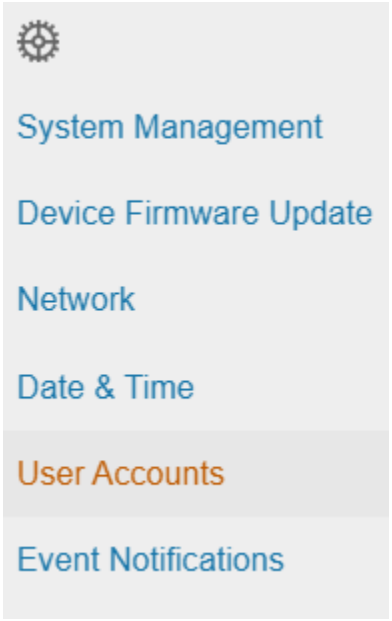


Figure 117: User Accounts

2. Select the pencil next to **Default Units**

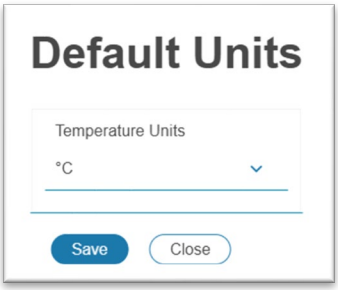


Figure 118: Temperature Units Setting

3. Select the correct units and select **Save.**

Configuring Environmental Sensors

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

1. Open the **Settings**.

2. View the Threshold section on the Settings page. Select **Threshold** to configure sensors.

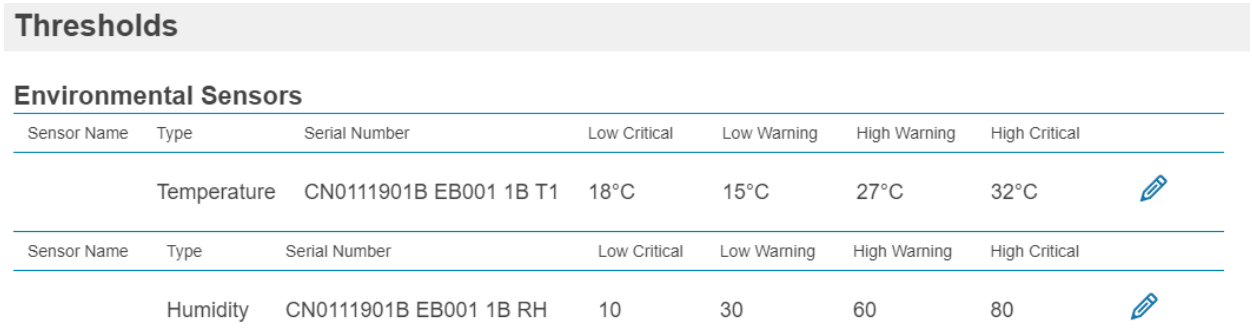


Figure 119: Environmental Sensor Threshold Configuration View

3. Select pencil next to the desired sensors.
4. In the **Edit** dialog box, type the name of the sensor
5. Type value of high critical, high warning, low warning, and low critical and check Enable box.
6. Select **Save** to exit the sensor setup

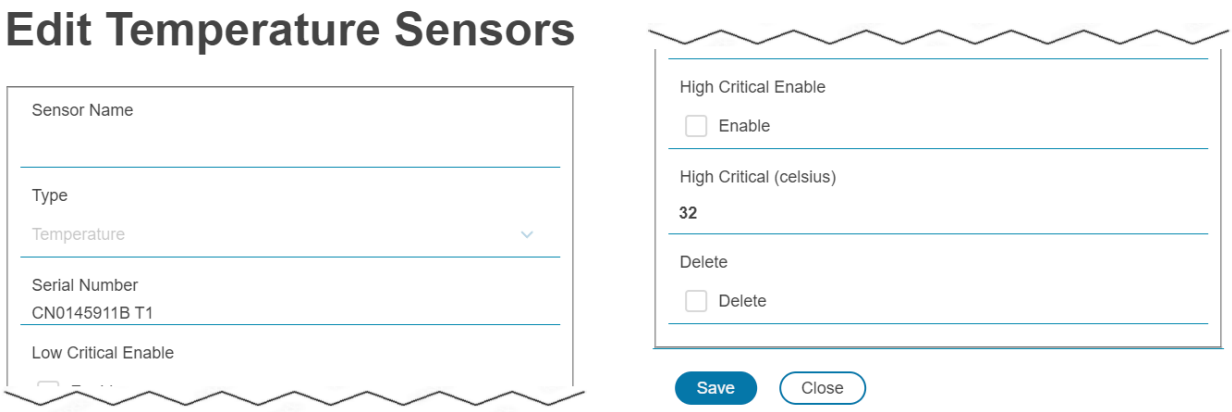


Figure 120: Temperature Sensor Edit dialog

Configuring Security Sensors

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

1. Open the **Settings**.
2. View the Threshold section on the Settings page. Select **Threshold** to configure sensors.

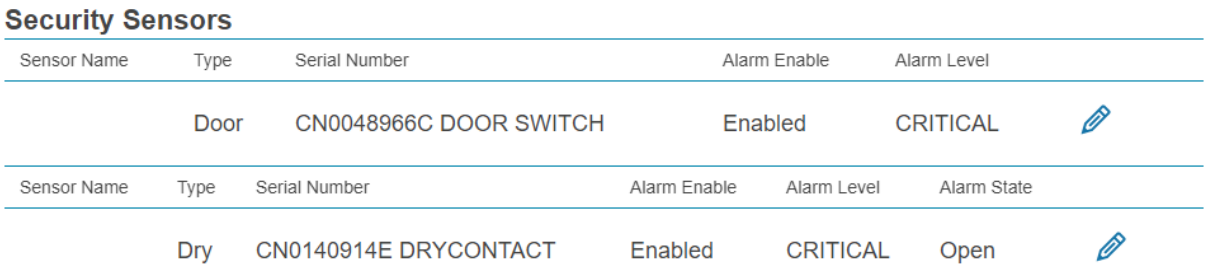


Figure 121: Security Sensor Alarm Configuration view

3. Select pencil next to the desired sensors.
4. In the **Edit** dialog box, type the name of the sensor
5. Set Alarm Level and State.
6. Select **Save** to exit the sensor setup

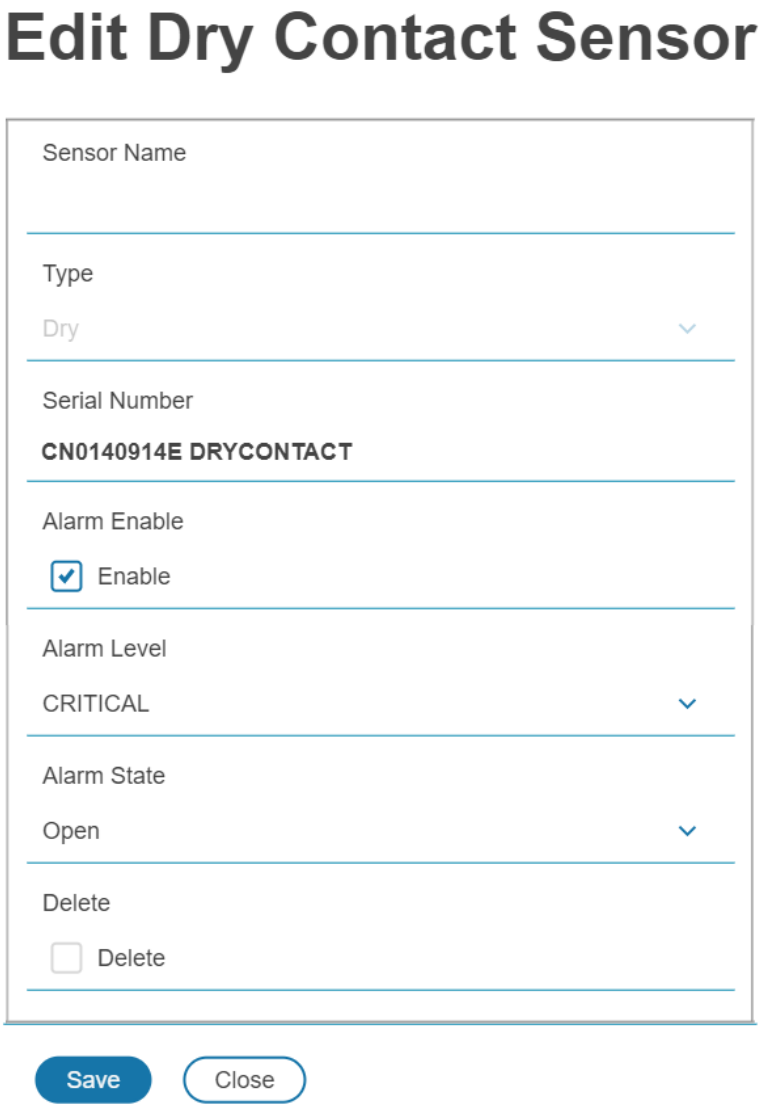


Figure 122: Dry Contact Sensor Edit dialog

Deleting Sensors

1. Select **Threshold** from **Settings** menus
2. Select pencil next to the desired sensors
3. Check **Delete** box, then save.

Section 7 – Security Handle

The Panduit EL2P PDU allows users to electronically secure and control access to cabinets.

Note. For security, verify that the handle is seated prior to engaging the locking mechanism. If the handle locks prior to the handle being properly seated, unlock the 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 123: Security Handles

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 NMC.

2. Go to the House icon > Rack Access Control.

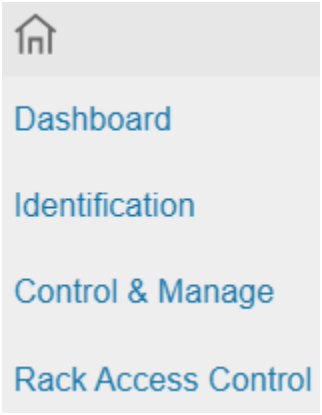


Figure 124: Rack Access Control

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.

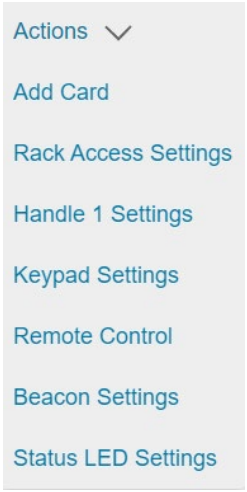


Figure 125: Rack Access Control Actions

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.

Determining Card ID

To determine the card ID, follow these steps:

1. Place the card near the reader (top of the handle).
2. Click on the **Logs** menu and choose **Event Logs** on the NMC.

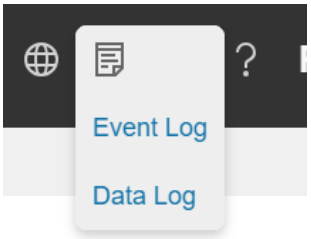


Figure 126: Event Log

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

Example:

Warning	Smart Cabinet Hot Aisle lock is swiped by non-authorized card 192292

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

Adding an access user

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

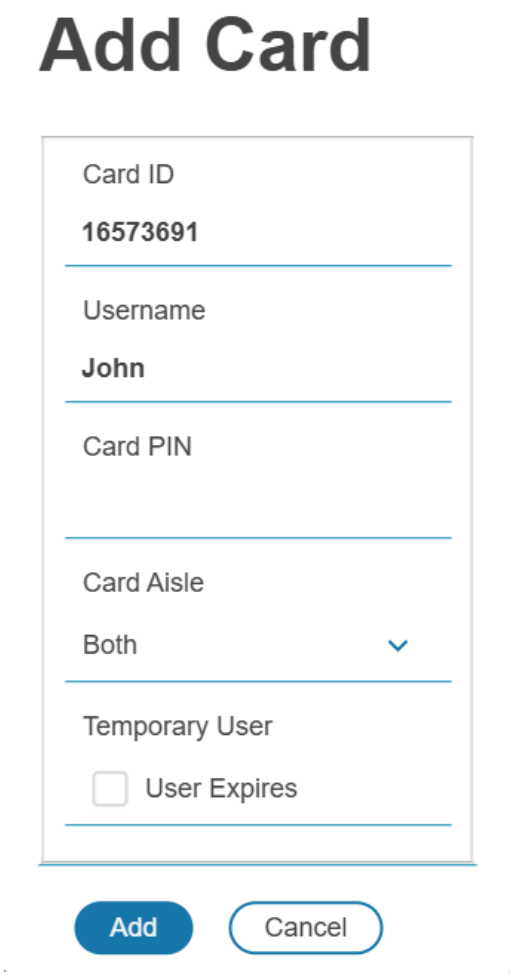


Figure 127: Add Card

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

   Note: In the above example, the card ID is 16573691
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 the user is a **Temporary User**, access begins at the **Start Time** and ends at the **Expiration Time**.

   a. Select **User Expires**.

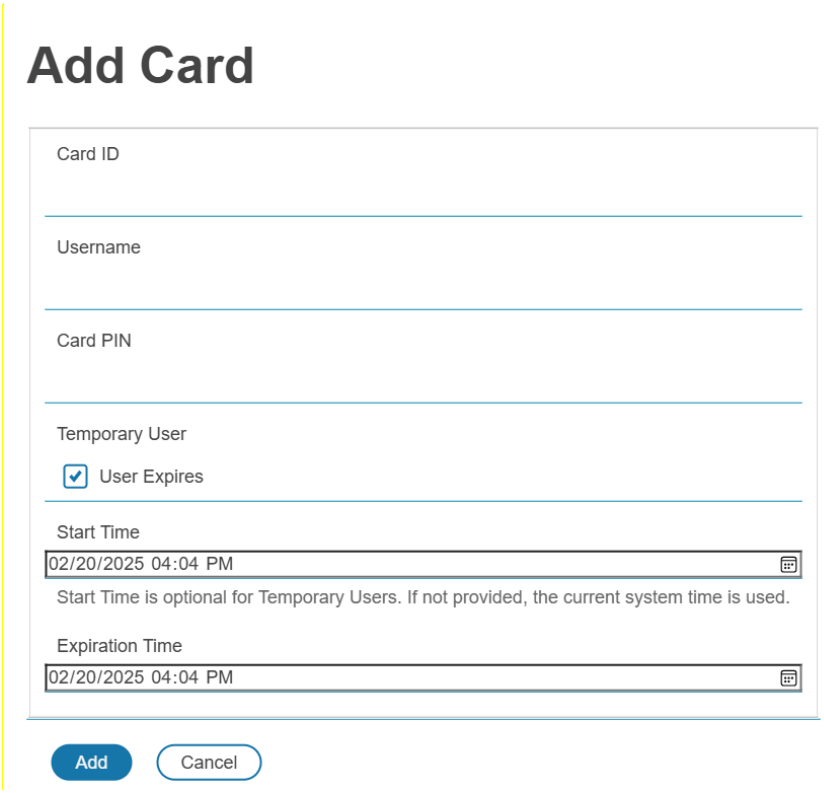


Figure 128: Add Card (Temporary User)

b. Choose a **Start Time**.

c. Choose an **Expiration Time**.

6. When **Rack Access Settings / Aisle Control** is set to **Hold/Cold Standalone**, then an additional Card Aisle field is available.

   a. Both - this user is valid for a handle configured for Hot Aisle or Cold Aisle.

   b. Cold - this user is valid for a handle configured for Cold Aisle.

   c. Hot - this user is valid for a handle configured for Hot Aisle.

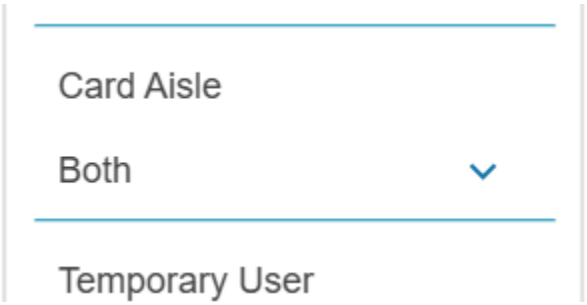


Figure 129: Add Card with Card Aisle

7. Click Add.

Editing an access user

1. To edit a card (or user), click on the pencil icon next to the user.

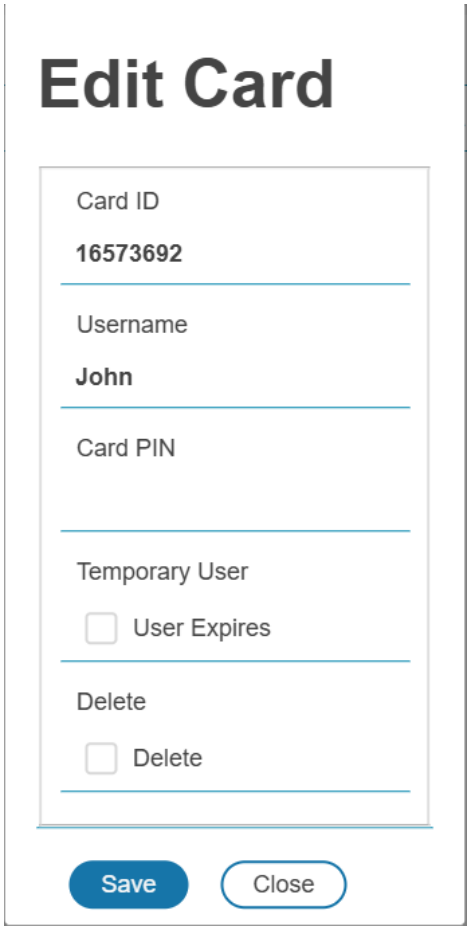


Figure 130: Edit Card

2. Modify **Card ID** if needed.
3. Modify **Username** if needed.
4. Enter **Card PIN** if needed.
5. Enter **Confirm PIN** if PIN is changed from above step.
6. If the user is a **Temporary User**, access begins at the **Start Time** and ends at the **Expiration Time**.

a. Select **User Expires**.

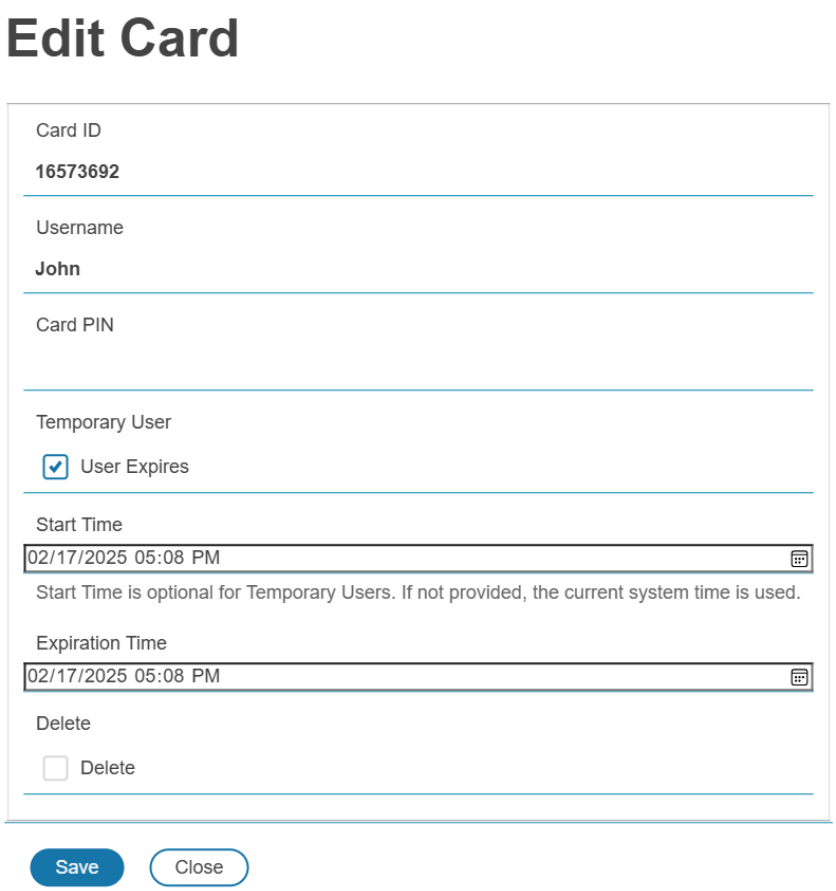


Figure 131: Edit Card (Temporary User)

b. Choose a **Start Time**.

c. Choose an **Expiration Time**.

7. When **Rack Access Settings / Aisle Control** is set to **Hold/Cold Standalone**, then an additional Card Aisle field is available.

   a. Both - this user is valid for a handle configured for Hot Aisle or Cold Aisle.

   b. Cold - this user is valid for a handle configured for Cold Aisle.

   c. Both - this user is valid for a handle configured for Hot Aisle.

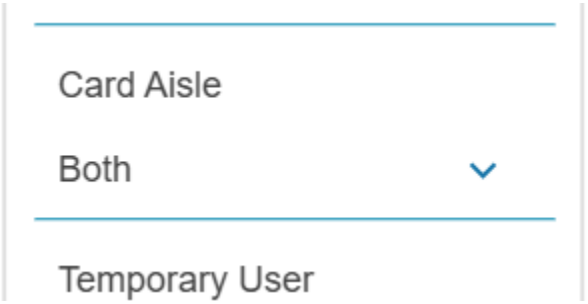


Figure 132: Add Card with Card Aisle

8. Click **Save**

Deleting an access user

1. To delete a card (or user), click on the pencil icon next to the user.
2. Check **Delete** Box.
3. Click **Save**.

Configuring Rack Access Settings

The **Rack Access Setting** is 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.

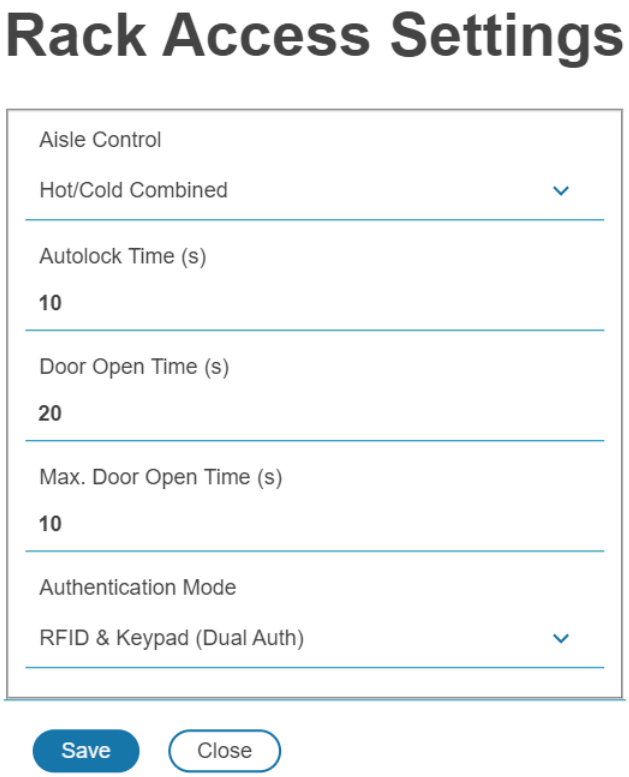


Figure 133: Rack Access Settings

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 the door open.
5. The **Max. Door Open Time** is the number of seconds before a critical alarm announces the door open.
6. Select desired **Authentication Mode**.
    a. **RFID & Keypad (Dual Auth)** – First swipe an authorized card, then within 5 seconds begin depressing an authorized secret PIN into the keypad.
    b. **RFID Only** – Gain access to cabinet through swiping an authorized card
    c. **Keypad Only** – Gain access to the cabinet through depressing an

authorized secret pin into the keypad.

7. Click **Save**.

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.

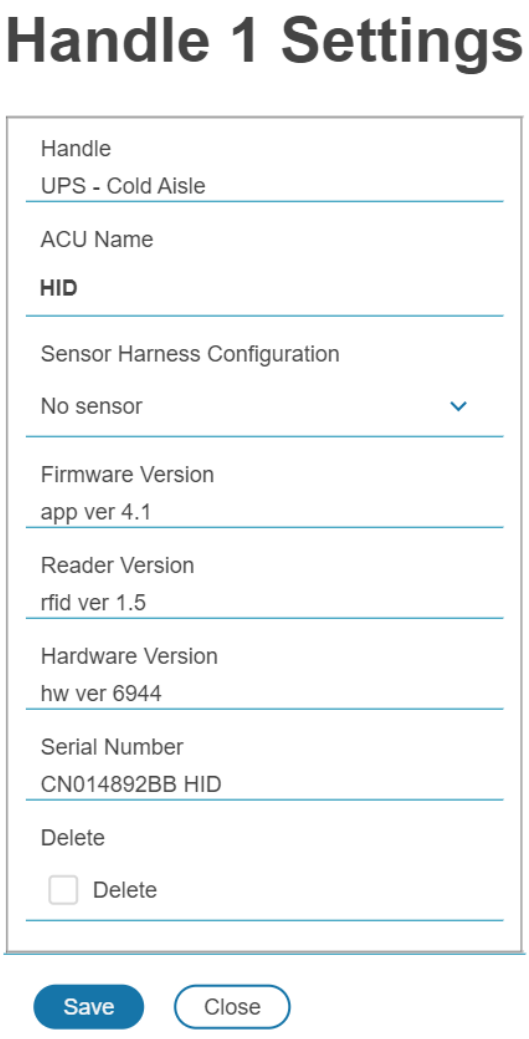


Figure 134: Handle Settings

2. 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.

3. Select **Sensor Harness** connected to the security handle.
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 Number** is the serial number of the handle.
5. To delete the handle from the system. Disconnect the handle, then check **Delete** box.
6. Click **Save**.

Configuring Keypad Settings

When the authentication mode is either keypad only or dual authentication, all users must adhere to the same PIN length, and user must select unique PIN codes in 'Keypad Only' mode.

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

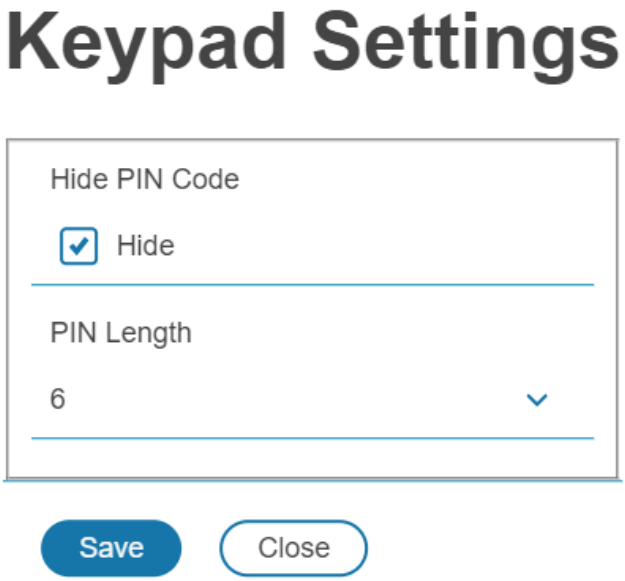


Figure 135: Keypad Settings

2. To Hide PIN code in the Web UI, check the **Hide Pin Code** box.
3. Set desired PIN length. PIN length can be one digit to 16 digits.

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.

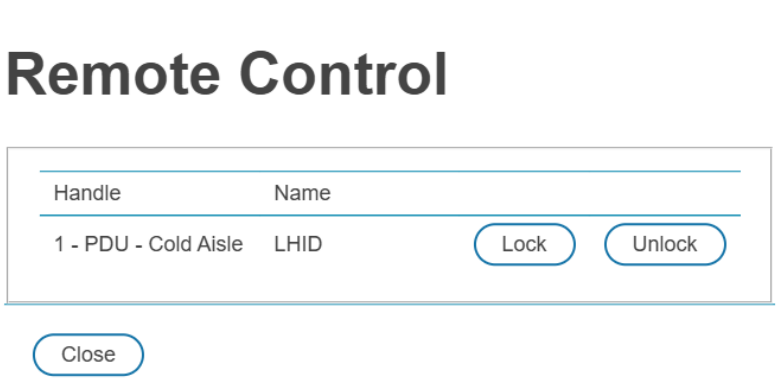


Figure 136: Remote Control

2. Select the action you wish to perform.
    a. **Lock** remotely locks the handle.
    b. **Unlock** remotely unlocks the handle.
3. When finished, Click **Close**.

Controlling the Beacon

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

Figure 137: Beacon

Beacon LED Table

Function	State	Color	Purpose
Locate	Blinking	Red, Green, Blue, Yellow, Magenta, Aqua, White	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	Red, Green, Blue, Yellow, Magenta, Aqua, White	Visual indicator on the handle. (customizable)

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

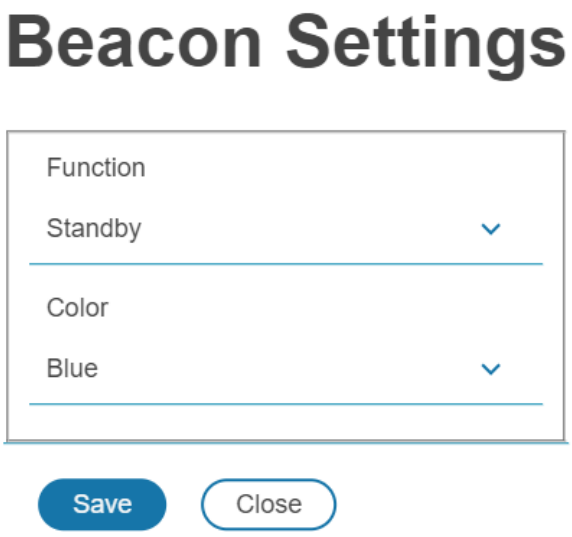


Figure 138: Beacon Settings

2. Select the function of the beacon:
    a. **Locate** – flash beacon.
    b. **Standby** – beacon color when there is no alarm.
3. Select color for **Standby** or **Locate**.
4. Click **Save**.

The Status LED

The 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 a solid green.

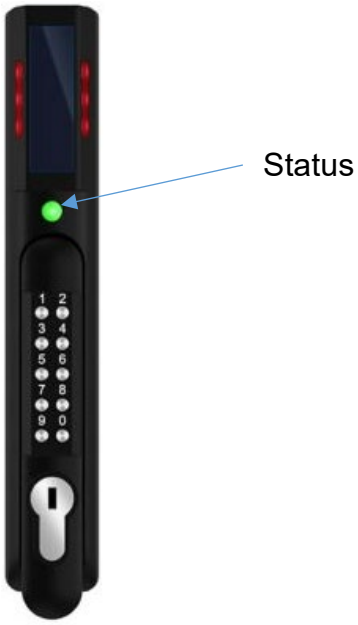


Figure 139: Status LED

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 before 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 Max Door Open Time (door sensor) (not customizable)

Note: the Door Open sensor state is the state of ANY close contact sensor connected to the system that is OPEN. The Door Open sensor state is not the same as the Mechanical Unlock state. If the handle has a Harness with a Door sensor, make sure

the Harness is configured.

Note: The Door sensor Threshold configuration is configured by default with the Alarm Enabled and the Alarm Level set to Critical. This will override the Door Open Time and Max Door Open Time alarms. Customize the Door sensors' Alarm Level, Alarm Enabled settings to meet your requirements.

Setting Status LED State

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

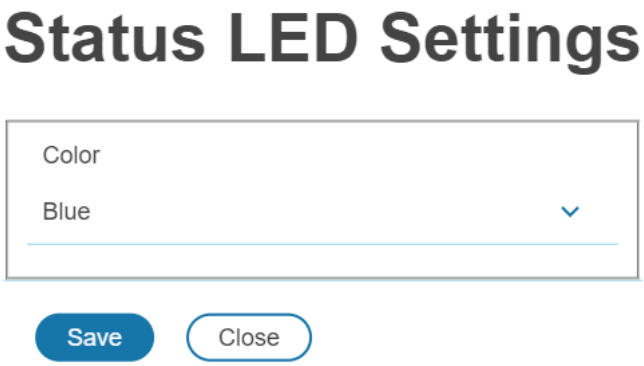


Figure 140: Status LED Settings

2. Select the color of Status LED when the handle is in standby state.
3. Click **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 ACF06L	UID	UID	UID	UID	CSN	CSN	Proprietary

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

Section 8 – 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.

API Access to Primary Features

- The product provides APIs to configure and control the system.
- The web server provides a backend REST API that is used by the web GUI frontend to manage the system.
- The web server provides a Redfish API to manage the system.

Primary Features

API Access allows authorized and permitted users to control functions of the product that are crucial to the operation of the product. Not all features may be available in all APIs. Please review the API documentation for details.

- The API user may turn on and off the outlet power on products that have controllable outlets.
- The API user may enable and disable the ability to turn on and off the outlet power on products that have controllable outlets.

Secure Disposal Features

- The product provides a “default settings” feature that can be activated using a button press on the product, from the web user interface, from the SSH command line interface, or the RJ45 serial interface.
- The default settings feature deletes the encrypted non-volatile storage files from a flash file system that contain configuration data and reinitializes the configuration data to default settings.
- When the NMC is connected to a PDU, the default settings feature deletes the encrypted non-volatile storage files from the flash file system that is stored on the PDU.
- The default settings feature deletes files from a flash file system that stores the Event Log and Data Log.
- The default settings feature deletes temporary files from a flash file system that is used to temporarily store firmware update uploads.
- The default settings feature causes the SSH RSA 2048-bit private host key to be regenerated.

Non-volatile Storage

- The product uses encrypted non-volatile files to store configuration information.
- The product uses industry standard encryption algorithms to protect non-volatile configuration data. It uses an aes-256-cbc algorithm with sha512 hash and PBKDF2 key derivation. The encryption key is stored in an internal HSM.
- The product disables the JTAG debugger.

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 as a one-way bcrypt hash.
- Passwords that the user enters are not returned to the customer. (They are ‘write only’ from a user perspective.)
- External service authentication credentials (RADIUS, LDAP) that must be provided in plain-text, are stored on encrypted non-volatile storage.
- SNMP v1/v2c community strings are stored on encrypted non-volatile storage.
- SNMP v3 usernames and passwords are stored on encrypted non-volatile storage.

Authentication Priority

Authentication checks credentials in this sequence for each enabled authentication domain:

- User Accounts
- RADIUS
- LDAP
- SSL

The User Accounts authentication domain cannot be disabled.

If a user does not exist in one domain, the next enabled authentication domain is checked.

Please do not define a valid username in multiple domains that has different passwords with different expected permission levels as it may result in a user having unexpected permission granted to them.

Network Transport Security

- The product generates a random SSH RSA 2048-bit private host key the first time the product starts up.
- The product has a randomly generated RSA 2048-bit private key configured by the factory. This key is used to generate a HTTPS certificate the first time the product starts up.
- 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 or prime256v1 (SECP256R1).
    - 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; ECC curves: SECP192R1, SECP224R1, SECP256R1, SECP384R1, SECP521R1, SECP192K1, SECP224K1, SECP256K1, BP256R1, BP384R1, BP512R1, CURVE25519.
- The user may upload a custom HTTPS private key that is encrypted using a password. Private key decryption is compatible with default openssl key generation password encryption formats.
- The product uses TLS 1.2 to communicate with HTTPS web browser clients.
- Secure communication cipher negotiation with HTTPS clients uses these Cipher Suites:
    - Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
    - Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
    - Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
    - Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
    - Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)
    - Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)
    - Cipher Suite: TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x009e)
    - Cipher Suite: TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x009f)
- The product uses TLS 1.2 to communicate with LDAPS and LDAP+StartTLS servers.
- The product uses TLS 1.2 to communicate with SMTP+STARTTLS and SMTPS servers.

- Secure communication cipher negotiation with SMTP servers and LDAP servers uses these Cipher Suites:
  - Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)
  - Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)
  - Cipher Suite: TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xccaa)
  - Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
  - Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
  - Cipher Suite: TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x009f)
  - Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)
  - Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
  - Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x006b)
  - Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
  - Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
  - Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
  - Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
  - Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
  - Cipher Suite: TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x009e)
  - Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)
  - Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)
  - Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x0067)
  - Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
  - Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
  - Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
  - Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
  - Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
  - Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
  - Cipher Suite: TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 (0xc032)

- Cipher Suite: TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 (0xc02a)
- Cipher Suite: TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f)
- Cipher Suite: TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02e)
- Cipher Suite: TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026)
- Cipher Suite: TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005)
- Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
- Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)
- Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
- Cipher Suite: TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 (0xc031)
- Cipher Suite: TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 (0xc029)
- Cipher Suite: TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e)
- Cipher Suite: TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02d)
- Cipher Suite: TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (0xc025)
- Cipher Suite: TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004)

- The product provides a SSH server with these algorithms to communicate with SSH clients:
  - Key exchange algorithms:
    - curve25519-sha256
    - curve25519-sha256@libssh.org
    - kexguess2@matt.ucc.asn.au
    - diffie-hellman-group14-sha256
    - ecdh-sha2-nistp256
    - ecdh-sha2-nistp384
    - ecdh-sha2-nistp521
  - Key exchange algorithms for compatibility:
    - diffie-hellman-group14-sha1
  - Host key algorithms:
    - rsa-sha2-256 (2048-bit)
  - Host key algorithms for compatibility:
    - ssh-rsa (2048-bit)
  - Encryption algorithms:
    - chacha20-poly1305@openssh.com
    - aes128-ctr
    - aes256-ctr
  - MAC algorithms:
    - hmac-sha2-256

- MAC algorithms for compatibility:
  - hmac-sha1

Wireless Communication

- NMC Part Number CNT05 and MA060 do not have Wi-Fi. This section does not apply to those part numbers.
- NMC Part Number CNT06 has Wi-Fi.
- The product will communicate via Wi-Fi if it is enabled and configured.
- The Wi-Fi configuration data is stored on encrypted non-volatile storage.
- The product will communicate via Wi-Fi as a wireless Access Point when the “Direct Connect” feature is enabled and activated.
- The product defaults to having Direct Connect enabled and configured for “On Demand” Mode: The user must momentarily physically actuate the reset button to enable the wireless Access Point.
- The product communicates using Wi-Fi on 2.4 GHz frequencies.
- The product communicates using Wi-Fi 802.11b standard.
- The product communicates using Wi-Fi 802.11g standard.
- The product communicates using Wi-Fi 4 (802.11n) standard.
- The product communicates using Wi-Fi and provides user configurable WPA2 Personal encryption support.
- The product communicates using Wi-Fi and provides user configurable WPA2 Enterprise encryption support.
- The product supports these following Wi-Fi Extensible Authentication Protocols: TLS, PEAP, TTLS.
- The product supports these following Wi-Fi inner authentication methods: MSCHAPv2, MSCHAP, PAP, CHAP.
- The product communicates using Wi-Fi and provides user configurable WPA3 Personal encryption support.
- The product communicates using Wi-Fi and provides user configurable WPA3 Enterprise encryption support.

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.

External Authorization Mechanisms

- LDAP & RADIUS – username & password are stored on encrypted non-volatile storage.
- CVE-2024-3596 BlastRADIUS: The firmware includes a “Always send Message-Authenticator attribute” feature that must be enabled to mitigate the BlastRADIUS vulnerability.
- LDAP is not encrypted over the network.
- LDAPS and LDAP with StartTLS are encrypted over the network.
- If a “Server Certificate” is configured and “Verify Server Certificate” is enabled, then the remote LDAP server authenticity is validated.
- The user may upload a custom LDAP Client Private Key that is encrypted using a LDAP Client Private Key Password. Private key decryption is compatible with default openssl key generation password encryption formats.
- The RADIUS protocol is designed to only transmit hashed and obfuscated passwords over the network.

Secure Boot Protection

- The product uses industry standard code signature algorithms to protect firmware booted by the device.
- A signature block is appended to the bootloader and internal HSM.
- The signature block contains a signature of the bootloader and the RSA 3072-bit public key.
- A digest of the RSA 3072-bit public key is stored in a write-once eFuse (which cannot be read or written to after being set) and used to verify the signature block.
- The public key signature is verified against the signature block and a digest of the bootloader to establish authenticity and integrity of the bootloader.
- The bootloader continues the chain of trust by verifying the authenticity and integrity of the application executable.

Firmware Update Protection

- The product uses industry standard cryptography to verify a firmware update package, to establish authenticity and integrity.
- The package contains a manifest describes items contained in the package payload.
- The items are described as a chunk size and a SHA256 hash of each sub-item and the payload container in the package.
- The manifest is hashed using SHA256 and signed using an RSA 4096 bit key.
- The package contains the signature of the hash of the manifest.
- The package contains a payload container holding the sub-items.
- The signature of the payload is verified before parsing the content of the manifest or the payload.
- The firmware application image uses AES encryption and RSA signatures to provide confidentiality, authenticity and integrity.

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.

Secure deployment

To maintain the highest level of security from, Panduit recommends the user configures the NMC with the following settings.

Upload Certificate

Certificates ensure that in a secure connection, the user is authorized to access the device. It is recommended that X.509 SSL certificate is uploaded to the NMC and that the certificate use a RSA 2048-bit key. The HTTPS Certificate and HTTPS Private Key can be accessed from **Settings → Network settings → Web Access Configuration**

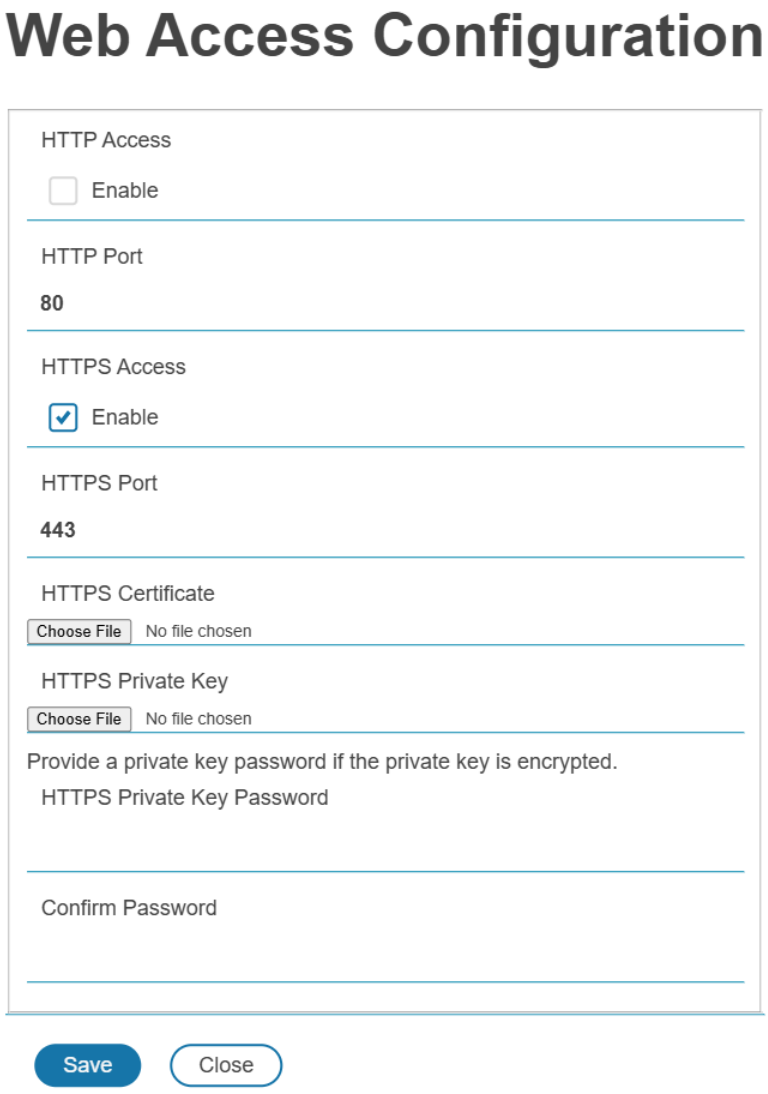


Figure 141: SSL Certificate Load Screen

Use SNMPv3c

The Panduit PDU NMC comes with support for both SNMPv2c and SNMPv3. For a higher security deployment, it is recommended to disable SNMPv2c. Another recommendation is to configure all SNMPv3 user and traps receiver with an “Auth Priv” security level, authentication algorithm of SHA and a privacy algorithm of AES256.

Use RADIUS with “Always send Message-Authenticator attribute” enabled

The RADIUS server should be configured to always require the RADIUS client to send the Message-Authenticator attribute.

Disabling unused interfaces

The default setting is to have HTTPS and SSH enabled. If these interfaces are not in use, it is recommended to disable these interfaces.

Unused physical ports may be protected using “lock out” plugs.

Review Session management

The NMC gives the customer the flexibility to change session management settings.

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, see *Safety and Compliance Information* at the Panduit website:

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

Product Support and Other Resources

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

Chatbot Available 24/7

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
- Technical Issues

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
- Technical Issues

Email: TechSupportEMEA@panduit.com

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

Global System Support for Deployed Solutions:

- Firmware Updates
- Device setup (Network, Access control, etc..)
- Third party DCIM, MIB Walk, SNMP Setup, Email Setup, Trap Recievers
- Return Material Authorizations (RMAs)

Email: SystemSupport@panduit.com

Acronyms and Abbreviations

A

Amps/Amperes

AC

Alternating Current

AES

Advanced Encryption Standard

CLI

Command Line Interface

DHCP

Dynamic Host Configuration Protocol

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

NMC

Network Management Card

PDU

Power Distribution Unit

SHA

Secure Hash Algorithms

SNMP

Simple Network Management Protocol

TCP/IP

Transmission Control Protocol/Internet Protocol

UPS

Uninterruptible Power Supply

USB

Universal Serial Bus

V

Volts

W

Watts

Appendix A: Firmware Update Procedure

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

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 NMC. For the latest firmware please visit: panduit.com → Support → Download Center → PDU

1. Download the firmware file from the web page.
2. Unzip the downloaded file.
3. Open the User interface in a web browser by entering the NMC IP address.
4. Login to with Administration credentials.
5. Go to **Settings > Device Firmware Update > Actions > Upload Firmware**.
6. In the Firmware Update dialog box, click on 'Choose File', then browse to the firmware file named 'pdu-package-*.*.*.bin'.

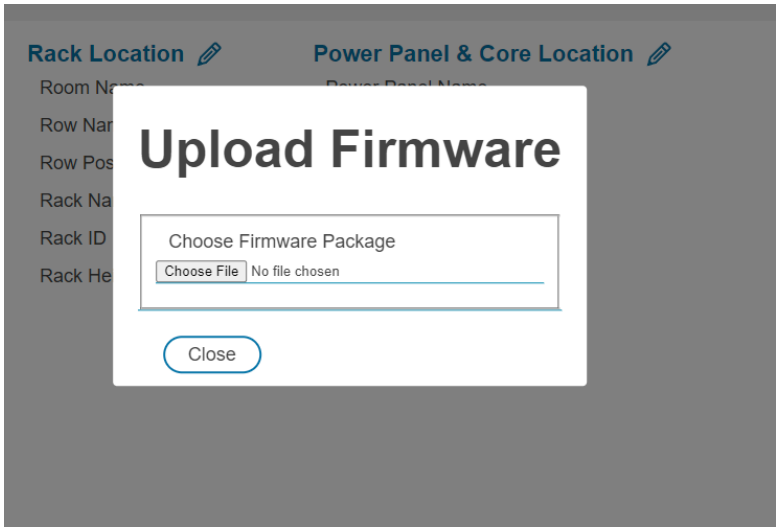


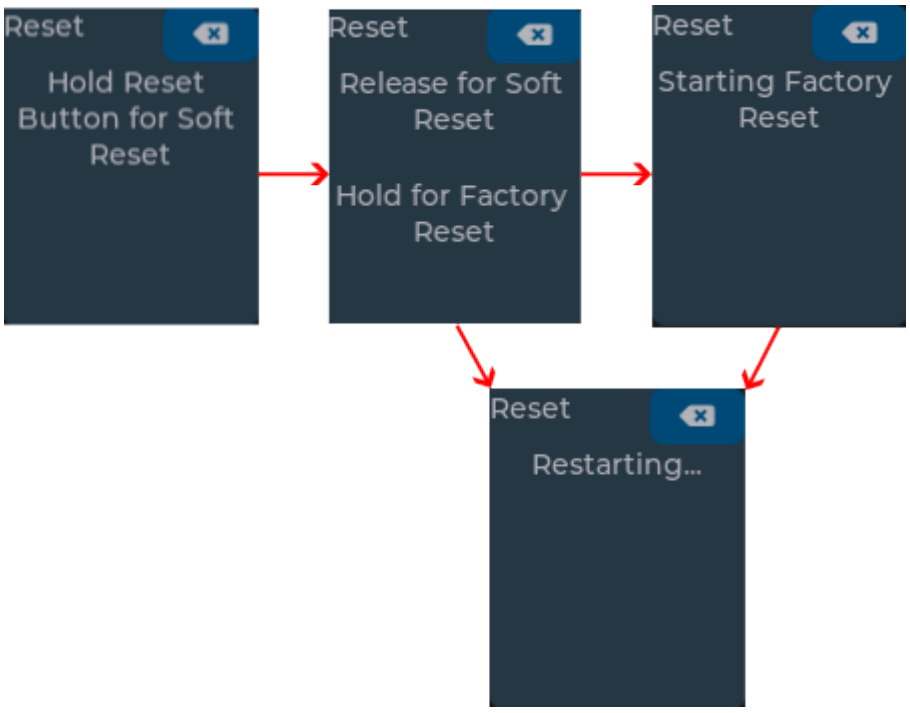
Figure 142: Upload

7. The system will update after selecting the file.
8. When the upload is finished, the system will reboot automatically.
9. In Daisy Chain Convention, once a user starts the firmware update on the primary PDU, all linked PDUs are automatically updated.

Appendix B: System Reset or Password Recovery

To perform a system reset, press and hold the **RESET** button, located on the front of the NMC, for 2 seconds to reboot the NMC. This will cause a reboot of the NMC controller; all configuration(s) will be retained.

To Default the controller to factory settings, press and hold the **RESET** button for at least 8 seconds. This will cause a factory reset of the NMC controller, erasing all existing configurations, including any usernames and passwords. The NMC will restart after this operation.



To recover a user's lost password, first login under an administrator account. Select the **User** icon in the top right corner of the screen, and then select **User Accounts**.

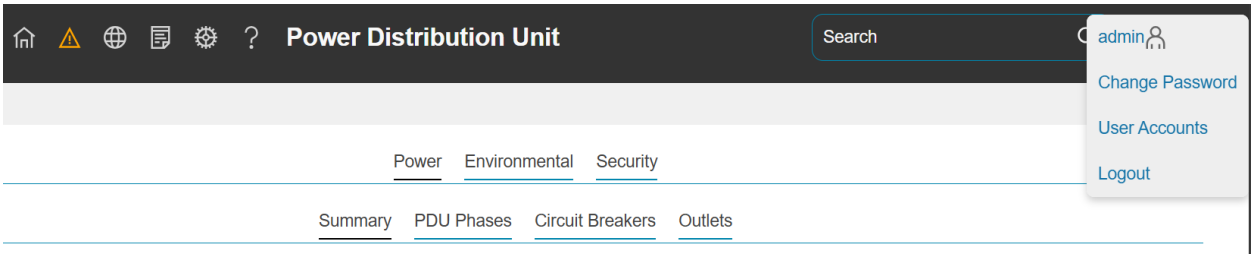


Figure 143: User Accounts from the User Icon

Alternatively, you can select the **Gear** icon and click on **User Accounts**. Both will take you to the same page.

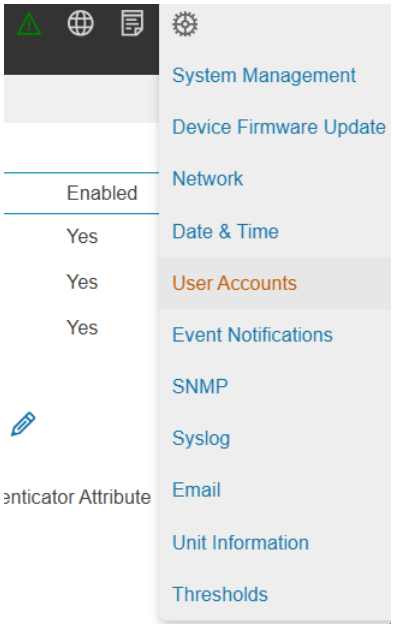


Figure 144:User Accounts from Gear Icon

On the left-hand side of the screen, you will see the **Users** table. Click the **Pencil Icon** next to the user who has lost their password.

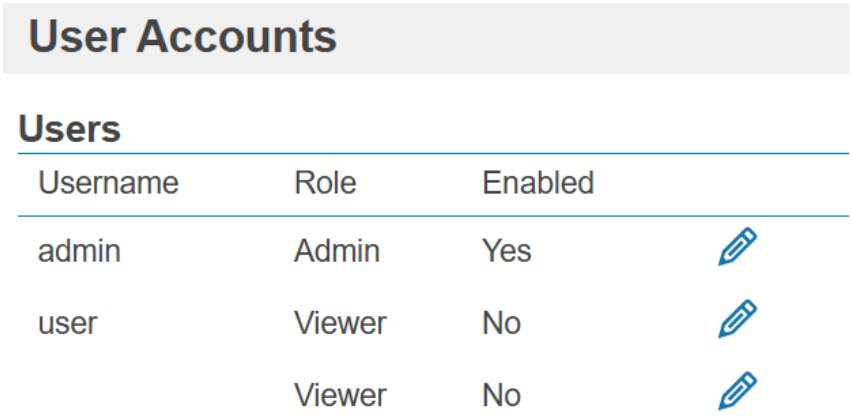


Figure 145: Users Table

In the Edit User screen, you can assign a new password by typing it into the Password field and then retyping it in the Confirm Password field. You may also choose to enable the "Must Change Password at next Log In" option, which will require the user to create a new password the next time they log in. When finished, click Save and log out. The user can then log in with the password you have created.

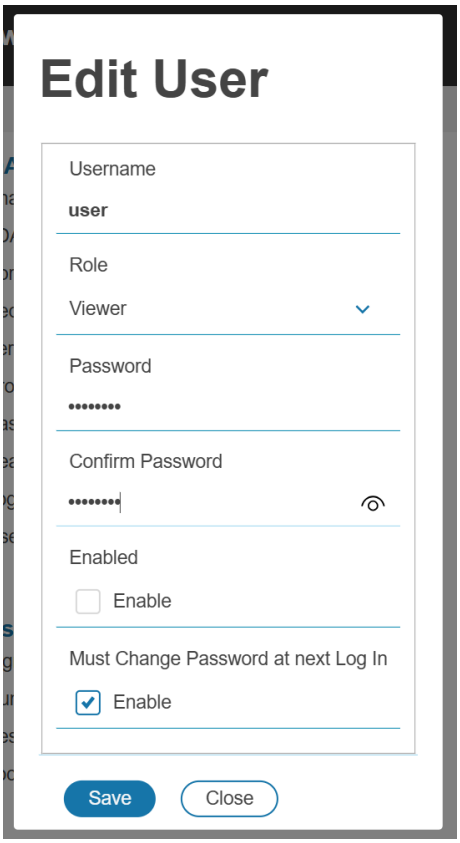


Figure 146: Edit User Screen

Appendix C: Direct connect via Ethernet without Bonjour

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

1. Type **network connections** into Windows Search and select **View network connections**.

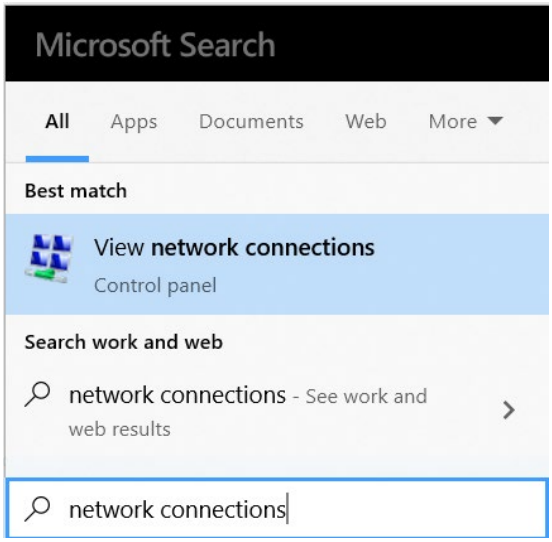


Figure 147: View network Connections

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

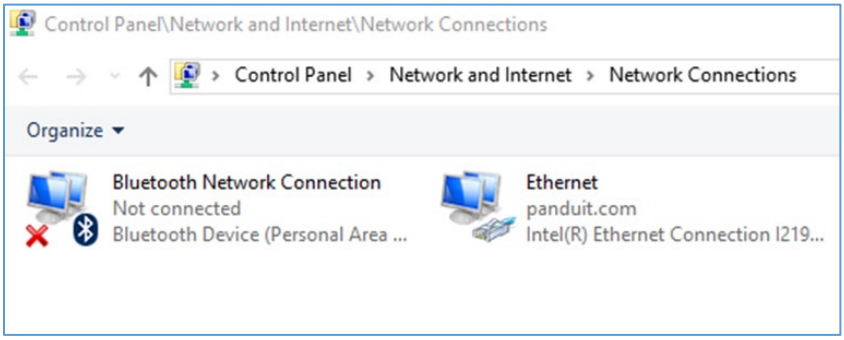


Figure 148: Properties

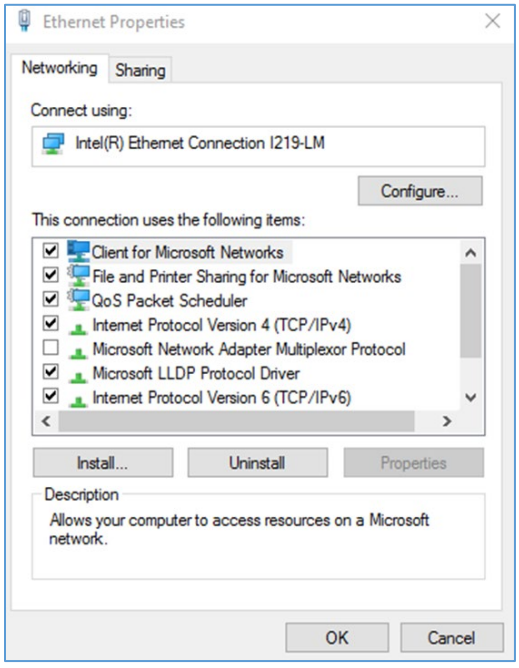


Figure 149: Ethernet Properties

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

Figure 150: Internet Protocol Version 4

4. If not already selected, select the **Obtain an IP address** radio button and the **Obtain DNS server address automatically** radio button.
5. Click **OK** to accept the configuration.
6. Connect the NMC network connection directly to the PC's Ethernet port using a patch cable.
7. Power the NMC unit.
8. Wait 60 seconds.
9. Open a web browser on the PC.
10. In web browser address bar, type **https://169.254.254.1,** and press <Enter>.

    A Privacy Error or an error explaining that the certificate (cert) authority is invalid may be displayed. This message is presented when a device has the initial certificate in-use. You may proceed as this error is expected.

Appendix D: Command Line Interface

The NMC provides its command line interface through the Serial port and the SSH network protocol. The command line interface allows the user to read or write to the NMC data model.

Logging in using Serial port

- Connect a USB console cable between a PC and the NMC Serial (RJ45) port
- Open a terminal emulator program such as Tera Term
- Set 115200 baud rate, 8 bit data, no parity, 1 stop bit, no flow control
- Connect corresponding COM port
- Use the same credentials from web UI

Logging in using SSH protocol

- Identify IP address of the NMC
- Open an SSH program such as PuTTY
- Open connection to the NMC
- Use the same credentials from web UI

Changing Your Password

At initial login, you are required to change the default password if not changed from web UI. The default username is admin and the default password is admin

Enter the username, current password, and new password twice to confirm. The passwords must be between 8 and 40 characters and follow three of the following four rules:

- Contain at least one lowercase character
- Contain at least one uppercase character
- Contain at least one number
- Contain at least one special character

Command list

After logging in 'PANDUIT>' prompt is shown and waiting for commands. Only following commands are accepted.

- **read**

  Read stored data from the data model. Parameter can be object name or individual item. When queried with object name, it will display all items in the object.

  Example: read status/mfgData

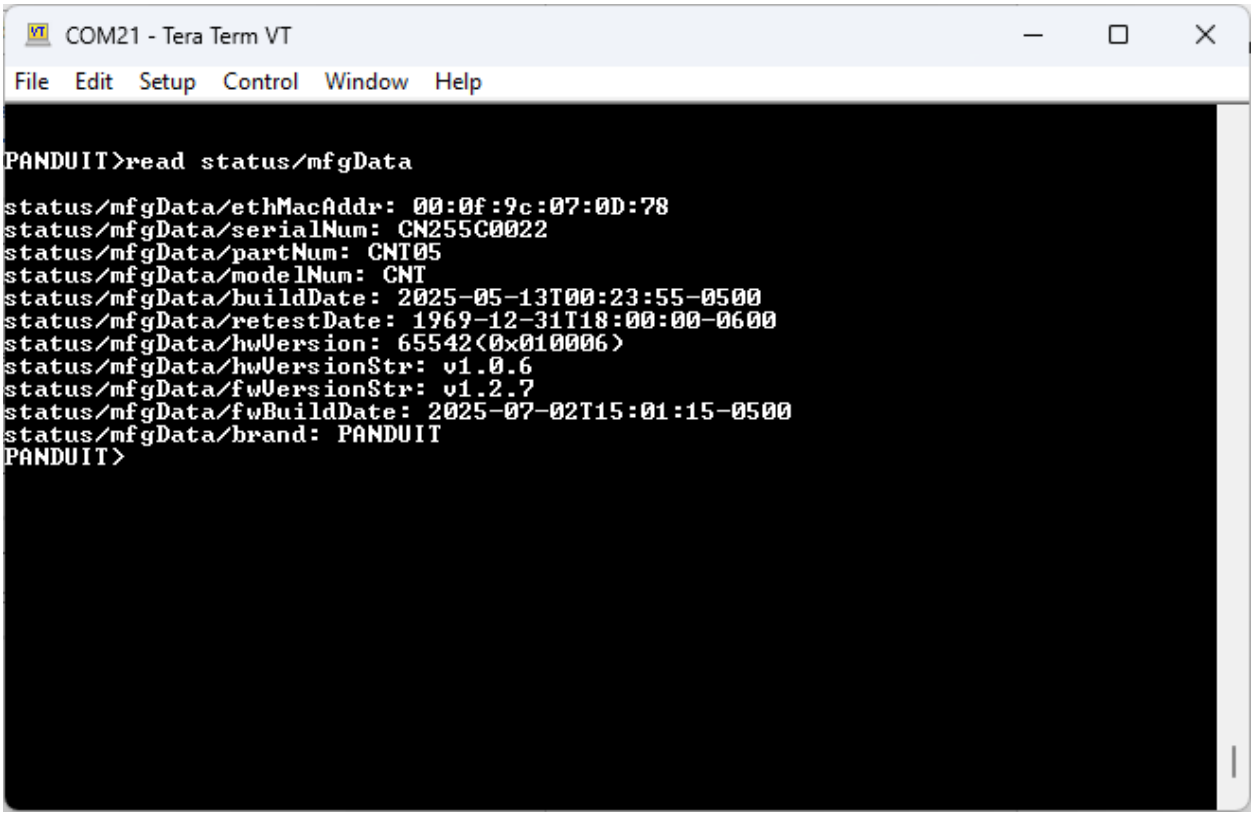


Figure 151: Reading from CLI

- **write**

  Set a value to an individual item in the data model

  Example: write config/systemInfo/systemName DC1-PDUA1

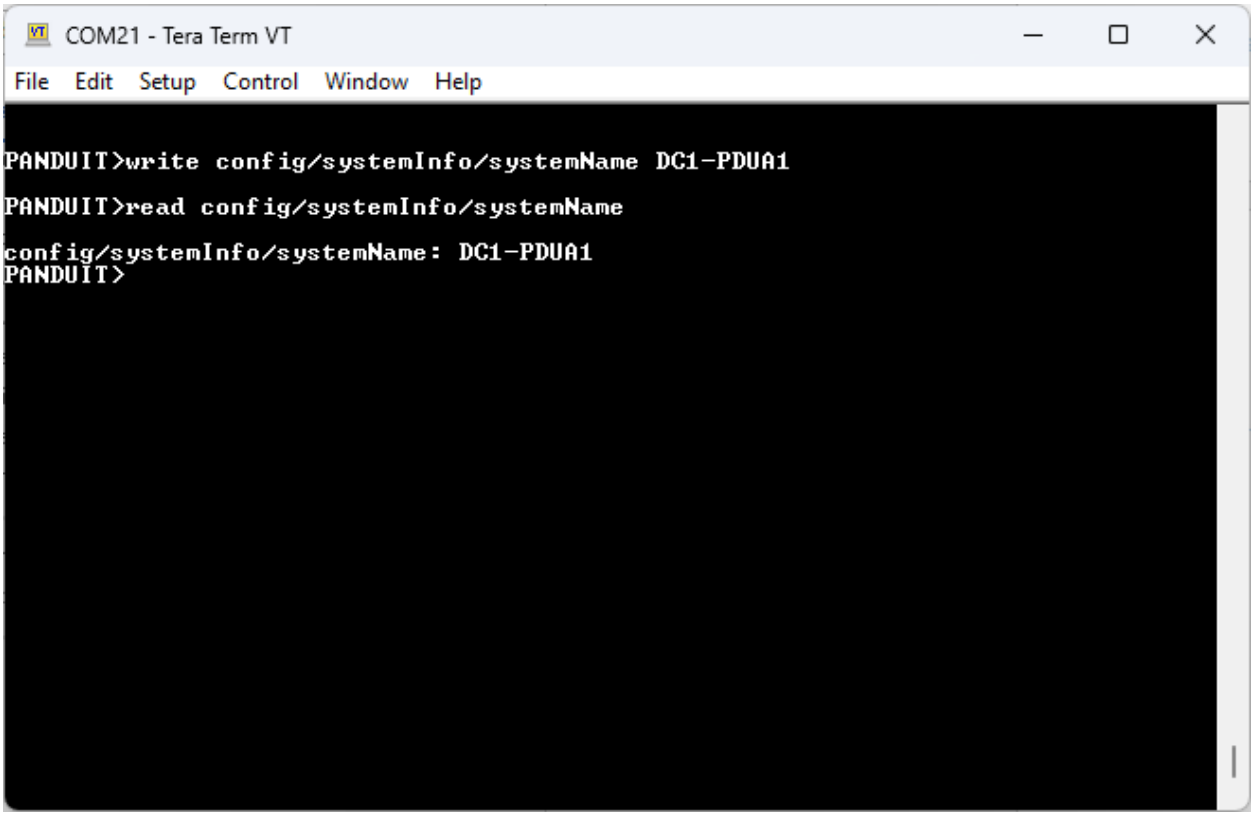


Figure 152: Writing from CLI

- **list**

  List all objects in the data model

- **list *object***

  Display options for an *object* in the data model

- **help, ?**

  Display all command list and usage

- **logout, quit**

  Log out the user

Appendix E: 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       Panduit-User-Role       1       integer
VALUE           Panduit-User-Role       User    1
VALUE           Panduit-User-Role       Admin   2
VALUE           Panduit-User-Role       Control 3
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 “viewer” 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"
                     Panduit-User-Role = Admin,
                     Service-Type = 1
    ```

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

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

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

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

7. 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
        Panduit-User-Role = Admin
        Service-Type = Framed-User
```

Appendix F: POSIX Time Zone Information

The custom time zone format is:

```
STD Offset DST DstOffset,DSTStart,DSTEnd
```

(Spaces added for clarity should be removed as shown in the examples below)

`STD` is the time zone abbreviation used when in standard time.

`Offset` is the standard time offset from UTC

`DST` is the time zone abbreviation used when in daylight-savings time.

`DstOffset` is the daylight-savings time offset from UTC

(May be omitted if DST is one hour less than STD)

`DSTStart and DSTEnd` are in format:

`Mm.n.d/H:MM:SS`

- m (1-12) for 12 months
- n (1-5) 1 for the first week and 5 for the last week in the month
- d (0-6) 0 for Sunday and 6 for Saturday
- H (0-24) hour
- MM (00-60) minute
- SS (00-60) second

Example 1: The US Central timezone is specified as follows:

```
CST6CDT,M3.2.0/2:00:00,M11.1.0/2:00:00
```

`CST` is the time zone abbreviation when daylight savings time is off.

`6` is the number of hours difference from UTC

`CDT` is the timezone abbreviation when daylight savings time is on

`M3.2.0/2:00:00` specifies DST starts on the second Sunday of March at 2AM

`M11.1.0/2:00:00` specifies DST end on the first Sunday of November at 2AM

Example 2: China time is specified as follows:

```
CST-8
```

`CST` is the time zone abbreviation for China Time

`-8` is the number of hours difference from UTC

(There is no daylight savings time in China, so the remaining fields are omitted)

Appendix G: Secure Zero Touch Provisioning (sZTP)

A fundamental business requirement for any network operator is to reduce costs where possible without compromising security.

For network operators, deploying devices is not only a significant cost but also introduces variability as trained specialists may differ in their deployment methodology. Secure Zero Touch Provisioning (sZTP), a bootstrapping strategy enabling devices to securely obtain bootstrapping data with no installer action beyond physical placement and connecting network and power cables.

Panduit's Secure Zero Touch Provisioning follows the RFC 8572.

Below is the step by step process to configuring Secure Zero Touch Provisioning on the EL2P line of PDUs.

Step 1: Request Signed Certificates from systemsupport@panduit.com

Step 2: Setup the environment as follows…