PANDUIT®
infrastructure for a connected world

Panduit EL2P PDU

User Manual

Version 1.8

Table of Contents

AI Ready Documentation 13
AI-Ready User Manual 13
Section 1 – System Overview 14
PDU Controller 14
Connecting the NMC via Ethernet Port 14
Connecting the NMC via Wi-Fi (PN: CNT06 Required) 15
Connecting the NMC to a Computer Serial Port 16
Section 2 – Web Graphical User Interface (GUI) 18
Internet Protocol (IP) Addressing 18
Web Connection 18
Introduction to the Web GUI 20
Introduction to the Dashboard 22
System Management 24
Network Settings 31
Unit Information 40
Setting Time and Date on the NMC 42
Control & Manage 45
Outlet Power Management 46
Outlet Control Enable/Disable 50
Outlet Power Sequence Setup 51
Reset All PDUs Energy 54
PDU Energy 55
Outlet Energy 56
Setting Metering Thresholds 58
Syslog Setup 68
Email Setup 72
Event Log 75
Data Log 76

Web Interface Access 77
Event Notifications 84
Wi-Fi Settings (PN: CNT06 Required) 86
Section 3 – Simple Network Management Protocol (SNMP) 92
SNMP Management Configuration 92
Configuring SNMP User 94
Configuring SNMP Traps 98
Section 4 – Local Display 102
Onboard Display and Network Controller 102
Network Controller Menu Structure 103
Main Menu Selections 103
Sensors Menu 109
Settings Menu 109
Help Menu 119
Search Box 120
Section 5 – Daisy Chain Configuration 123
Daisy-Chain Overview 124
Daisy-Chain Setup 124
Bridge Mode Daisy Chain 125
Bridge Mode Setup 126
Power Share 127
Section 6 – EL2P PDU Accessories 129
Hardware Overview 129
Configuring Temperature Scale 132
Configuring Environmental Sensors 132
Configuring Security Sensors 133
Deleting Sensors 135
Section 7 – Security Handle 136
Configuring Cabinet Access Control 137

Adding a User for Local Rack Access 138
Configuring Rack Access Settings 144
Configuring Handle Settings 146
Configuring Keypad Settings 147
Remote Controlling the Handle 148
Controlling the Beacon 148
The Status LED 150
Setting Status LED State 152
Handle and Compatible Card Types 152
Section 8 – Security 153
Standards Compliance 153
API Access to Primary Features 153
Primary Features 153
Secure Disposal Features 153
Secure Erase — NIST SP 800-88 Media Sanitization 154
Overview 154
NIST SP 800-88 Rev. 1 Classification 154
eMMC Purge Procedure (NMC) 155
SPI NOR Flash Clear Procedure (Backplane) 155
Trigger and Execution Flow 156
Log and Audit Record 157
Limitations 157
References 157
Non-volatile Storage 157
Authentication Data 157
Authentication Priority 158
Network Transport Security 158
Wireless Communication 162
Network Configuration Data 163

Logging 163
External Authorization Mechanisms 163
Secure Boot Protection 164
Firmware Update Protection 164
Other Features 165
Protocols 165
Secure deployment 165
Security Response 168
Warranty and Regulatory Information 169
Warranty Information 169
Regulatory Information 169
Product Support and Other Resources 170
Accessing Panduit Support 170
Acronyms and Abbreviations 172
Appendix A: Firmware Update Procedure 173
Manual Update 173
Auto Update 174
Auto Update Configuration 174
Appendix B: System Reset or Password Recovery 176
Appendix C: Direct connect via Ethernet without Bonjour 180
Appendix D: Command Line Interface 183
Appendix E: RADIUS Server Configuration 186
Appendix F: POSIX Time Zone Information 188
Appendix G: Secure Zero Touch Provisioning (SZTP) 189
Getting Started with SZTP 189
Summary of SZTP Setup 189
Certificate Configuration 190
Voucher Request 190
SZTP Operation 190

Appendix H: Zero Touch Provisioning (1-Touch ZTP) 192
Getting Started with 1-Touch ZTP 192
Summary of 1-Touch ZTP Setup 192
Appendix I: SZTP Server Discovery (via DHCP or mDNS) 194
mDNS 194
DHCP Option 194
Appendix J: SZTP Bootstrap Server Installation 197
Bootstrap Server Configuration 201
Troubleshooting SZTP 203
Appendix K: Onboard Data Collector Configuration 205
Requirements 205
Collector PDU Setup 205
Device PDU Setup 207
Registering PDUs to Cisco Nexus Dashboard 209
Notes 213
Security 213
Communication Diagrams 213
Appendix L: Bulk Management with SiteCommand Utility 216
Appendix M: Frequently Asked Questions (FAQ) 217

Table of Figures

Figure 1: LCD Configuration 14
Figure 2: Ethernet Port for Network Connection 15
Figure 3: Serial In Port 16
Figure 4: Network information from + ... 17
Figure 5: Refused Connection Example 18
Figure 6: Certificate Warning 19
Figure 7: Login Page 19
Figure 8: After Login 20
Figure 9: Landing Page/Dashboard 20
Figure 10: Power Summary Page 22
Figure 11: Power Outlets Page 23
Figure 12: Environmental Monitoring Page 23
Figure 13: Security Monitoring Page 24
Figure 14: System Management 25
Figure 15: System Information Configuration 25
Figure 16: LCD Configuration 26
Figure 17: PDU Locate 27
Figure 18: PDU Region 28
Figure 19: System Management Actions 28
Figure 20: Upload Configuration 29
Figure 21: Default Settings Warning 29
Figure 23: Secure Erase Warning 30
Figure 22: Secure Erase Complete 30
Figure 24: Restart Warning 31
Figure 25: Ethernet Interface Configuration 32
Figure 26: DNS Configuration 33
Figure 27: Web Access Configuration 33
Figure 28: Network Settings 34
Figure 29: Web Access Configuration 34
Figure 30: Upload Certificates 35
Figure 31: SSH Configuration 35
Figure 32: IEEE 802.1X Configuration 37
Figure 33: IEEE 802.1X Verification Options 38
Figure 34: Unit Information 40
Figure 35: Rack Location Configuration 41
Figure 36: Power Panel & Core Location 42

Figure 37: Setting the Date and Time 43
Figure 38: NTP Configuration 43
Figure 39: Daylight Saving Time Zone Configuration 44
Figure 40: Starting NTP Test 45
Figure 41: Status of NTP Test 45
Figure 42: Control & Manage 46
Figure 43: Control & Manage default page view 46
Figure 44: Outlet Naming, Time Delay, State on Startup or Reboot 48
Figure 45: Outlet Control 49
Figure 46: Outlet Control 50
Figure 47: Outlet Control menu item 51
Figure 48: Outlet Control enable/disable dialog 51
Figure 49: Control & Manage PDU 52
Figure 50: Edit Outlets 52
Figure 51: Sequence On-Delay Time 53
Figure 52: Saved Sequence 54
Figure 53: Reset All PDUs Energy menu item 54
Figure 54: Reset All PDUs Energy dialog 55
Figure 55: PDU Energy 55
Figure 56: PDU Energy Configuration 56
Figure 57: Outlet Energy 56
Figure 58: Multiple Outlet Energy Configuration dialog 57
Figure 59: Outlet Energy Configuration 58
Figure 60: Threshold Settings 59
Figure 61: Threshold Configuration 60
Figure 62: Power Threshold 60
Figure 63: Selecting between Primary and Linked PDUs 61
Figure 64: Phase Current Alarm 62
Figure 65: Phase Voltage Alarm 63
Figure 66: Load Segment Breaker 65
Figure 67: Outlet Information 67
Figure 68: Email Setup 69
Figure 69: Syslog Configuration 70
Figure 70: Syslog Mapping 71
Figure 71: Email Setup 72
Figure 72: SMTP Account Settings 73
Figure 73: Email Recipient 75
Figure 74: Event log 75

Figure 75: Event log Actions menu 76
Figure 76: Data Log 76
Figure 77: Data Log Configuration 77
Figure 78: Data Log Configuration Panel 77
Figure 79: User Accounts 79
Figure 80: RADIUS Configuration 80
Figure 81: User Accounts 81
Figure 82: TACACS+ Configuration 81
Figure 83: LDAP Configuration 83
Figure 84: Enable Role Privileges 84
Figure 85: Event Notifications 85
Figure 86: Wi-Fi Settings screen 86
Figure 87: Wi-Fi Radio Configuration 87
Figure 88: Wi-Fi Direct Connect Configuration 88
Figure 89: Wi-Fi Personal security Network configuration 89
Figure 90: Wi-Fi Enterprise security Network configuration 90
Figure 91: Wi-Fi Interface Configuration 91
Figure 92: SNMP Configuration 92
Figure 93: SNMP General 93
Figure 94: SNMP Port 93
Figure 95: Setup SNMP Port and Trap Port 94
Figure 96: Define SNMP V1/V2c User 95
Figure 97: Edit V1/2c Manager 95
Figure 98: SNMP v3 Manager 96
Figure 99: SNMP V3 Edit 97
Figure 100: SNMPv2c Trap Receiver Configuration Information 99
Figure 101: SNMPv3 Trap Server configuration Information. 100
Figure 102: Network Controller 102
Figure 103: Network Controller Menu Structure 103
Figure 104: Main Menu Selections 103
Figure 105: Alarms Menu 104
Figure 106: Power Menu 105
Figure 107: Device Submenu 105
Figure 108: Phase Submenu 106
Figure 109: Breaker Submenu 107
Figure 110: Outlet Submenu 108
Figure 111: Sensors 109
Figure 112: Setup Menu 110

Figure 113: Network Submenu 111
Figure 114: Screen Submenu 112
Figure 115: Language Submenu 113
Figure 116: Units Submenu 115
Figure 117: USB Enable 115
Figure 118: USB Submenu 117
Figure 119: Network Menu 118
Figure 120: Info Menu 119
Figure 121: Help & Support 120
Figure 122: Example Search Box 122
Figure 123: System Management 123
Figure 124: Linked Configuration 124
Figure 125: Connection Diagram 6 PDU Daisy Chain 125
Figure 126: Bridge Mode Daisy Chain with Redundancy and Power Share 128
Figure 127: Sensor Ports 131
Figure 128: User Accounts 132
Figure 129: Temperature Units Setting 132
Figure 130: Environmental Sensor Threshold Configuration View 133
Figure 131: Temperature Sensor Edit dialog 133
Figure 132: Security Sensor Alarm Configuration view 134
Figure 133: Dry Contact Sensor Edit dialog 135
Figure 134: Connection Diagram 136
Figure 135: Security Handles 137
Figure 136: Rack Access Control 138
Figure 137: Rack Access Control Actions 138
Figure 138: Event Log 139
Figure 139: Add Card 140
Figure 140: Add Card (Temporary User) 141
Figure 141: Add Card with Card Aisle 142
Figure 142: Edit Card 142
Figure 143: Edit Card (Temporary User) 143
Figure 144: Add Card with Card Aisle 144
Figure 145: Rack Access Settings 145
Figure 146: Handle Settings 146
Figure 147: Keypad Settings 147
Figure 148: Remote Control 148
Figure 149: Beacon 149
Figure 150: Beacon Settings 150

Figure 151: Status LED 151
Figure 152: Status LED Settings 152
Figure 153: SSL Certificate Load Screen 166
Figure 154: Upload 173
Figure 155: Auto Update 174
Figure 156: Auto Update Configuration 175
Figure 157: User Accounts from the User Icon 177
Figure 158:User Accounts from Gear Icon 177
Figure 159: Users Table 178
Figure 160: Edit User Screen 179
Figure 161: View network Connections 180
Figure 162: Properties 180
Figure 163: Ethernet Properties 181
Figure 164: Internet Protocol Version 4 181
Figure 165: Reading from CLI 185
Figure 166: Writing from CLI 185
Figure 167: Windows DHCP Config 196
Figure 168: SZTP License 197
Figure 169: Install Folder 198
Figure 170: Start Menu Location 198
Figure 171: Installation Review 199
Figure 172: Bootstrap Server Configuration 200
Figure 173: Post Install Options 201
Figure 174: Configuration Download 202
Figure 175: Windows Event Viewer 203
Figure 176: SZTP Event Examples 204
Figure 177: Example Admin User for Collector PDU 206
Figure 178: Onboard Data Collector Configuration for Collector PDU 207
Figure 179: Example Viewer User for Device PDU 208
Figure 180: Onboard Data Collector Configuration for Device PDU 209
Figure 181: Cisco Nexus Dashboard Integrations 210
Figure 182: Cisco Nexus Dashboard Panduit PDU Integration 210
Figure 183: Registering Collector PDU to Cisco Nexus Dashboard 210
Figure 184: Selecting Fabric 211
Figure 185: Registered Collector PDU 211
Figure 186: Example Credentials for Device PDU 212
Figure 187: Cisco Nexus Dashboard to Onboard Data Collector Communication 214
Figure 188: Register Device Communication 214

Figure 189: Onboard Data Collector Communication when Polling 215
Figure 190: SiteCommand Utility..... 216

AI Ready Documentation

AI-Ready User Manual

This user manual has been specially prepared to be AI-ready. The structure, terminology, and organization are optimized so it can be directly provided to your AI tool of choice. (*For Example: Microsoft Co-Pilot®, Open AI ChatGPT®, Google Gemini® or Grok®*).

By supplying this manual as input, you can immediately begin prompting the AI to:

- Ask configuration, operation, or troubleshooting questions
- Retrieve step-by-step guidance from the manual
- Get contextual explanations based on EL2P features and behavior

This enables faster access to information, reduces time spent searching, and supports a more interactive support and learning experience.

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

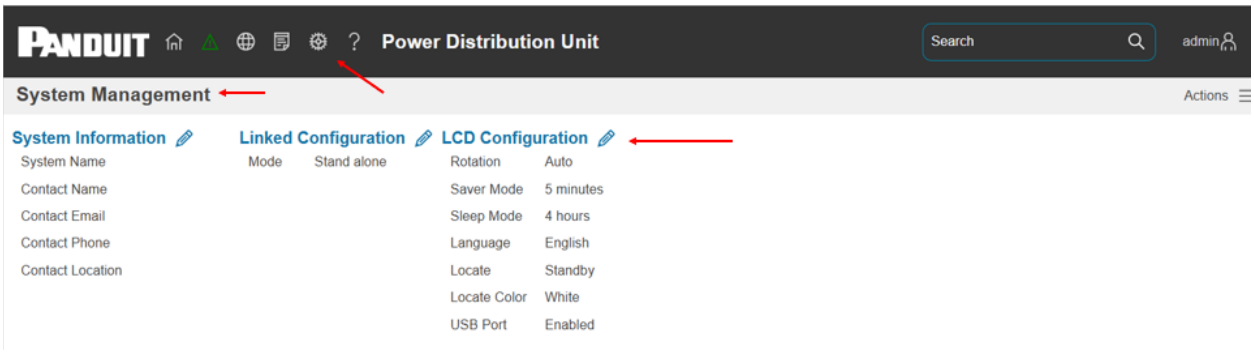


Figure 1: LCD Configuration

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

   Note: By default, wireless access is only available for 10 minutes after pressing the “Start On Demand” button on the LCD screen under “Network” -> “Wi-Fi AP”. 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

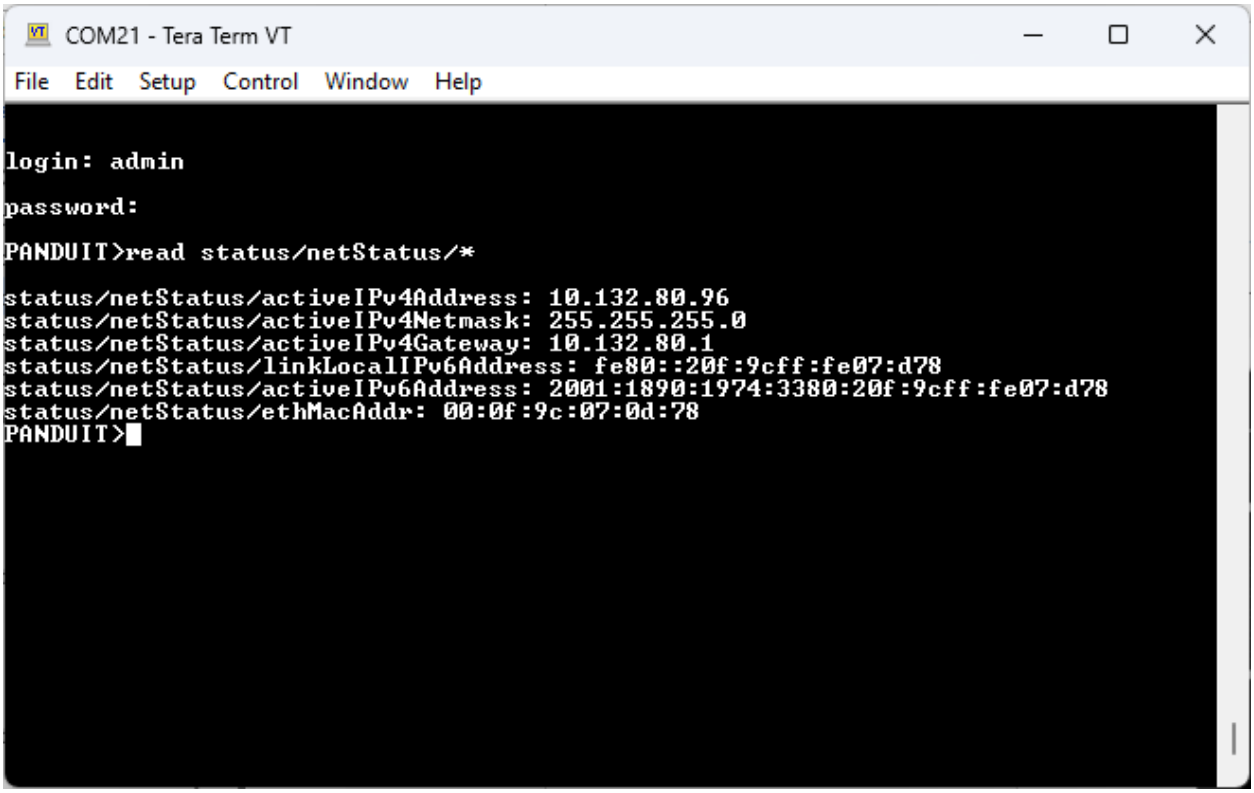


Figure 4: Network information from +

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://”

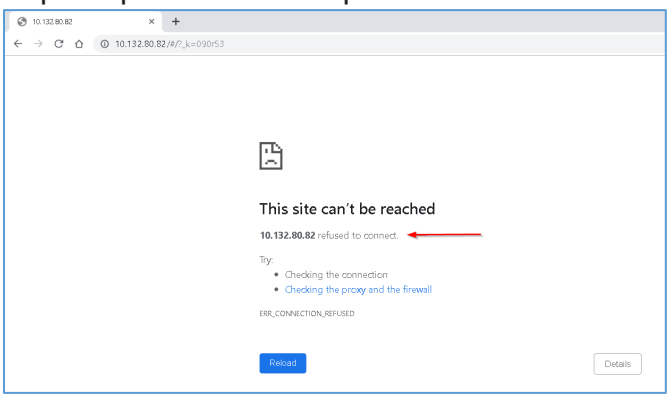


Figure 5: Refused Connection Example

- 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.

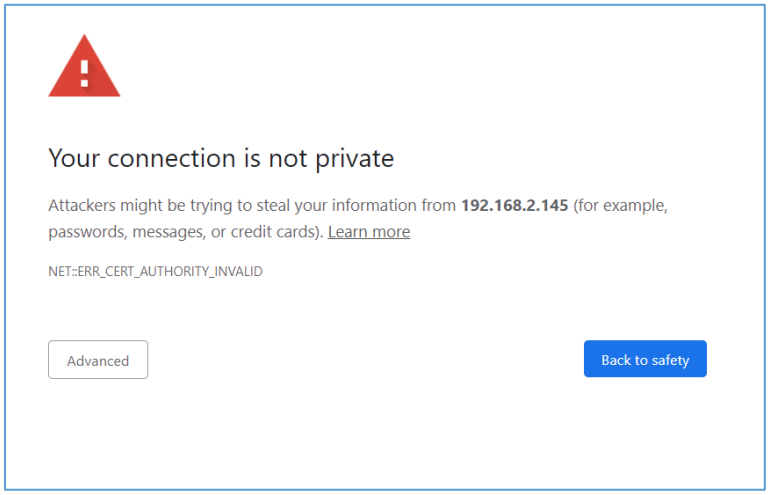


Figure 6: Certificate Warning

- 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.

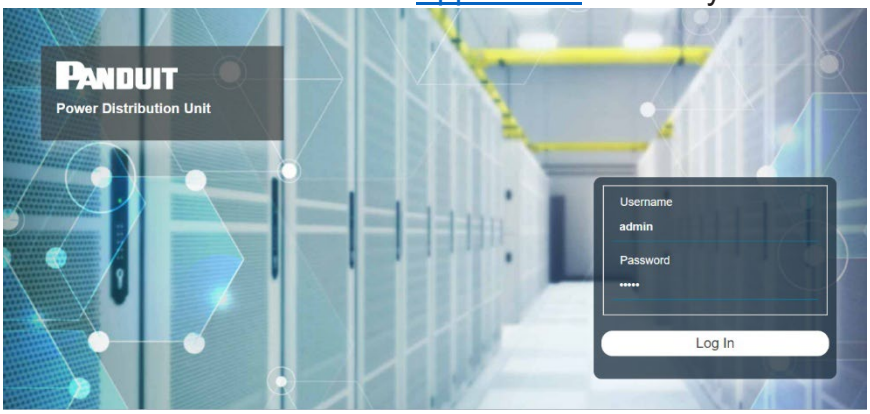


Figure 7: Login Page

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**.

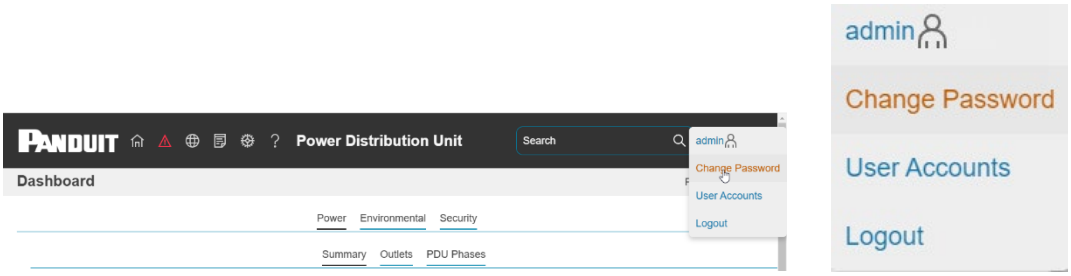


Figure 8: After Login

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

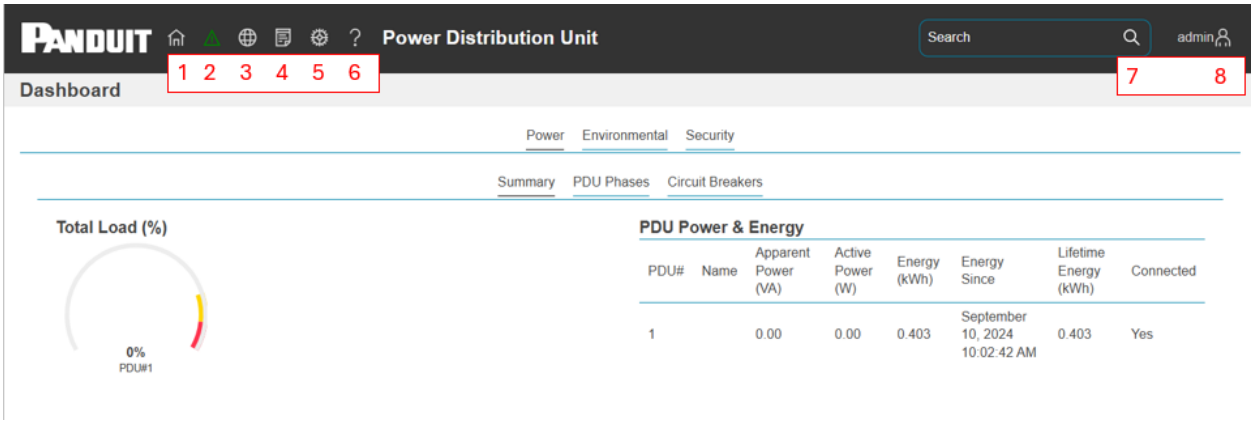
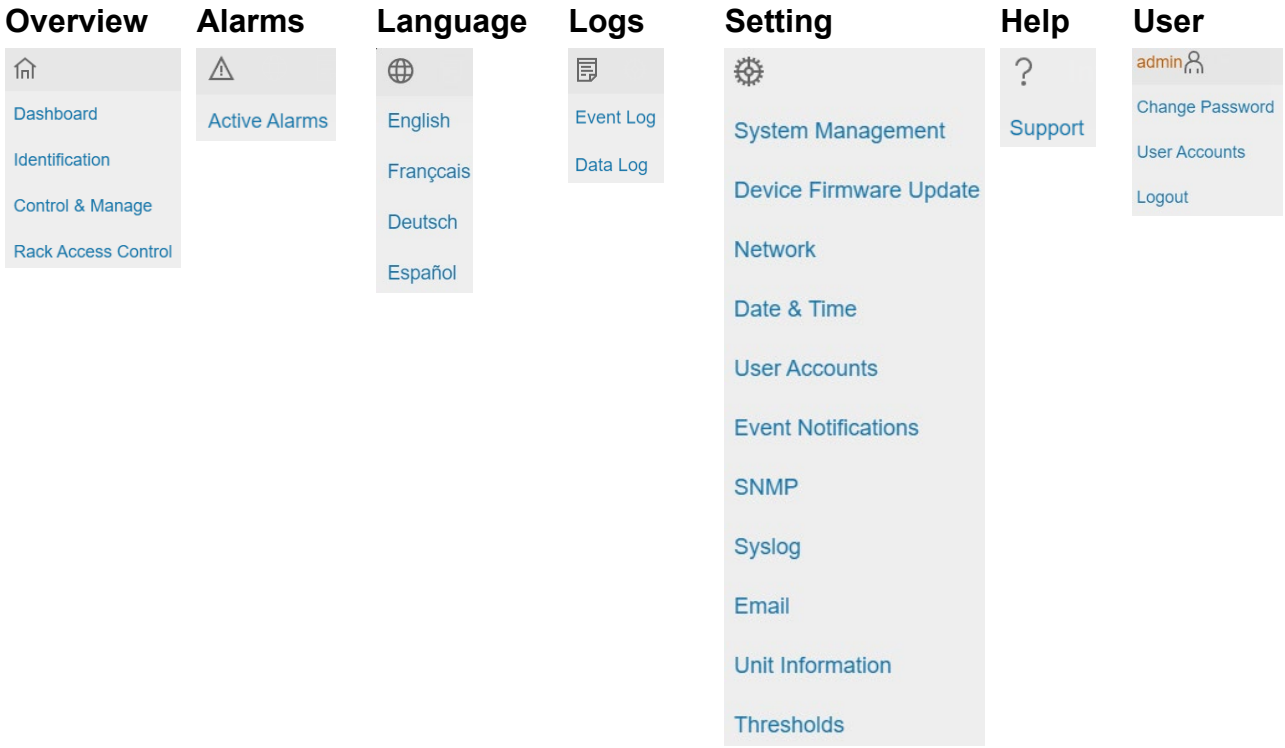


Figure 9: Landing Page/Dashboard

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

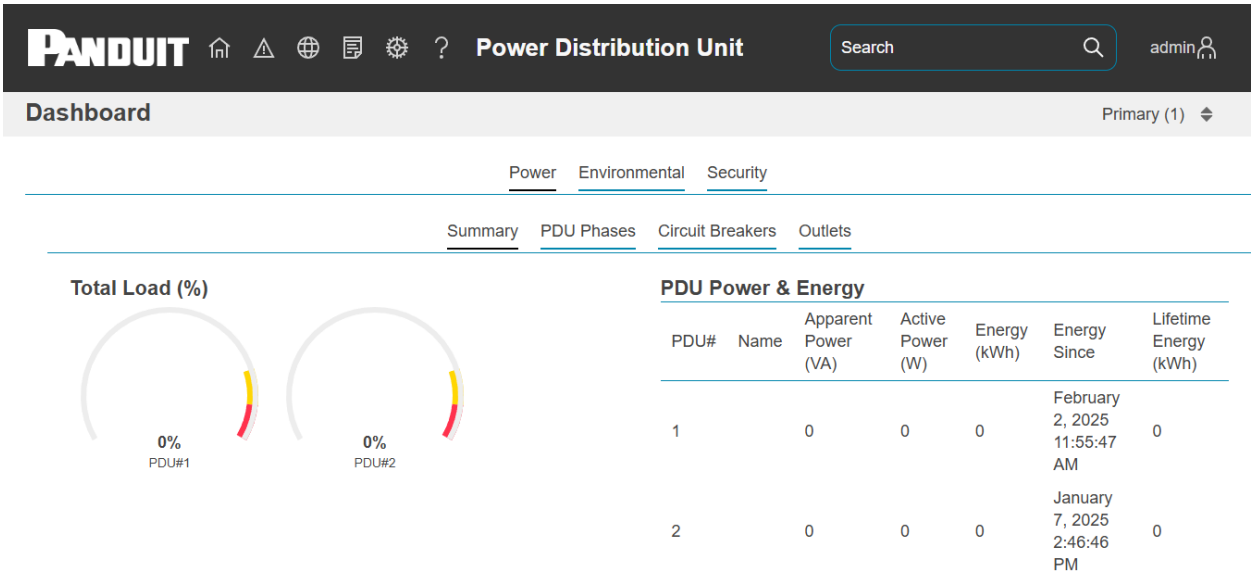


Figure 10: Power Summary Page

Power Outlets Page

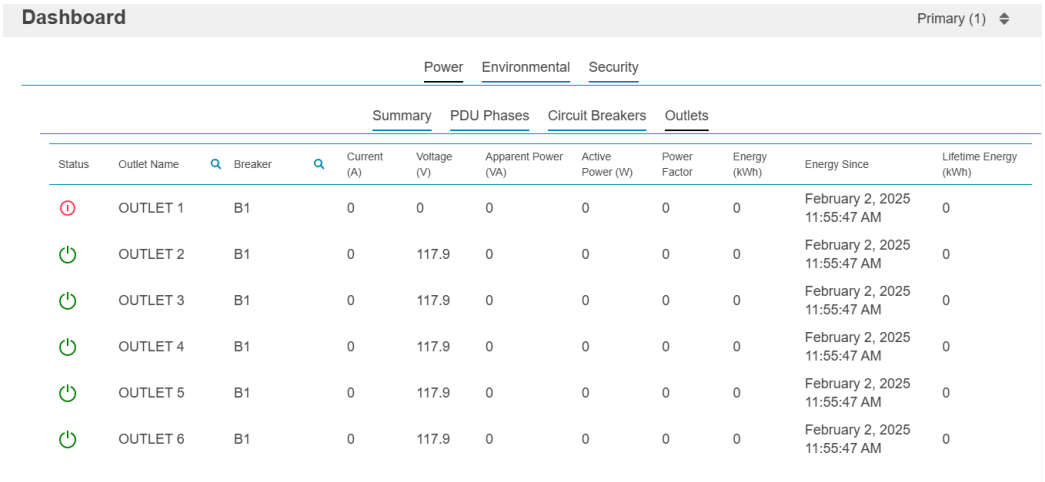


Figure 11: Power Outlets Page

Environmental Monitoring Page

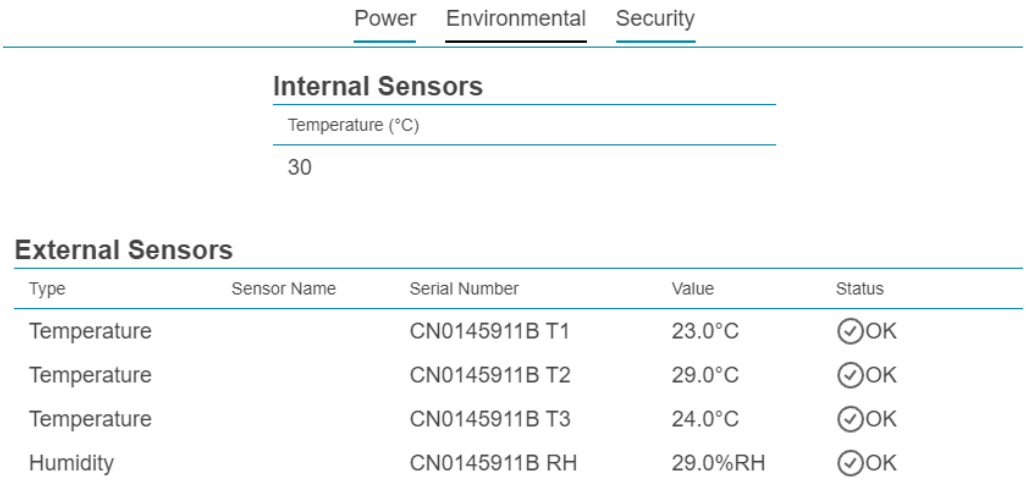


Figure 12: Environmental Monitoring Page

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

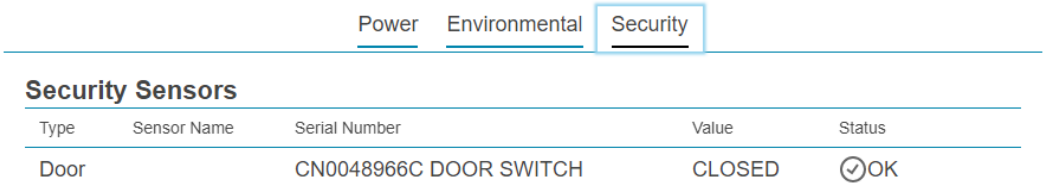


Figure 13: Security Monitoring Page

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

System Management

System management includes configuration of system information used to identify the PDU inside the data center as well as other system configuration options and actions.

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

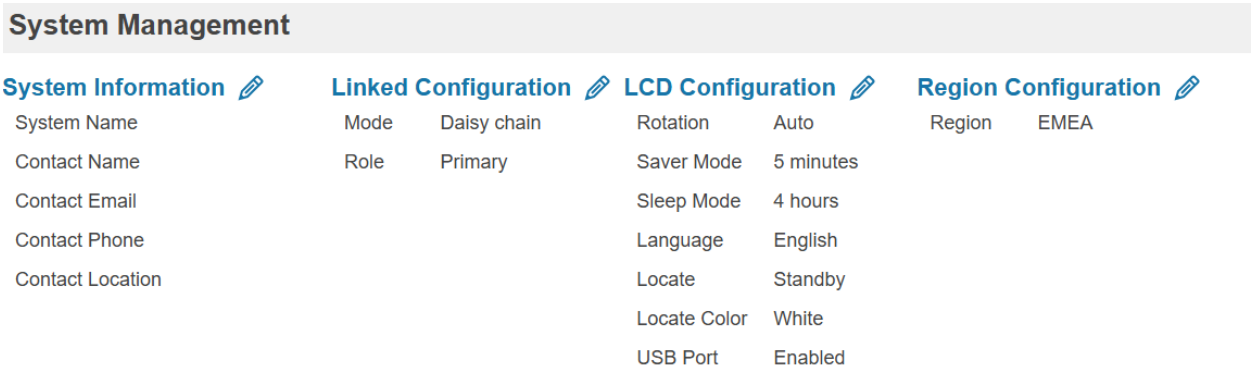


Figure 14: System Management

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.**

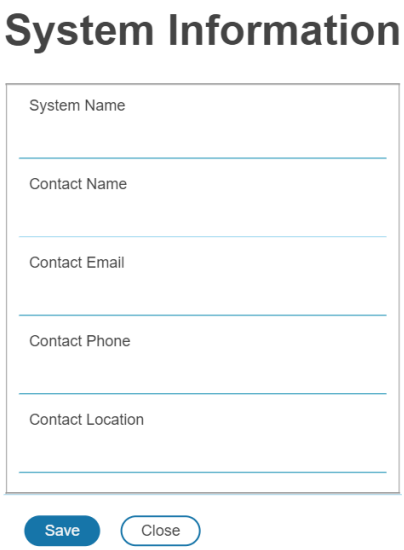


Figure 15: System Information Configuration

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**.

Linked Configuration

The Linked Configuration submenu is used to enable a PDU Daisy Chain, see Section 5 – Daisy Chain Configuration for more information.

LCD Configuration

The LCD Configuration allows customization of LCD settings.

1. System Management → LCD Configuration

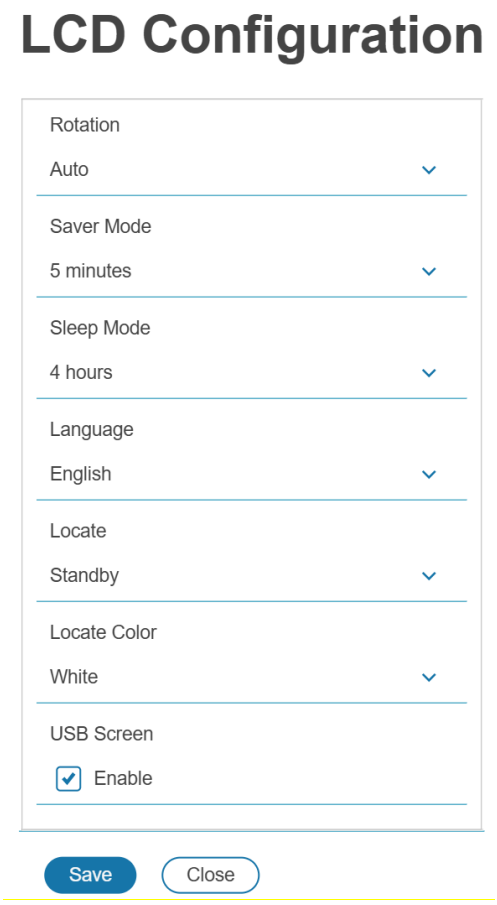


Figure 16: LCD Configuration

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.

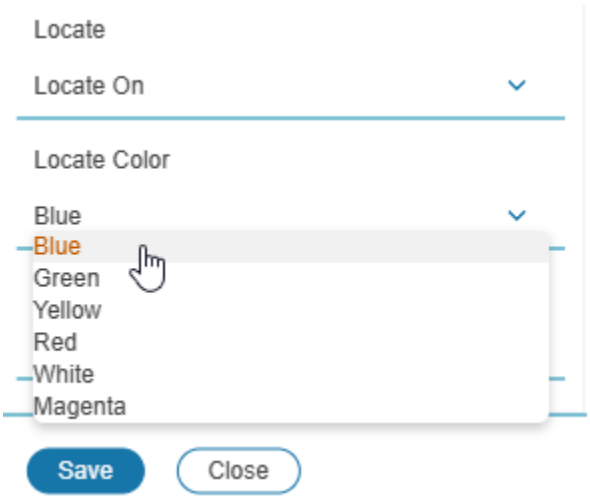


Figure 17: PDU Locate

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.

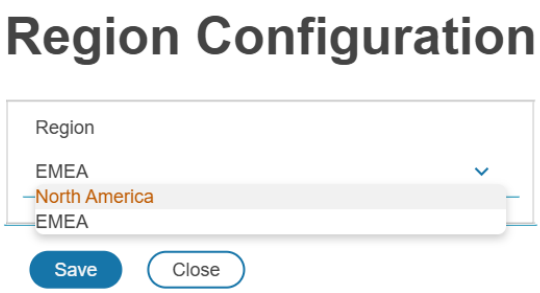


Figure 18: PDU Region

3. Press Save.

System Management Actions

System management includes an action menu at the top right of the screen. It provides options for bulk configuration, defaulting and restarting the PDU.

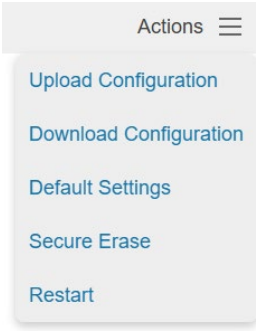


Figure 19: System Management Actions

Bulk Configuration

Download configuration provides a method to back up a PDU configuration. When clicked, the download configuration action will automatically download a config.json file.

Upload configuration restores the configuration from a previously downloaded config.json. Upload may be used to restore the configuration on the original device, or a PDU with the same part number.

Note: Device unique network configuration settings such as static IP are not included in the config.json to prevent network collisions.

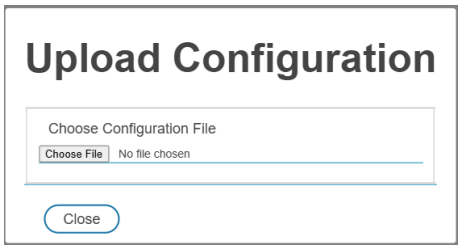


Figure 20: Upload Configuration

Default Settings

Default Settings will perform a quick erase of all settings and logs and reboot the PDU. Energy data is not erased.

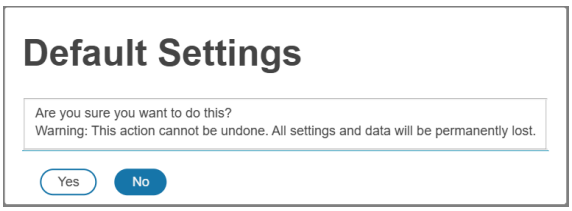


Figure 21: Default Settings Warning

Secure Erase

Secure Erase performs a complete and irreversible erasure of all user data stored on the PDU. Compared to default erase settings, a secure erase will take longer—potentially tens of minutes—depending on the condition and state of the internal flash memory.

Once the process is complete, the PDU will automatically reboot and display “Secure Erase Complete” on the LCD.

Secure erase enables the PDU to be securely redeployed, resold, or reused by ensuring all prior configuration and user data has been removed, supporting responsible asset reuse and extended product lifecycle (“second-life”) initiatives.

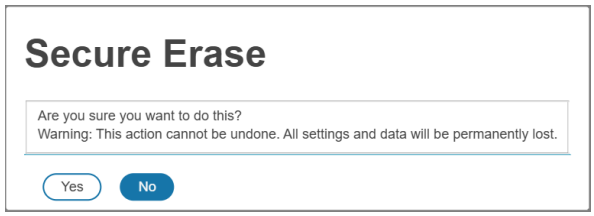


Figure 23: Secure Erase Warning

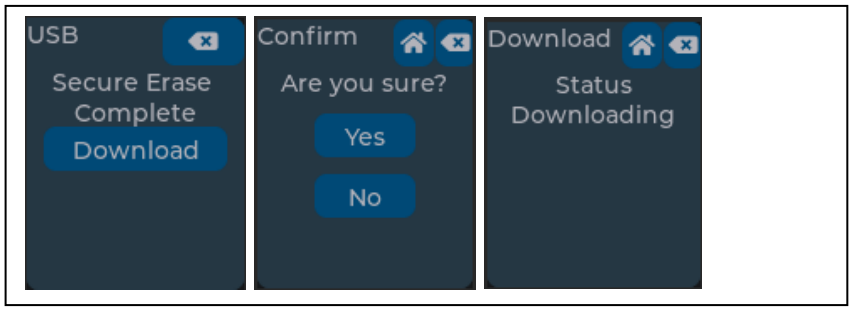


Figure 22: Secure Erase Complete

Restart

Restart will perform a warm reboot of the PDU. In general, it should be unnecessary as all network configuration changes take effect immediately.

Figure 24: Restart Warning

Network Settings

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

Ethernet Interface Configuration:

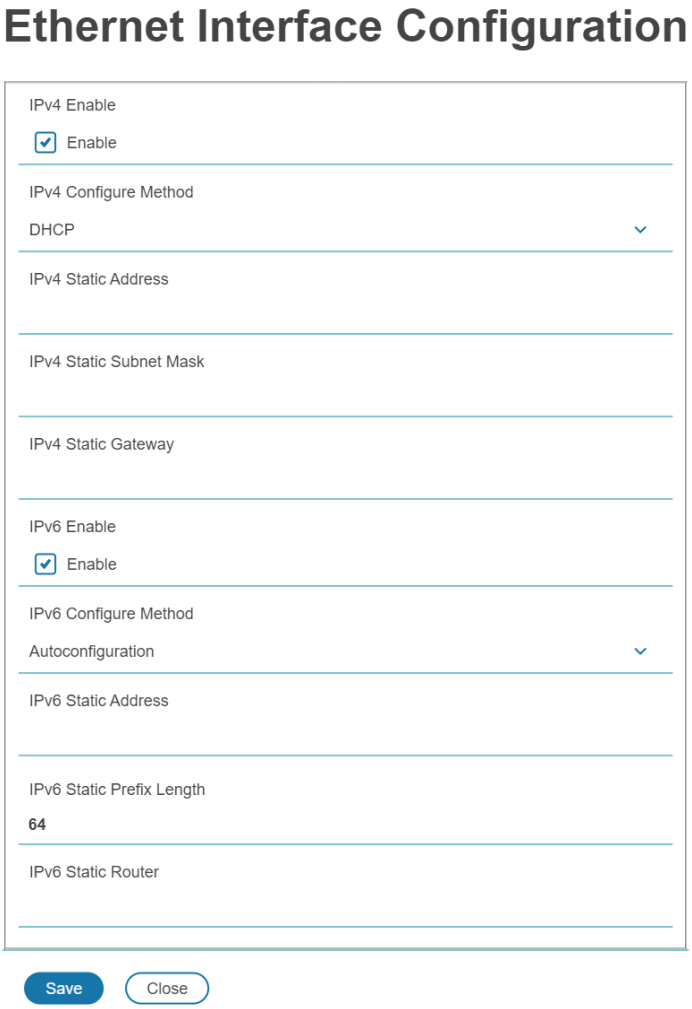


Figure 25: Ethernet Interface Configuration

DNS configuration:

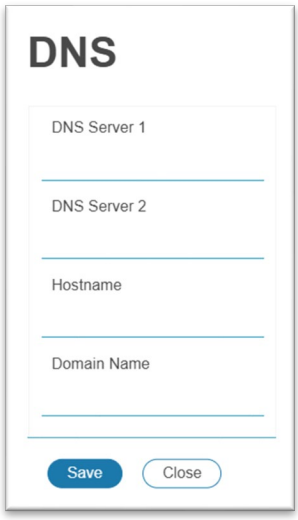


Figure 26: DNS Configuration

Web Access Configuration

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

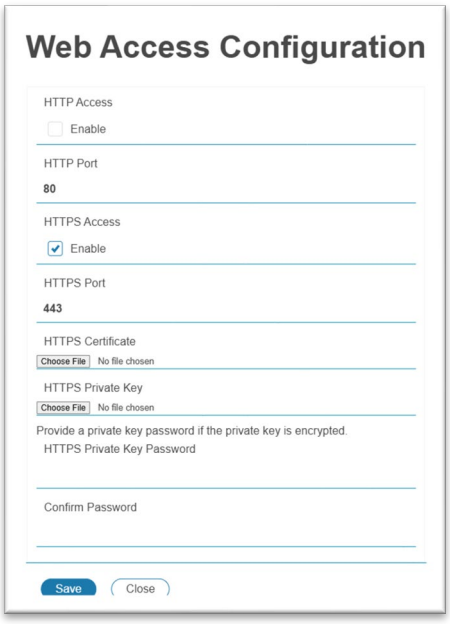


Figure 27: Web Access Configuration

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.

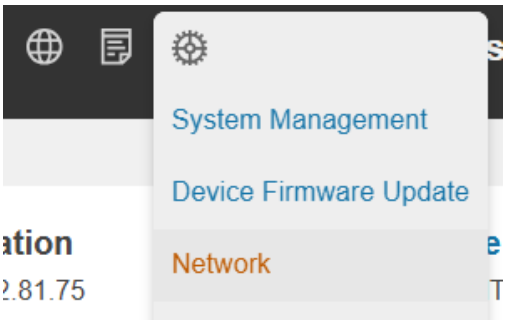


Figure 28: Network Settings

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

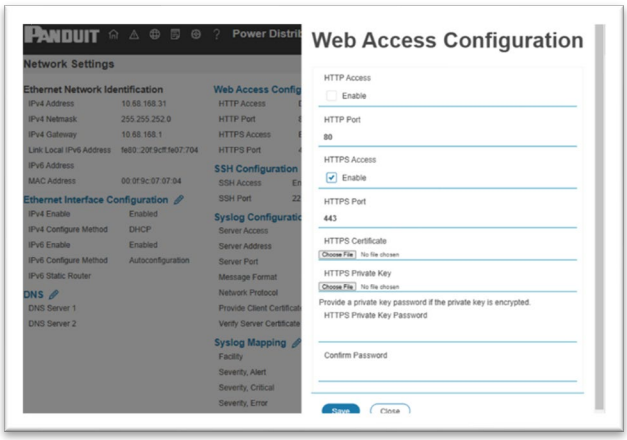


Figure 29: Web Access Configuration

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

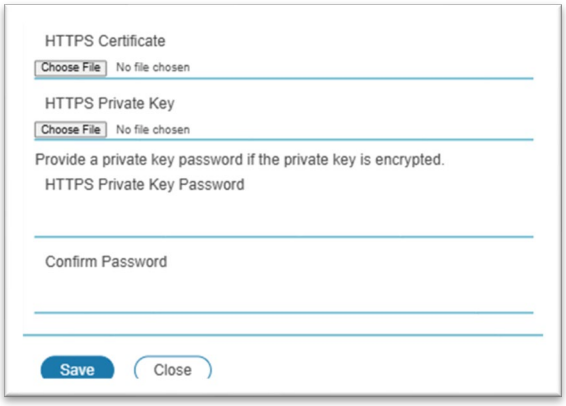


Figure 30: Upload Certificates

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:

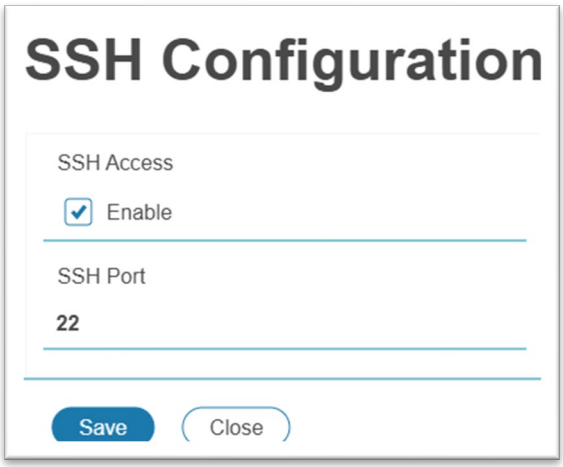


Figure 31: SSH Configuration

IEEE 802.1X Configuration:

IEEE 802.1X is a network access control standard that authenticates devices before they are allowed onto a wired or wireless network.

IEEE 802.1X acts as a gatekeeper, ensuring that only authorized devices can communicate on the network.

IEEE 802.1X uses a client–server model involving three components:

Component	Role
Supplicant	The device requesting network access (EL2P in this case)
Authenticator	The network switch or access point controlling access
Authentication Server	Typically, a RADIUS server validating credentials

When 802.1X is enabled, the EL2P must authenticate (username/password or certificate) before its Ethernet port becomes active.

Organizations often enable 802.1X to:

Enhance Security

Prevents unauthorized devices from joining the network — a critical requirement in government, healthcare, finance, and regulated industries.

Meet Compliance Requirements

Standards such as PCI-DSS, ISO 27001, and NIST guidelines often require controlled network access.

Reduce Attack Surfaces

Blocks rogue devices, unauthorized laptops, or compromised IoT equipment from connecting.

Ensure Device Identity

Each device must authenticate, ensuring traceability and accountability.

When connected to a switch port configured for 802.1X The EL2P sends an EAPOL (EAP over LAN) request to start authentication.

The switch relays credentials to a RADIUS authentication server.

If credentials are valid, the switch opens the port for normal IP traffic.

If not, the device is blocked or placed in a restricted VLAN (if configured).

Configuration Fields Explained:

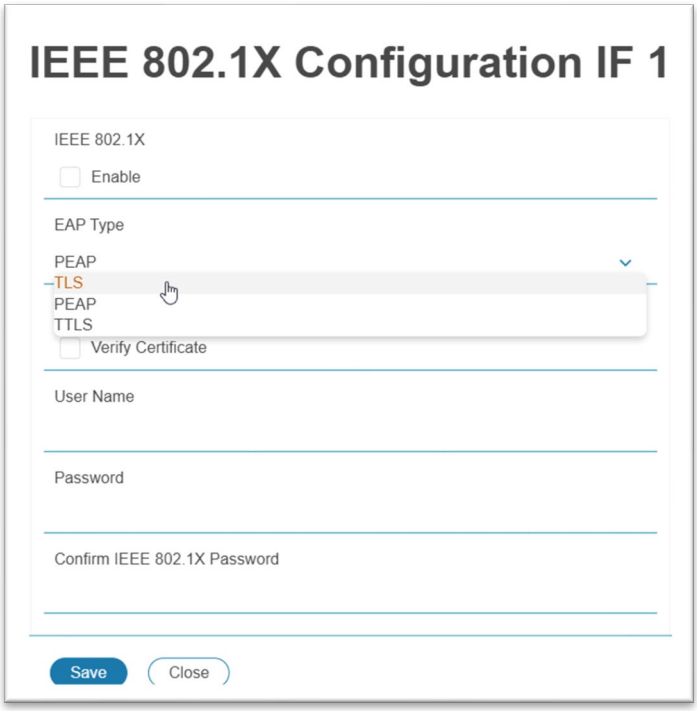


Figure 32: IEEE 802.1X Configuration

Enable: Turns 802.1X authentication on for the interface.

EAP Type (Extensible Authentication Protocol):

- PEAP (Protected EAP) – Username/password in a secure TLS tunnel (most common)
- EAP-TLS – Certificate-based authentication (strongest security)

- EAP-TTLS – Similar to PEAP but more flexible

Verify Certificate

If enabled, the EL2P will verify the identity of the RADIUS server using its certificate.

Enable this when:

- Using trusted commercial or internal PKI certificates
- You want maximum protection from spoofed authentication servers

When Verify Certificate is enabled, additional settings are visible in the dialog:

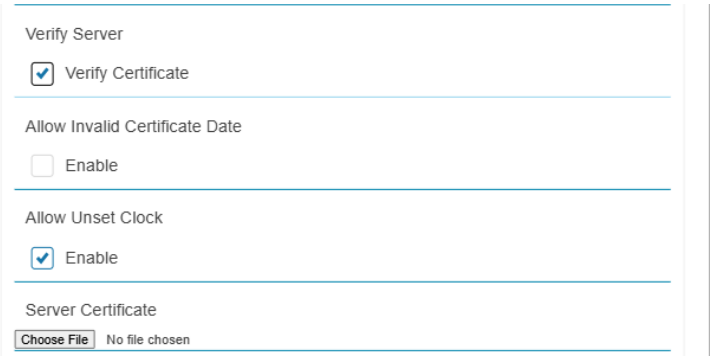


Figure 33: IEEE 802.1X Verification Options

Allow Invalid Certificate Date: Allows server certificates that are expired.

Allow Unset Clock: Prevents an unset clock from causing a validation fail, the EL2P RTC has a short uptime, it is recommended to leave this set.

Server Certificate: Upload a self-signed certificate or a certificate chain for the authentication server.

User Name: The 802.1X identity used for authentication on the RADIUS server.

Password / Confirm Password: Shared secret used for PEAP authentication.

Configuring IEEE 802.1X on the EL2P

IEEE 802.1X Implementation on EL2P

Prerequisites

Before enabling IEEE 802.1X on the EL2P, ensure that the connected network infrastructure supports 802.1X authentication. This includes a switch port configured for 802.1X operation and a RADIUS authentication server with valid credentials or certificates assigned for the EL2P device.

To enable authentication on the EL2P:

- Open the IEEE 802.1X Configuration screen for the appropriate interface.
- Select Enable to turn on 802.1X functionality.
- Choose the required EAP Type (for example, PEAP).
- Enable Verify Certificate if certificate validation is required by your network.
- Enter the assigned User Name.
- Enter the associated Password, then re-enter it in Confirm IEEE 802.1X Password.
- Select Save to apply the settings.

The device will attempt to authenticate immediately after saving.

Network-Side Requirements

Successful operation requires proper configuration on the network side. Ensure the switch port is operating in 802.1X mode and that the RADIUS server contains an authentication policy permitting the EL2P device to connect using the provided credentials. If certificate validation is used, any necessary certificates must be correctly installed on both the RADIUS server and the EL2P.

Verification

After configuration, verify successful authentication by checking logs on the RADIUS server or by reviewing the authentication status of the switch port. Once authenticated, the EL2P is granted normal network access.

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.

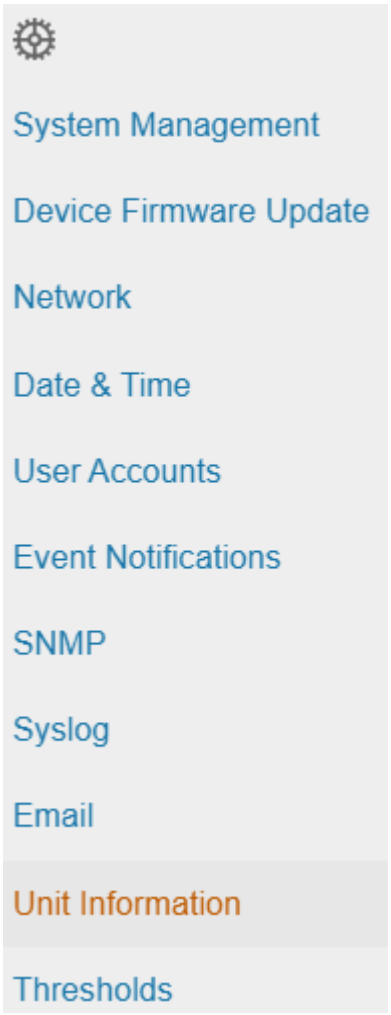
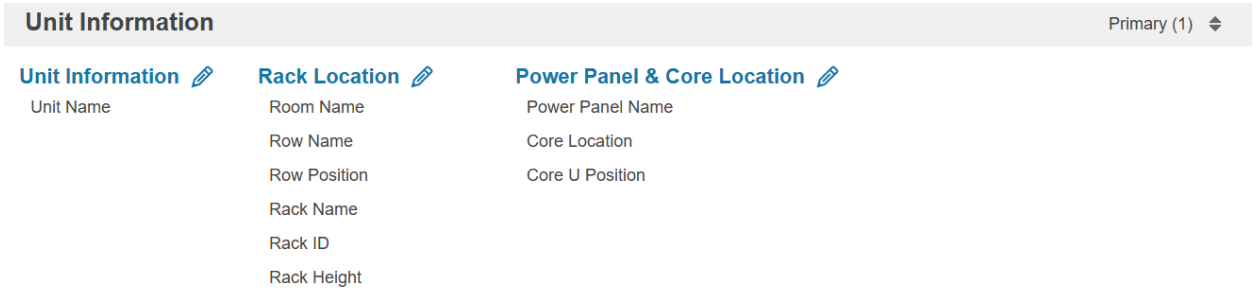


Figure 34: Unit Information

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.**

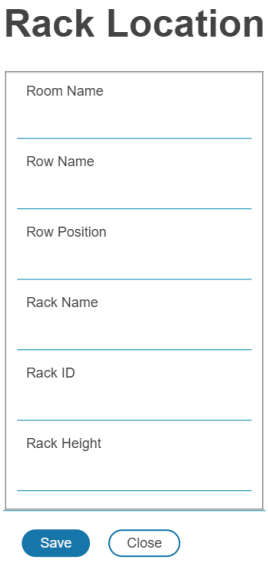


Figure 35: Rack Location Configuration

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**.

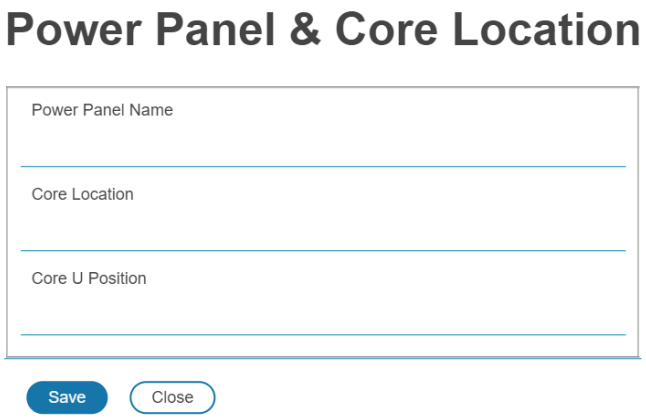


Figure 36: Power Panel & Core Location

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**.

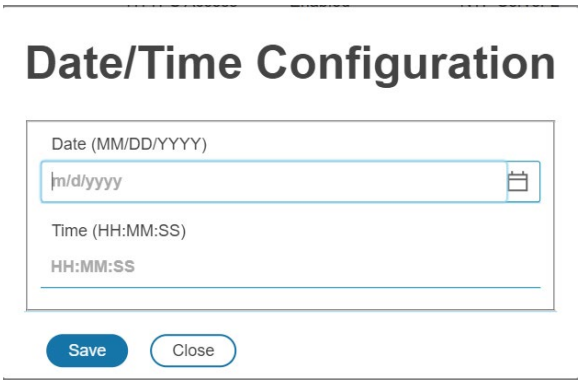


Figure 37: Setting the Date and Time

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).

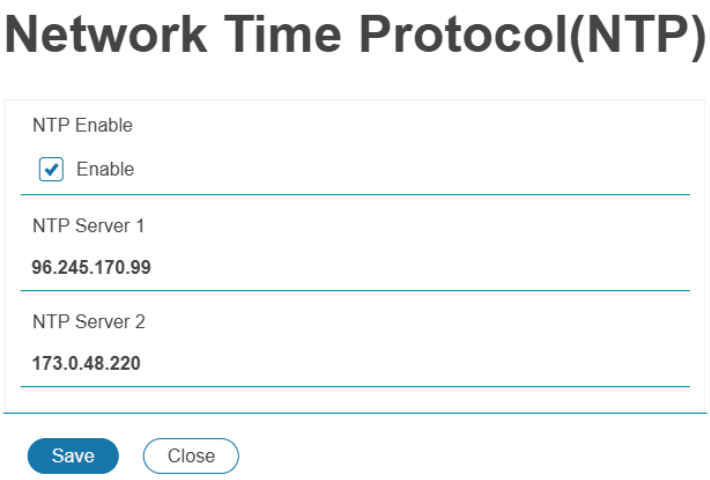


Figure 38: NTP Configuration

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**.

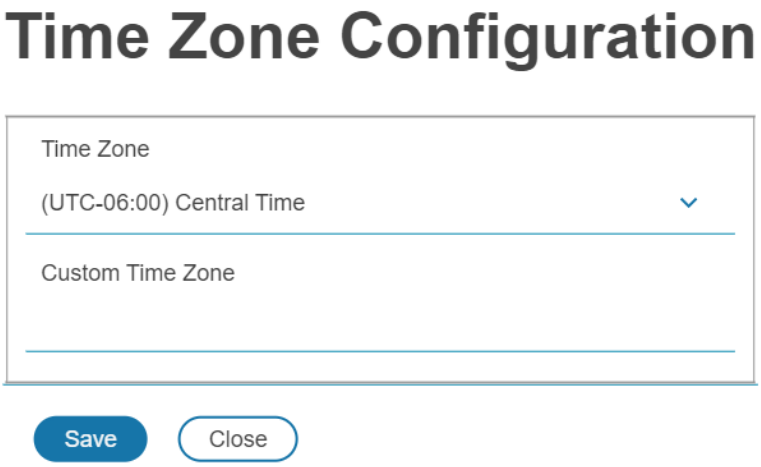


Figure 39: Daylight Saving Time Zone Configuration

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

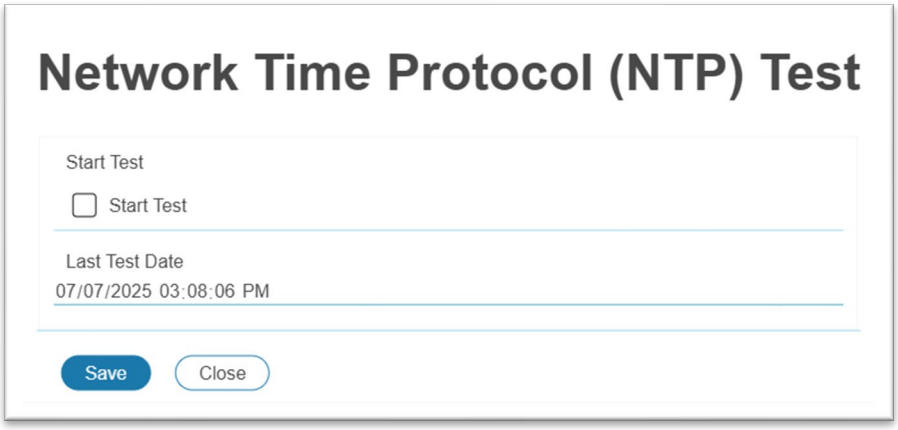


Figure 40: Starting NTP Test

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

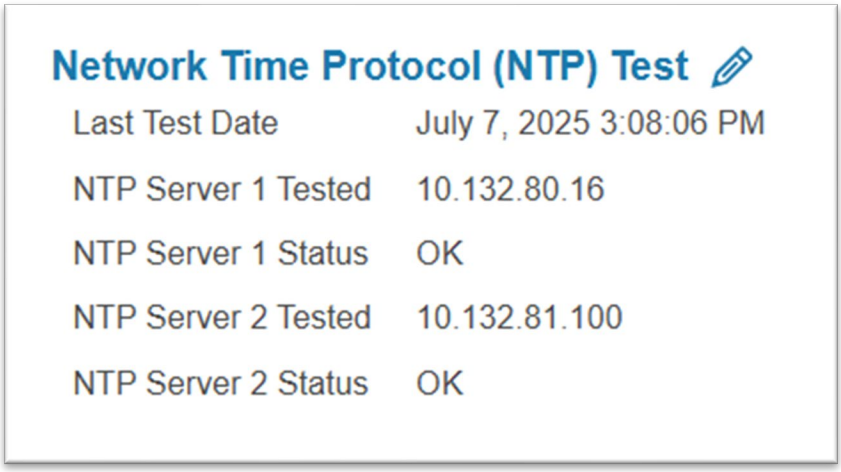


Figure 41: Status of NTP Test

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.

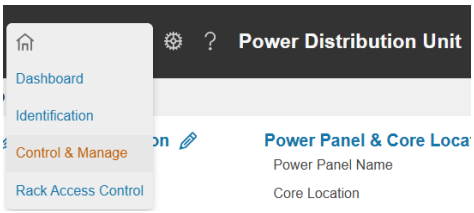


Figure 42: Control & Manage

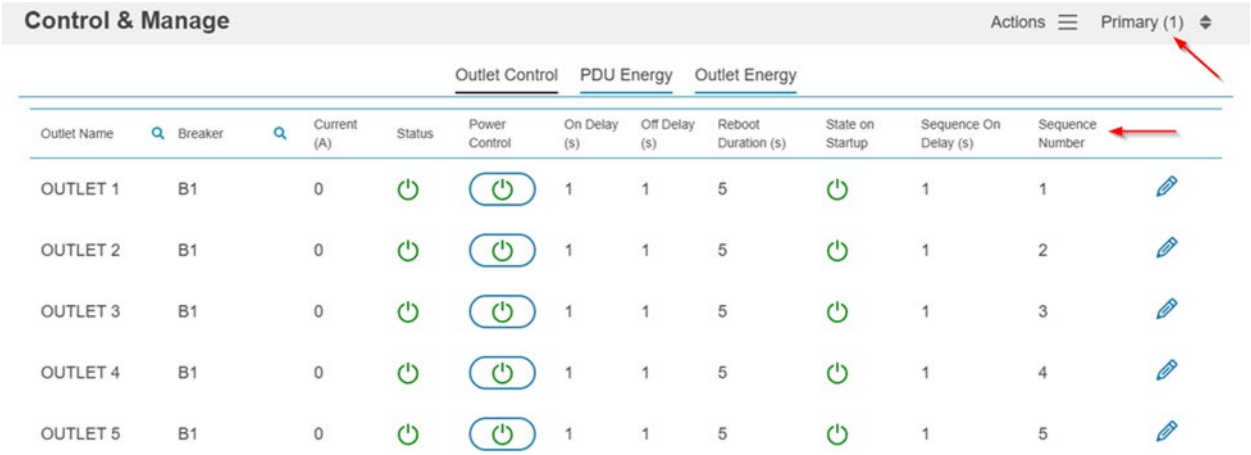


Figure 43: Control & Manage default page view

Outlet Power Management

Outlet LED

The Outlet LED indicates the status of the relay's DC coil on the internal PCB—not the presence of AC power at the outlet. When the LED is ON (green), it means the relay coil is energized and the control circuitry (PDU power supply and firmware command path) is healthy and actively commanding the outlet ON. When the LED is OFF, the relay coil is de-energized and the outlet is being commanded OFF.

Important: if a circuit breaker trips (manually or due to overload), the Outlet LED may remain ON because the relay coil still has DC power; in this case, the LED confirms control-path health and command state, not downstream line voltage. This design ensures a firmware fault cannot mistakenly shut off outlets by falsely sensing a breaker event—preventing unintended service interruptions.

What the LED is informing (plain language):

- Control state: Whether the PDU is commanding the outlet ON (coil energized) or OFF (coil de-energized).

- Control-path health: That the PDU's low-voltage DC power supply and relay driver are working.
- What it is not informing: It does not guarantee AC power is present at the outlet receptacle (e.g., a tripped breaker or upstream power loss can leave the outlet unpowered while the LED is still ON).

Outlet Status

For Panduit PDUs with outlet level control the **Status** of the outlet on the Web interface 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**.

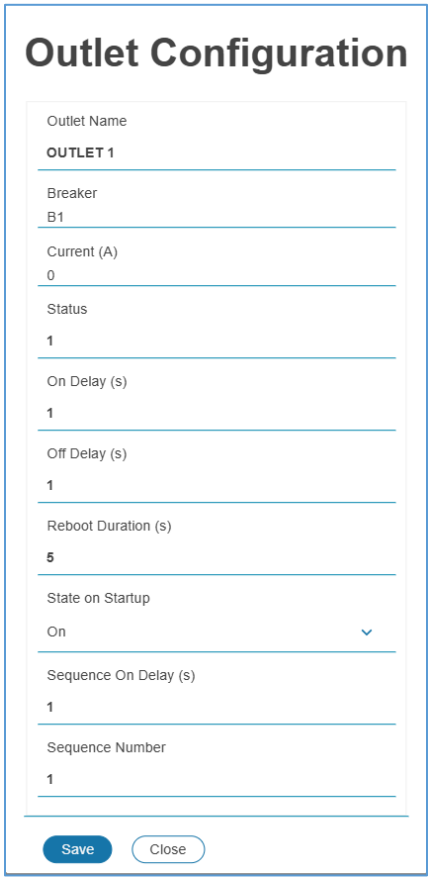


Figure 44: Outlet Naming, Time Delay, State on Startup or Reboot

*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.

- When the PDU breaker for an outlet is turned off or the NMC is in Power Share, the Outlet Name and Breaker text are show in colored gray and strike-through style to indicate the outlet is not active.

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.

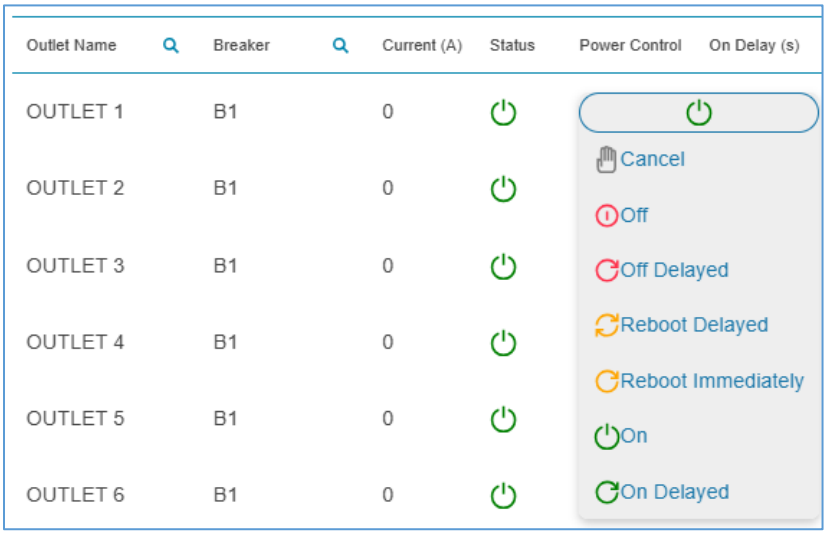


Figure 45: Outlet Control

4. A confirmation dialog is displayed.

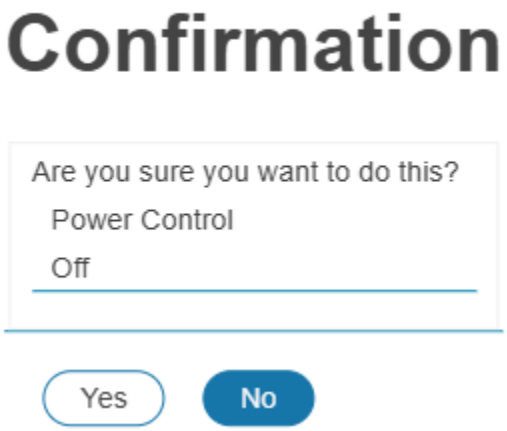


Figure 46: Outlet Control

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.

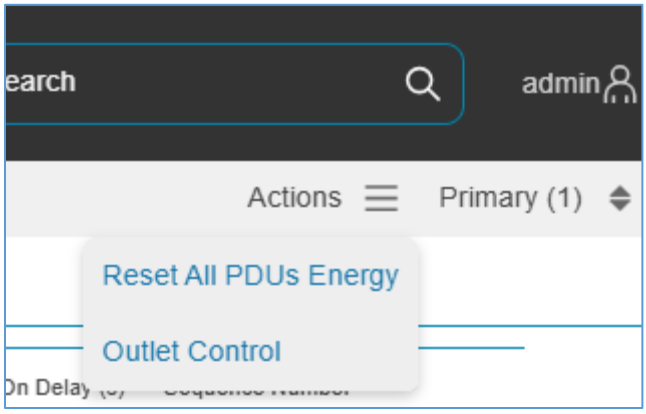


Figure 47: Outlet Control menu item

3. Select the Outlet Control Enabled/Disabled state.

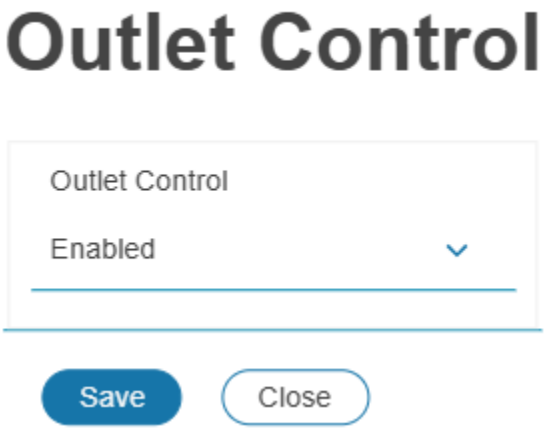


Figure 48: Outlet Control enable/disable dialog

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**.

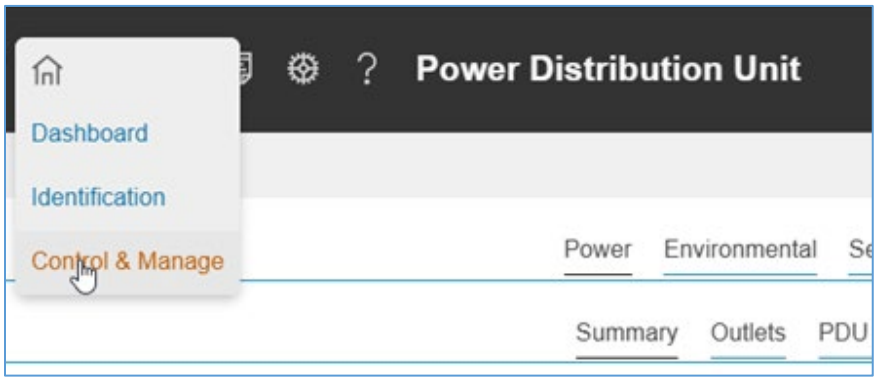


Figure 49: Control & Manage PDU

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

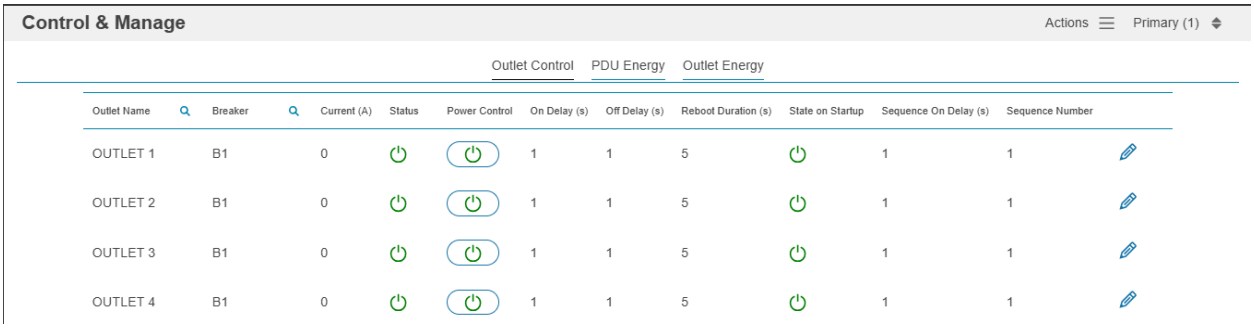


Figure 50: Edit Outlets

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.

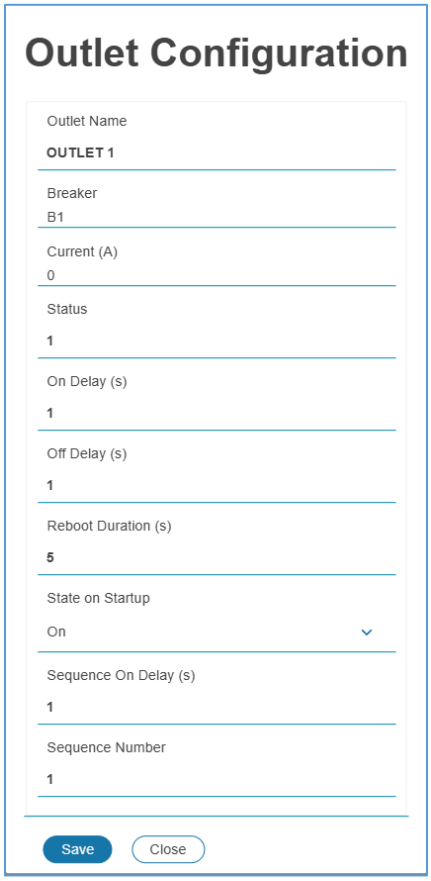


Figure 51: Sequence On-Delay Time

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.

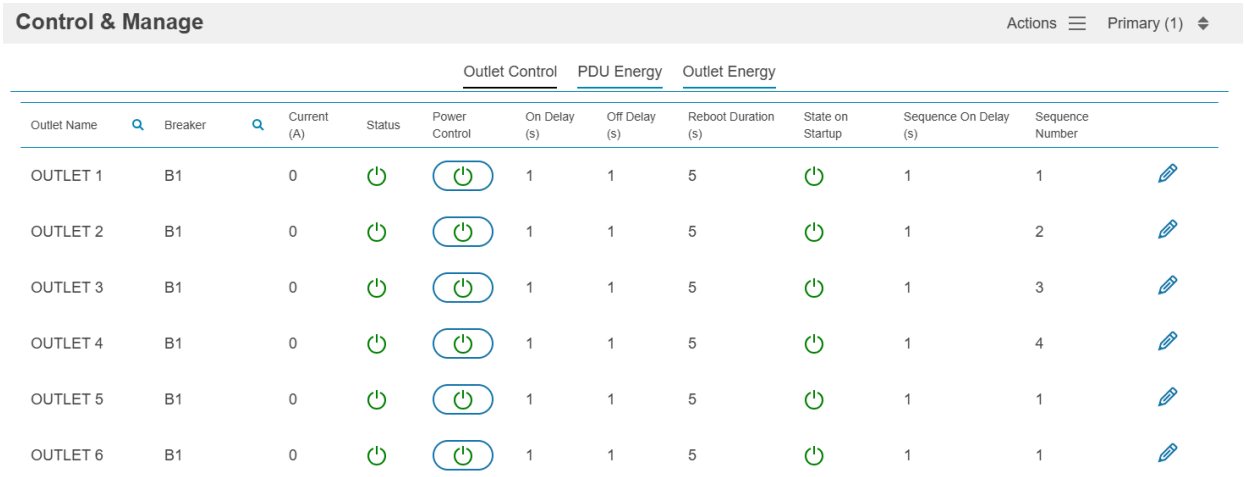


Figure 52: Saved Sequence

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.

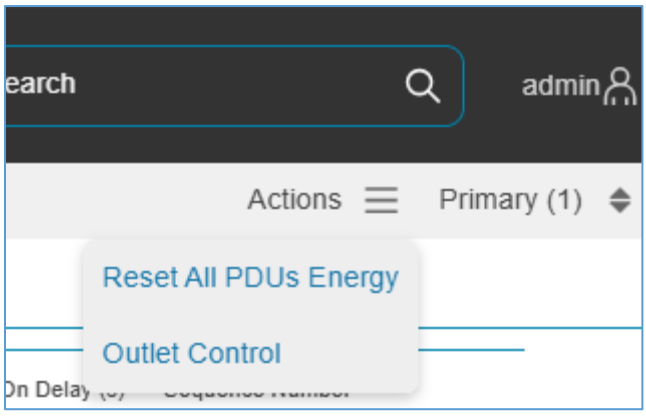


Figure 53: Reset All PDUs Energy menu item

3. Select Yes to reset all PDUs Energy.

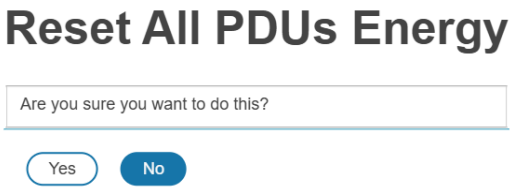


Figure 54: Reset All PDUs Energy dialog

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.

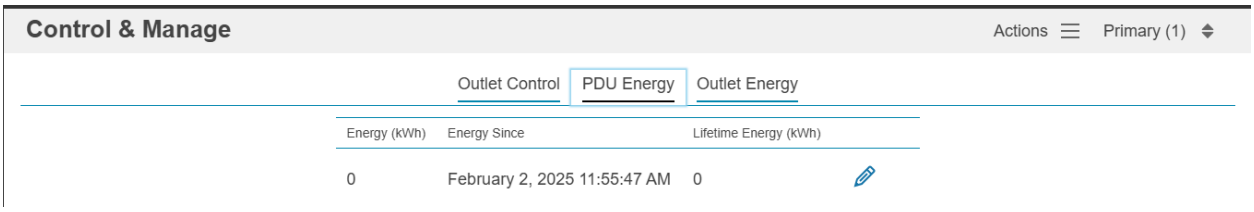


Figure 55: PDU Energy

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.

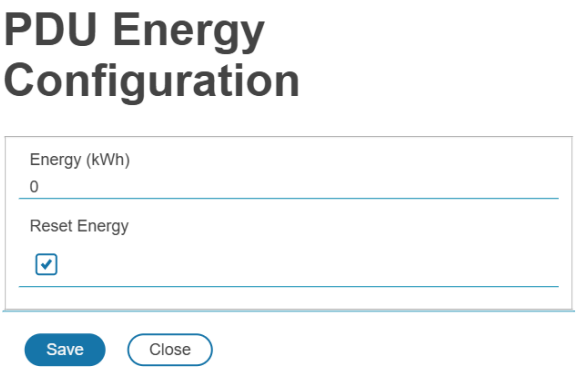


Figure 56: PDU Energy Configuration

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.

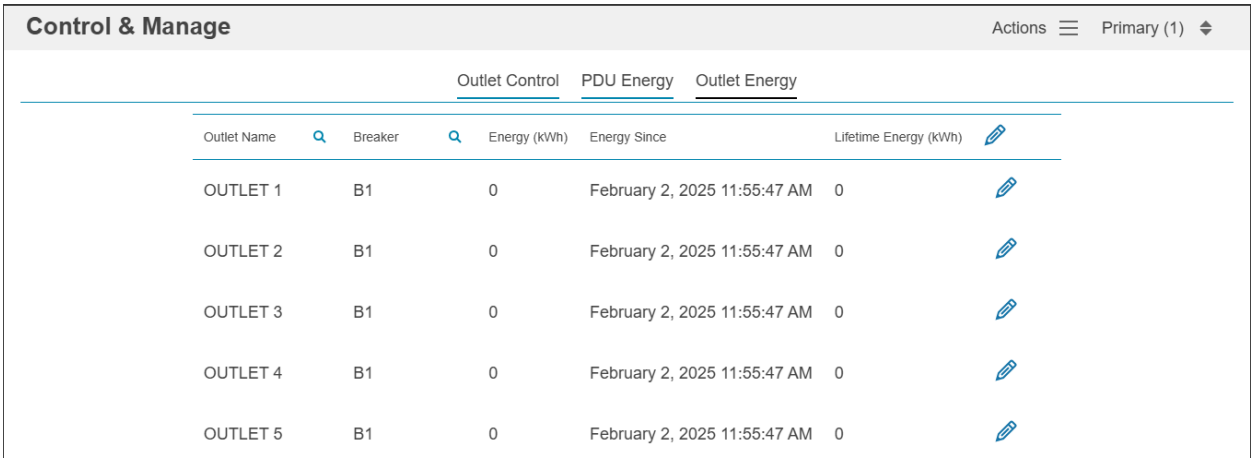


Figure 57: Outlet Energy

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.

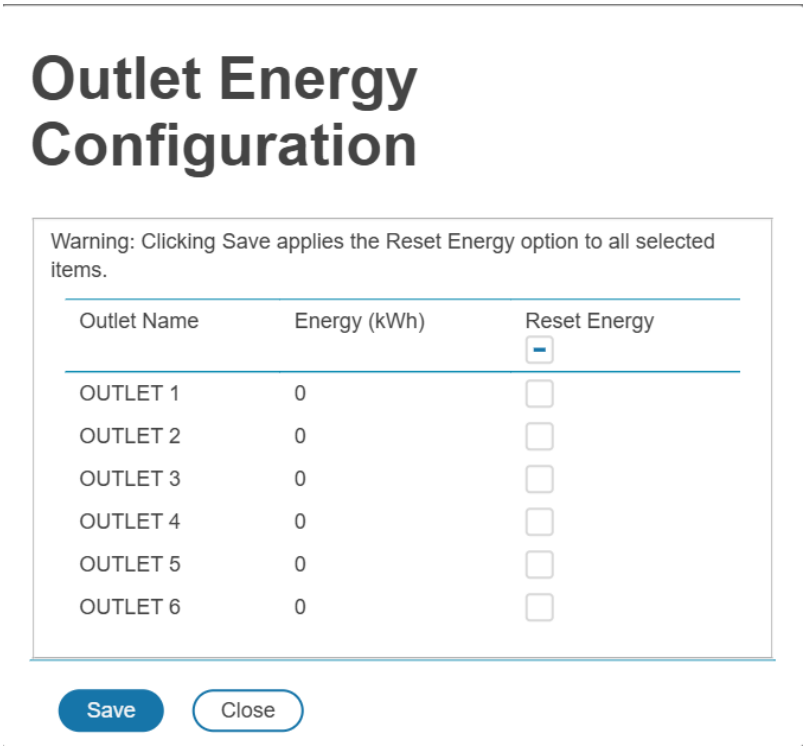


Figure 58: Multiple Outlet Energy Configuration dialog

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.

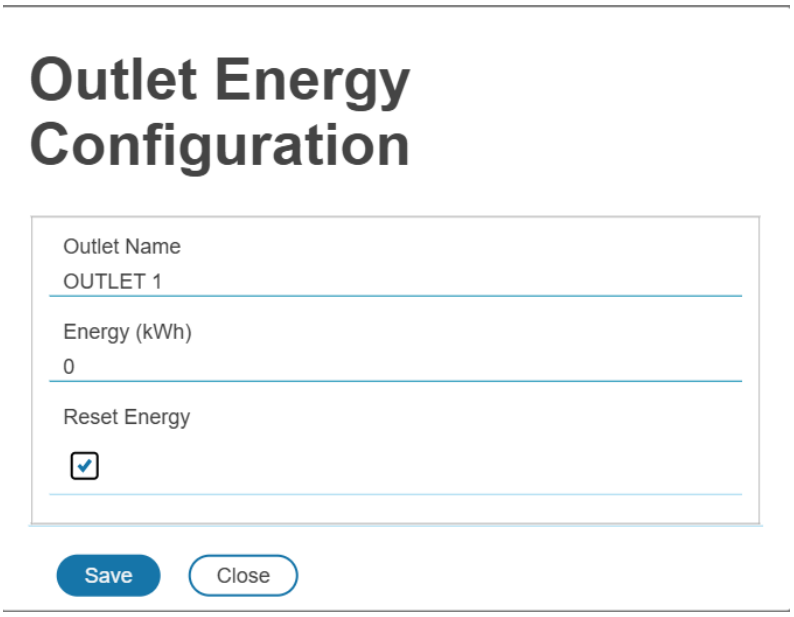


Figure 59: Outlet Energy Configuration

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.

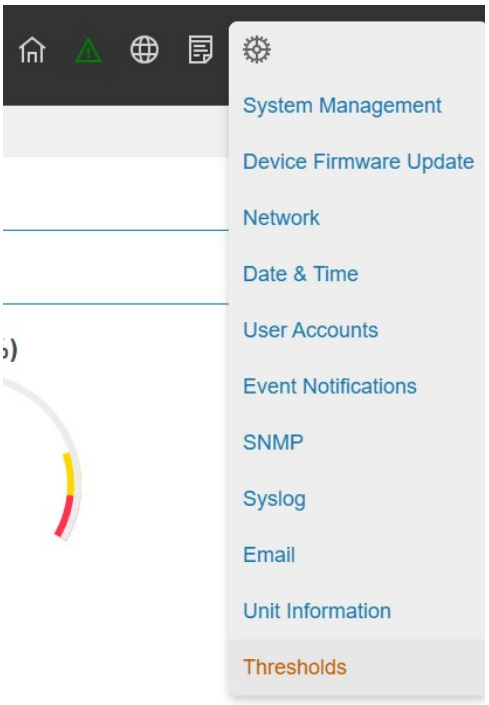


Figure 60: Threshold Settings

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.

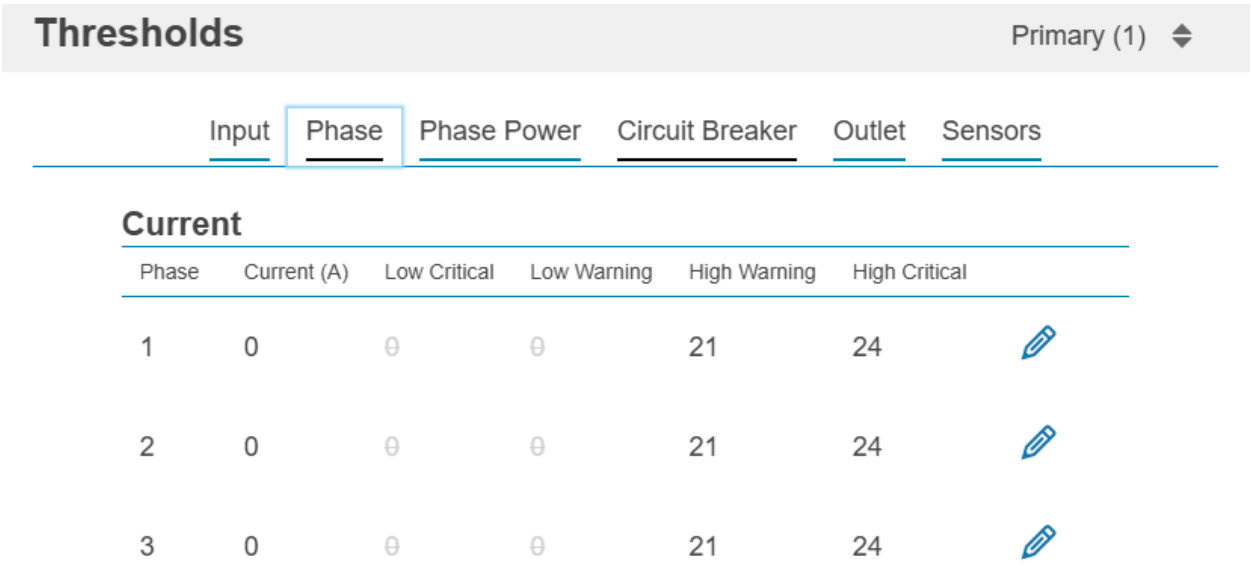


Figure 61: Threshold Configuration

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.

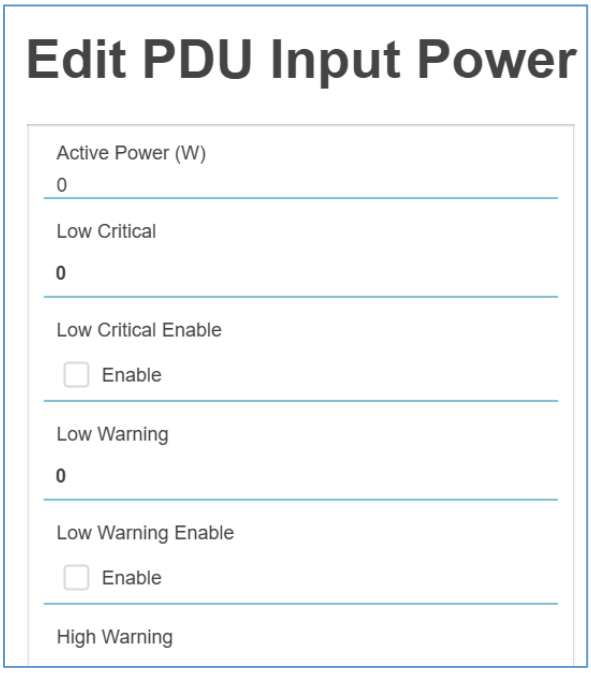


Figure 62: Power Threshold

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.

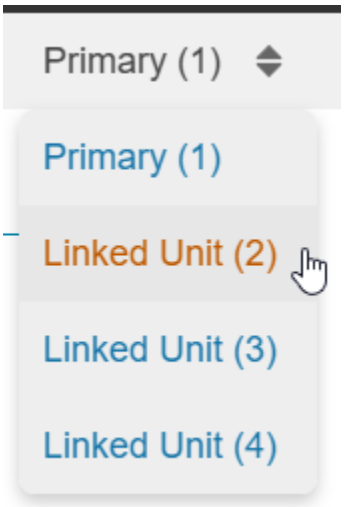


Figure 63: Selecting between Primary and Linked PDUs

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.

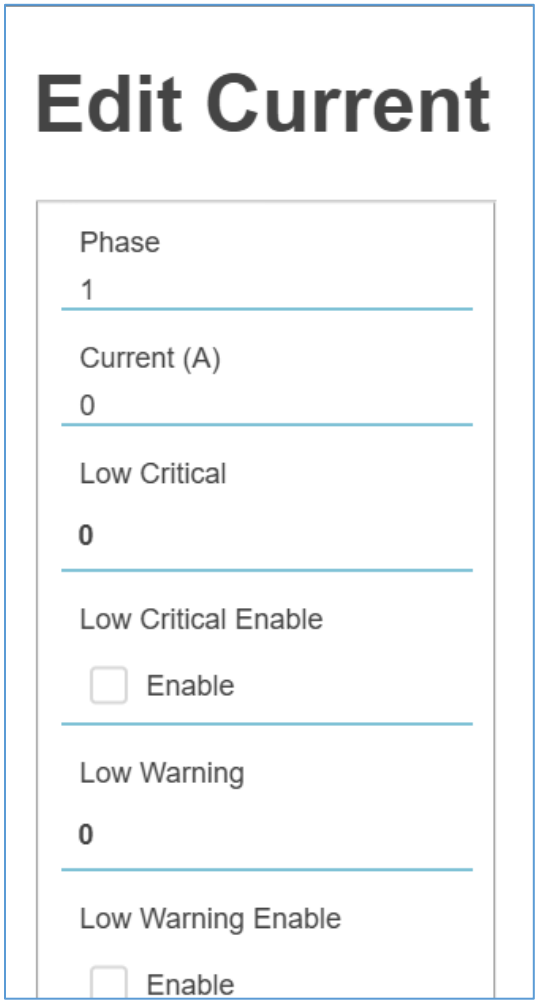


Figure 64: Phase Current Alarm

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.

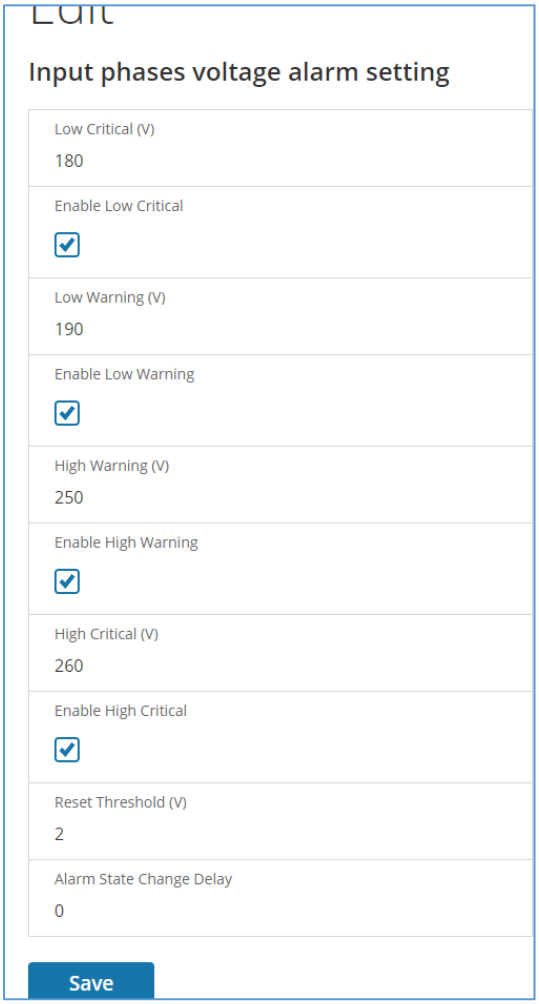


Figure 65: Phase Voltage Alarm

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.

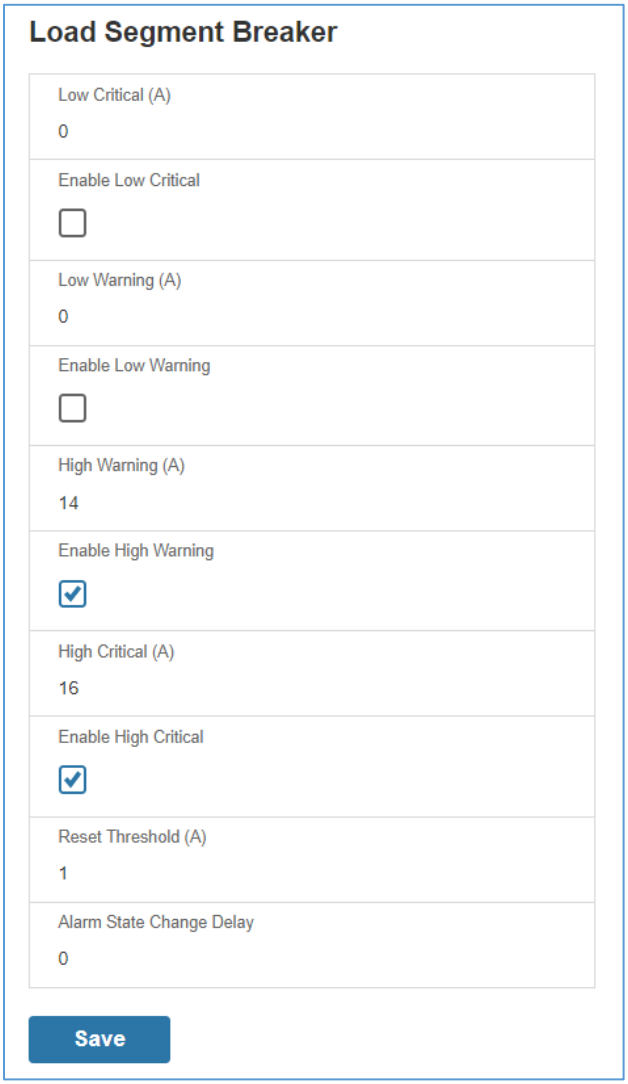


Figure 66: Load Segment Breaker

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.

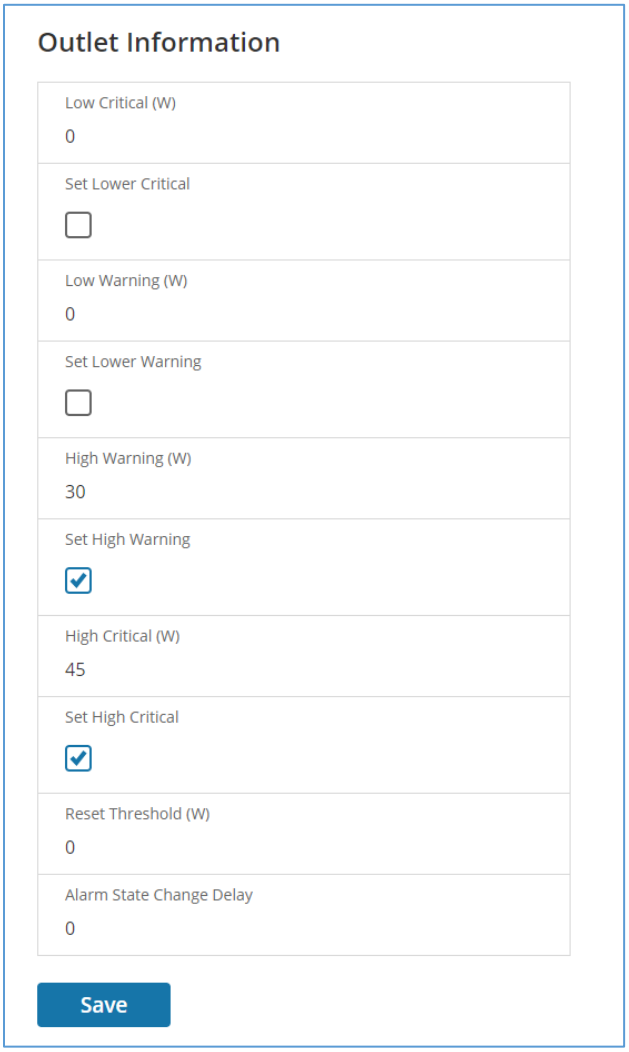


Figure 67: Outlet Information

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 68: Email Setup

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

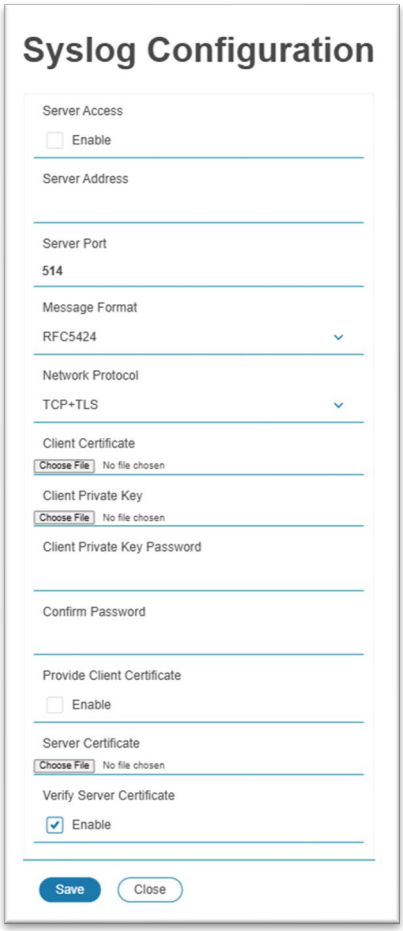


Figure 69: Syslog Configuration

- 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.

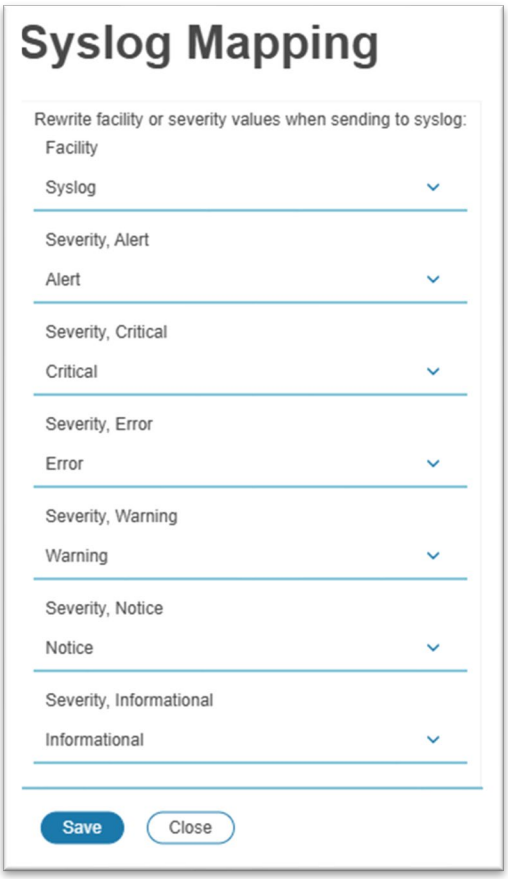


Figure 70: Syslog Mapping

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**.

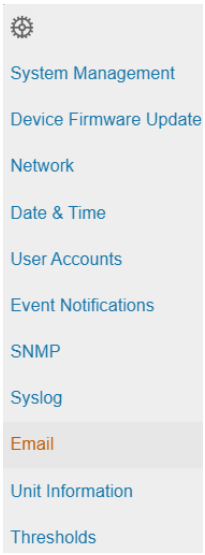


Figure 71: Email Setup

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

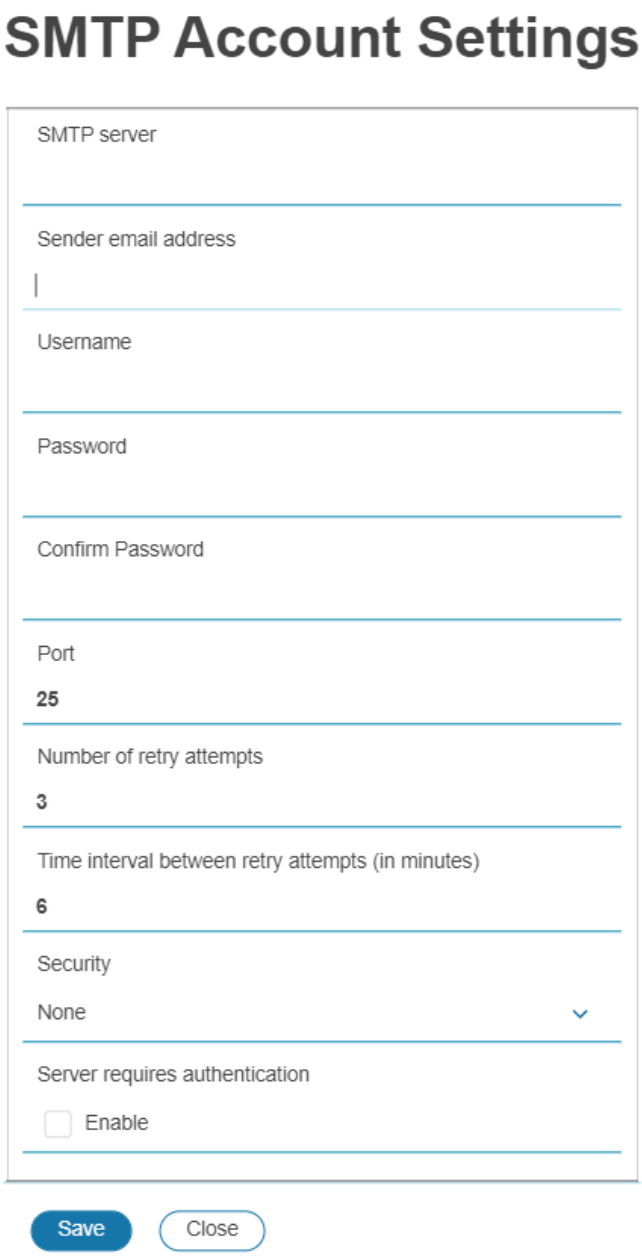


Figure 72: SMTP Account Settings

- 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.

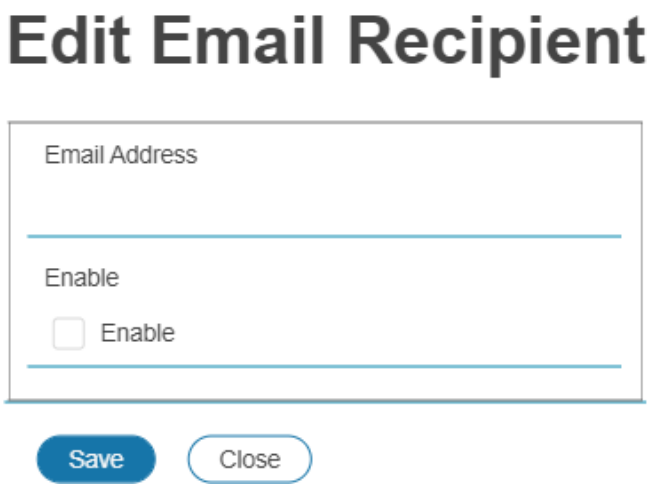


Figure 73: Email Recipient

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.

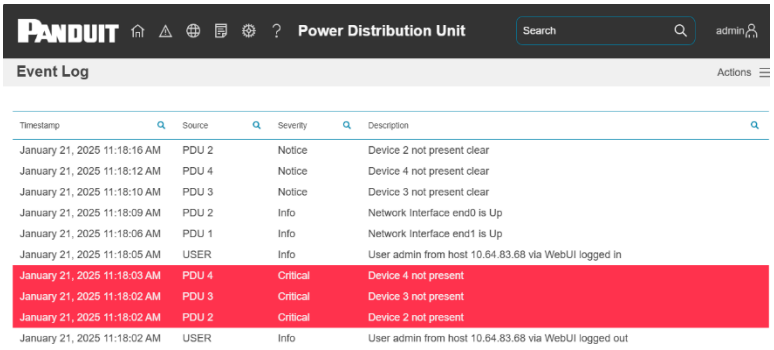


Figure 74: Event log

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

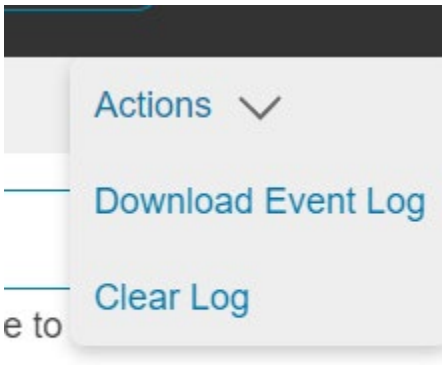


Figure 75: Event log Actions menu

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**.

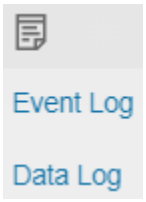


Figure 76: Data Log

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

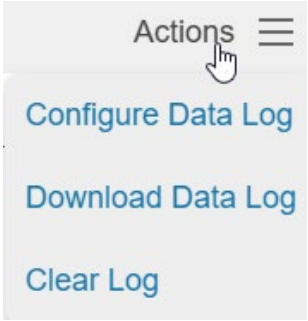


Figure 77: Data Log Configuration

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.)

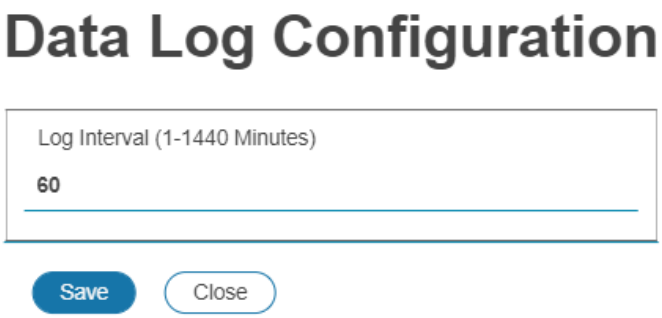


Figure 78: Data Log Configuration Panel

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.

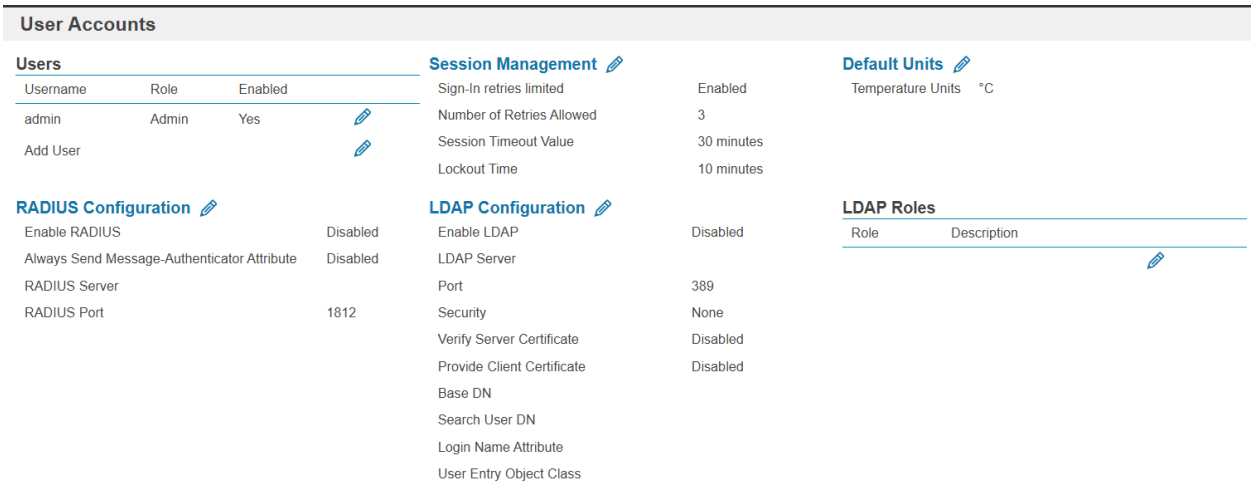


Figure 79: User Accounts

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

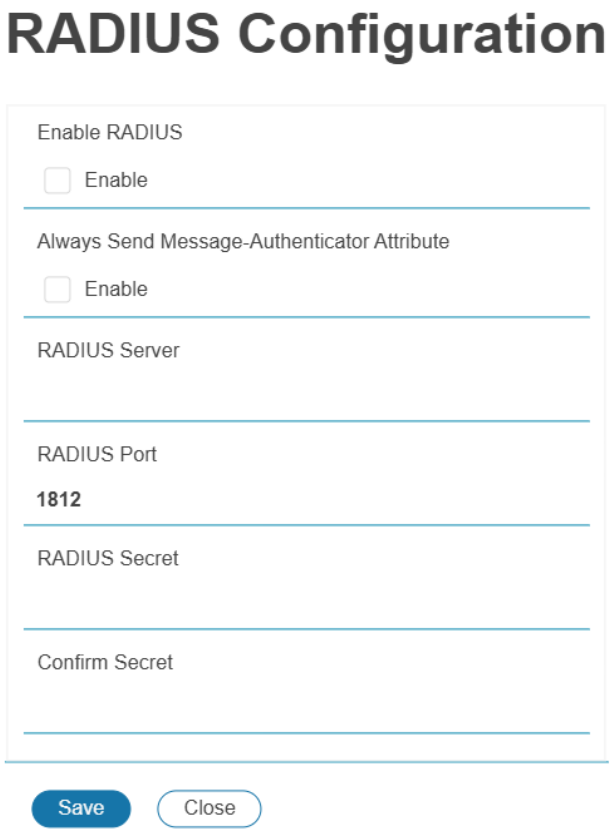


Figure 80: RADIUS Configuration

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

Setting Up the System for TACACS+ Authentication

1. Go to **User Accounts** in the settings menu.
2. Go to **TACACS+ Configuration** and click the edit pencil.

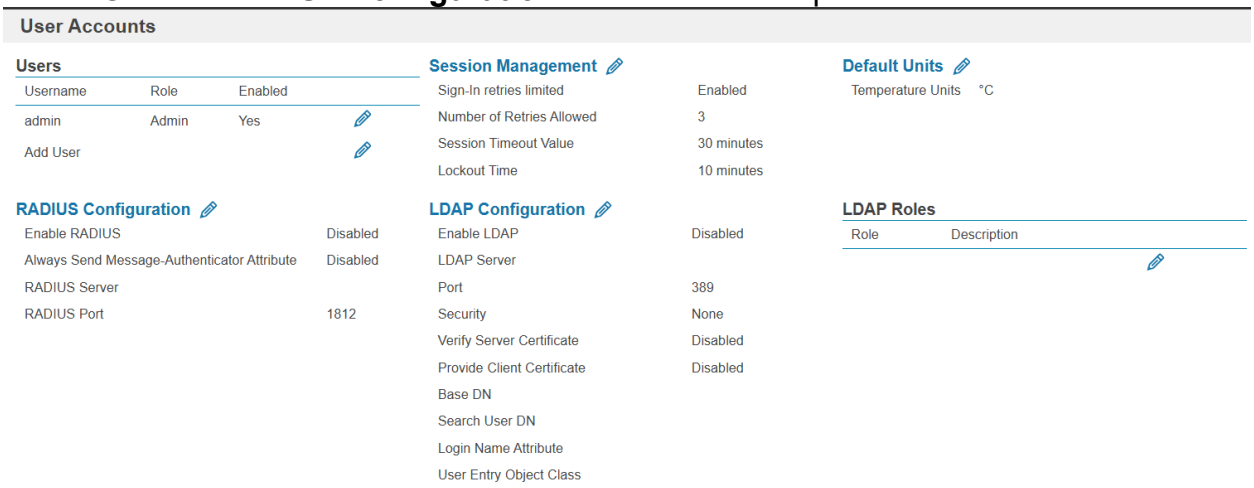


Figure 81: User Accounts

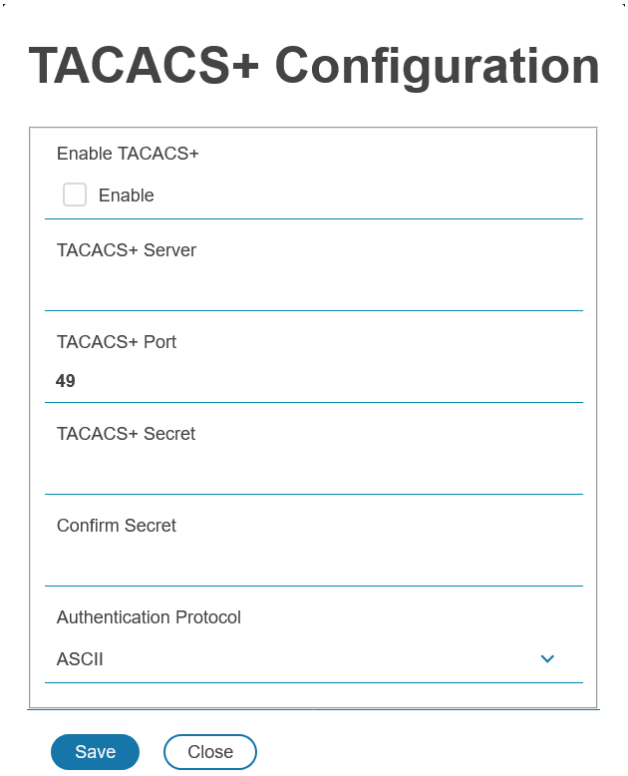


Figure 82: TACACS+ Configuration

3. Select the **Enable** button.
4. Enter Server IP address field, Port number field, Secret field, and choose an Authentication Protocol.
5. Click save and your TACACS+ authentication is complete.

Note: The administrator of the TACACS+ server may configure either:
- Panduit vendor-specific attributes with "panduit-user-role" set to User, Control, or Admin
- Standard privilege levels ("priv-lvl") set to 1 (User), 7 (Control), or 15 (Admin)

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 **Pencil** icon next to **LDAP Configuration** and check the **Enable** checkbox.
3. Enter an IP Address of the domain controller (LDAP Server)/Active Directory (AD) Server.
   e.g. *192.168.1.101*
4. Enter a Port.
   Note: Example Microsoft, this is typically 389.
5. Enter the Security. None for unencrypted transmission. StartTLS to upgrade the connection after connect to a TLS connection. TLS to start with TLS connection
6. 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*
7. Enter the password in the Bind Password and Confirm Password fields.
8. In the Search User DN field:
   e.g. *DC=subdomain,DC=mydomain,DC=com*
9. In the Login Name Attribute field, enter **sAMAccountName** (typically).
10. In the User Entry Object Class field, enter **person**.

With these LDAP settings configured, the Bind is complete.

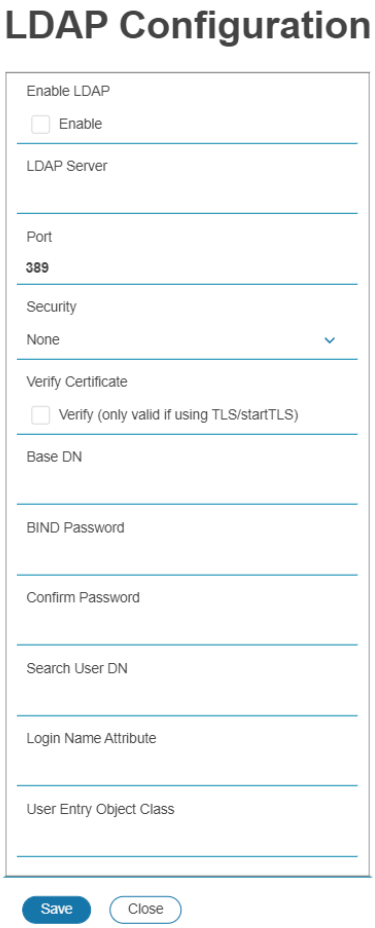


Figure 83: LDAP Configuration

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).

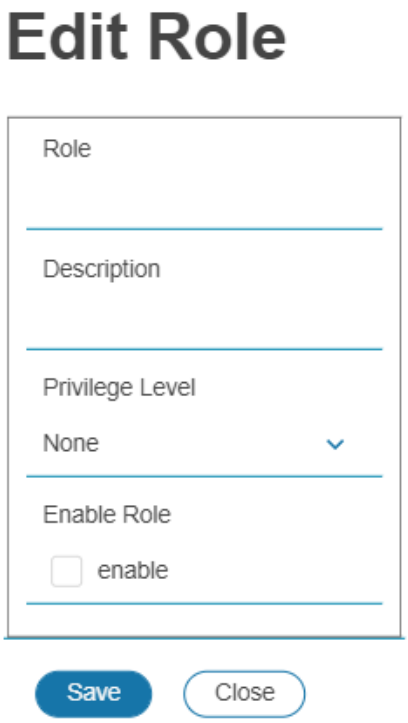


Figure 84: Enable Role Privileges

4. LDAP authentication is ready to use.

Event Notifications

The PDU can be configured to provide event notifications.

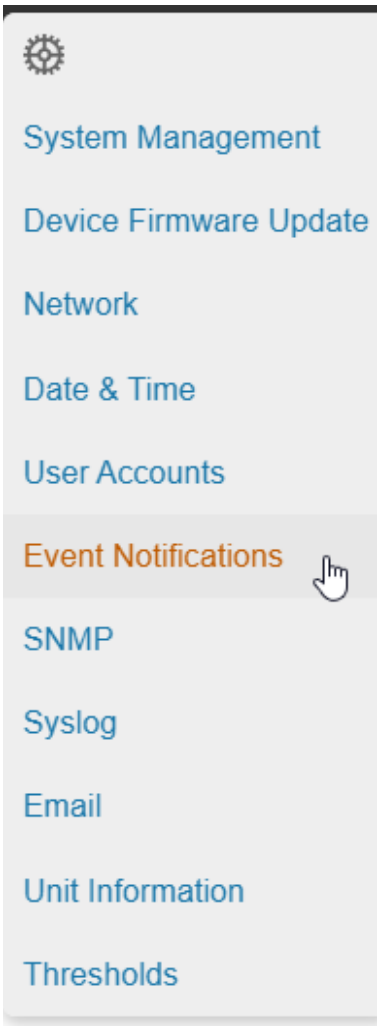


Figure 85: Event Notifications

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

The below table documents just the events that are not supported across all PDU types:

Event Notifications	Monitored Input (MI Series)	Monitored Input > 6 Breakers (MI Series)	Monitored Switched (MS Series)	Monitored Switched > 6 Breakers (MS Series)	Monitored Per Outlet (MPO Series)	Monitored and Switched Per Outlet (MSPO Series)
Circuit Breaker Status Changed	X	X	✓	X	✓	✓

Breaker Voltage	X	X	✓	X	✓	✓
Breaker/Group Current	✓	X	✓	X	✓	✓
Outlet Power Control Status Changed	X	X	✓	✓	X	✓

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.

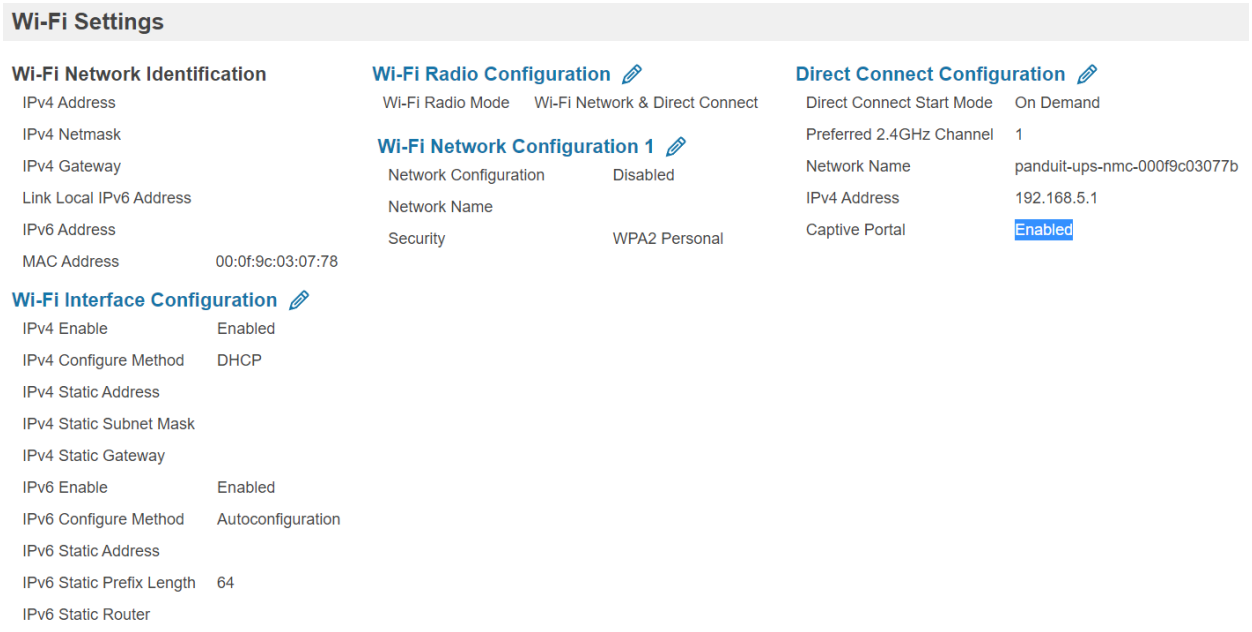


Figure 86: Wi-Fi Settings screen

Configuring Wi-Fi Radio mode

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

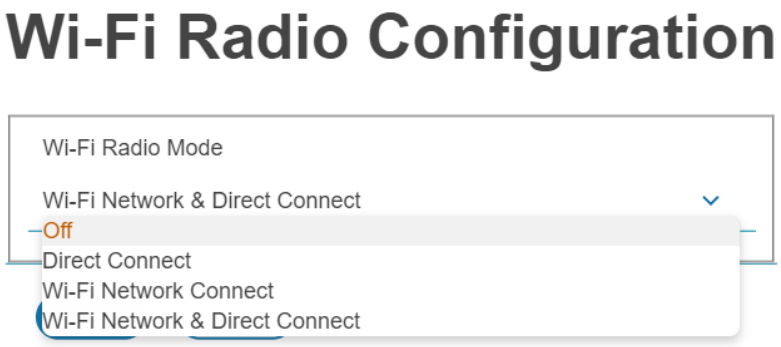


Figure 87: Wi-Fi Radio Configuration

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.

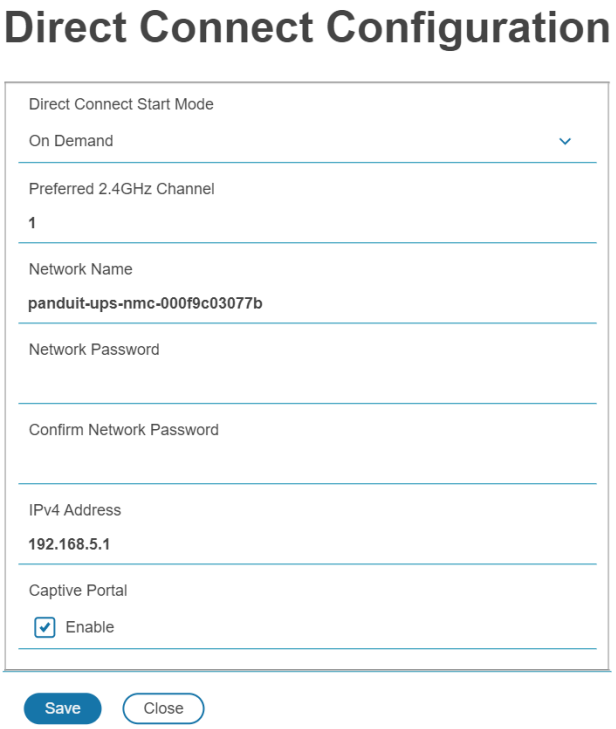


Figure 88: Wi-Fi Direct Connect Configuration

1. Select Start mode option
    - On Demand: Press the "Start On Demand" button on the LCD screen under "Network" -> "Wi-Fi AP" 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.

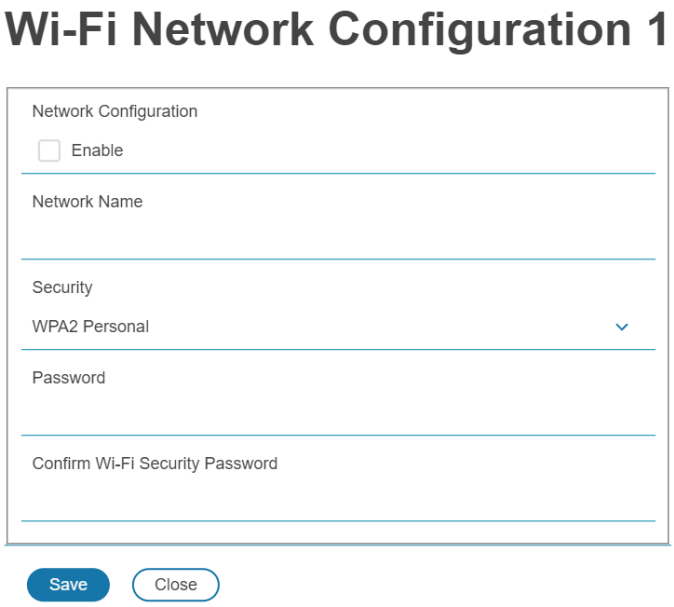


Figure 89: Wi-Fi Personal security Network configuration

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.

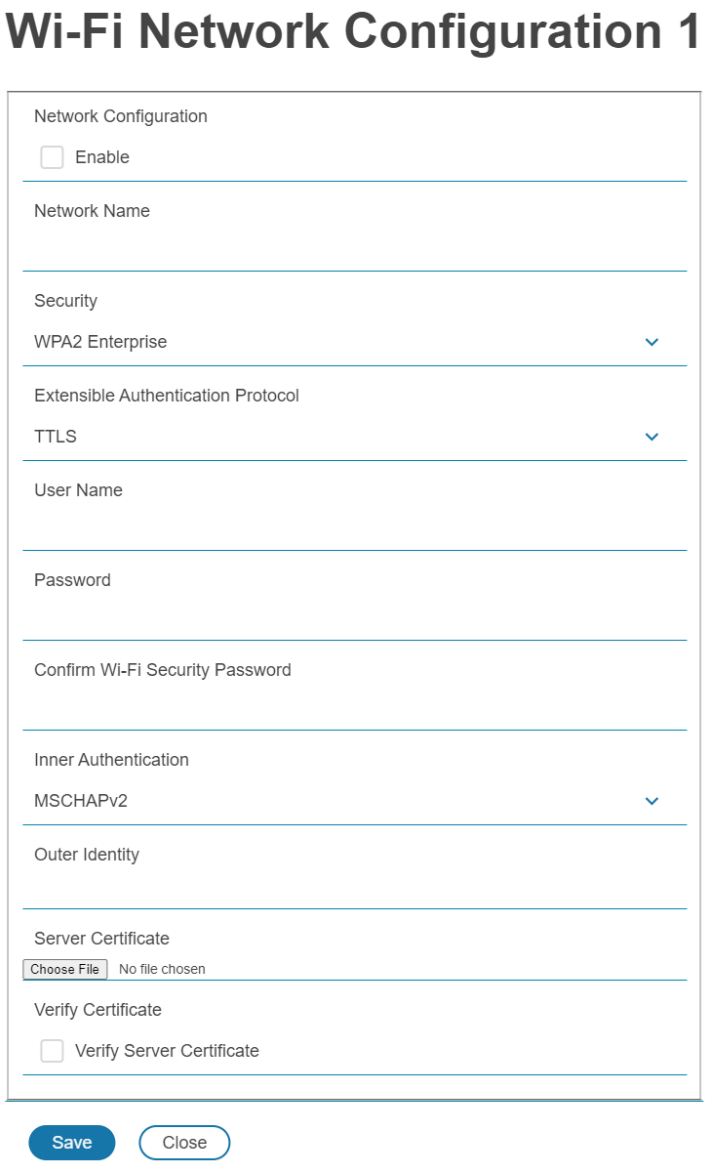


Figure 90: Wi-Fi Enterprise security Network configuration

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.

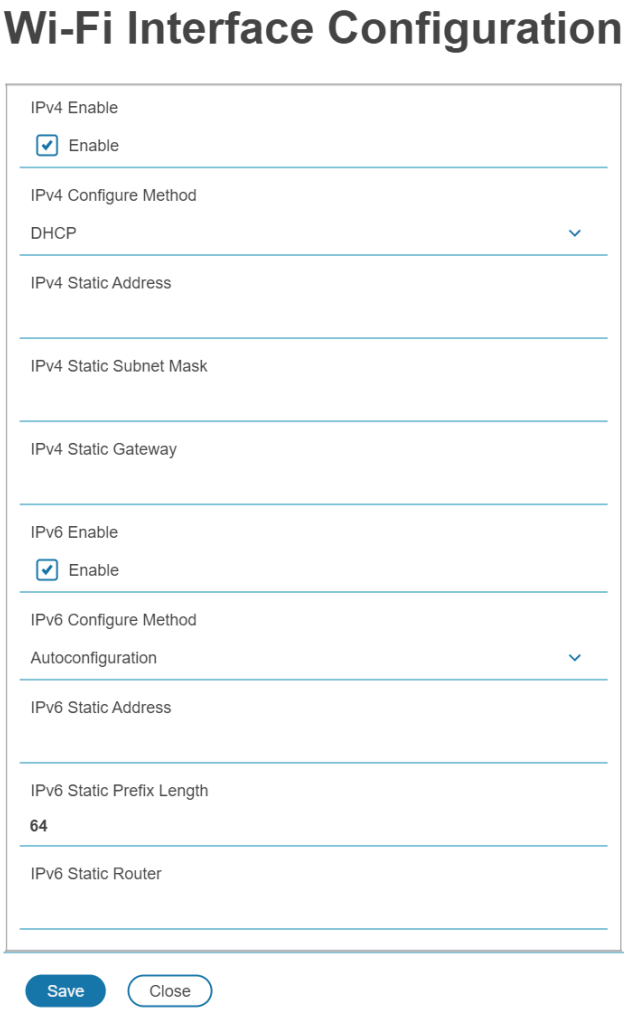


Figure 91: Wi-Fi Interface Configuration

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.

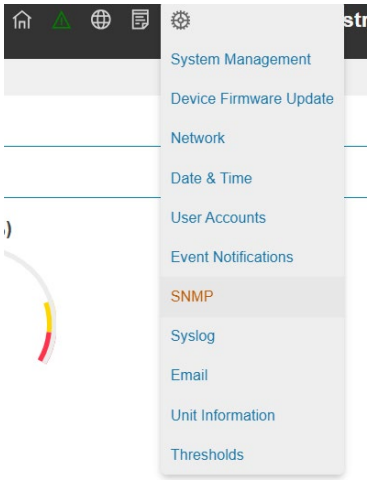


Figure 92: SNMP Configuration

3. The SNMP General includes SNMP Access and Version.

Figure 93: SNMP General

Setup SNMP Port

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

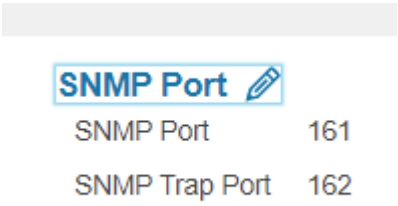


Figure 94: SNMP Port

3. Set up SNMP Port and SNMP Trap Port.

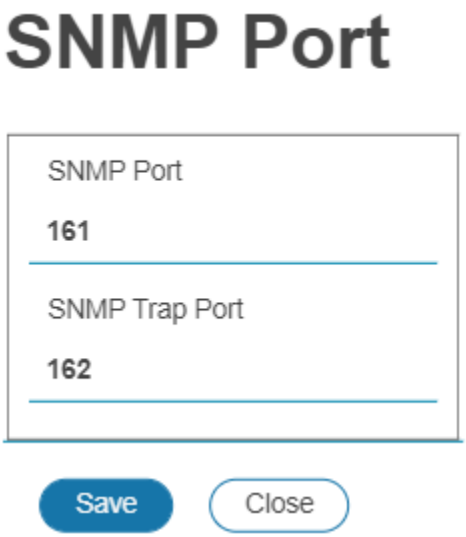


Figure 95: Setup SNMP Port and Trap Port

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.

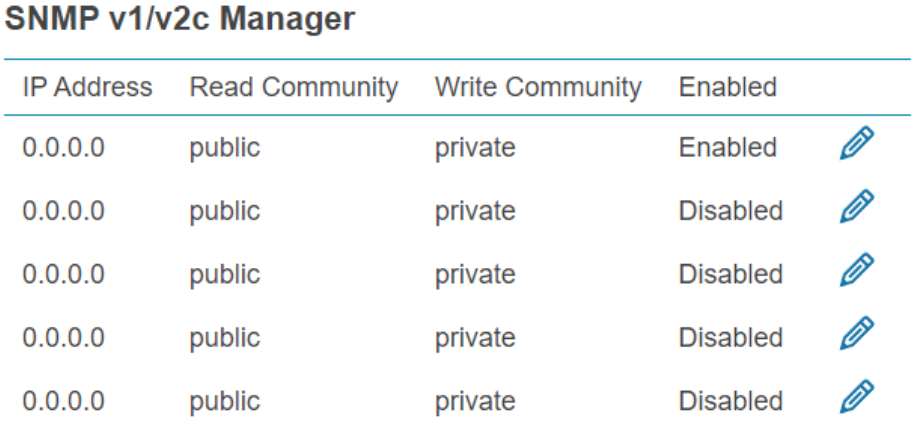


Figure 96: Define SNMP V1/V2c User

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

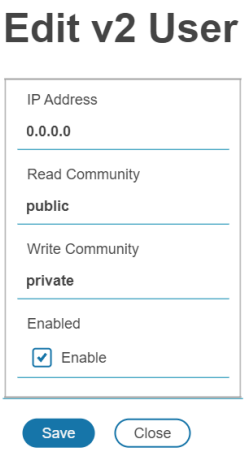


Figure 97: Edit V1/2c Manager

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.

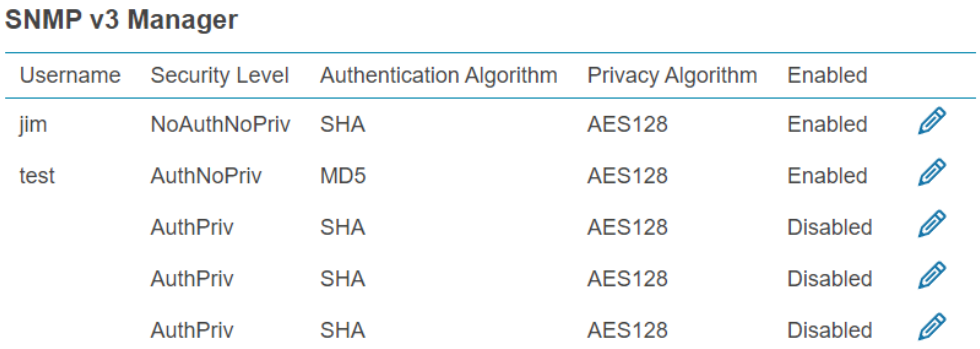


Figure 98: SNMP v3 Manager

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

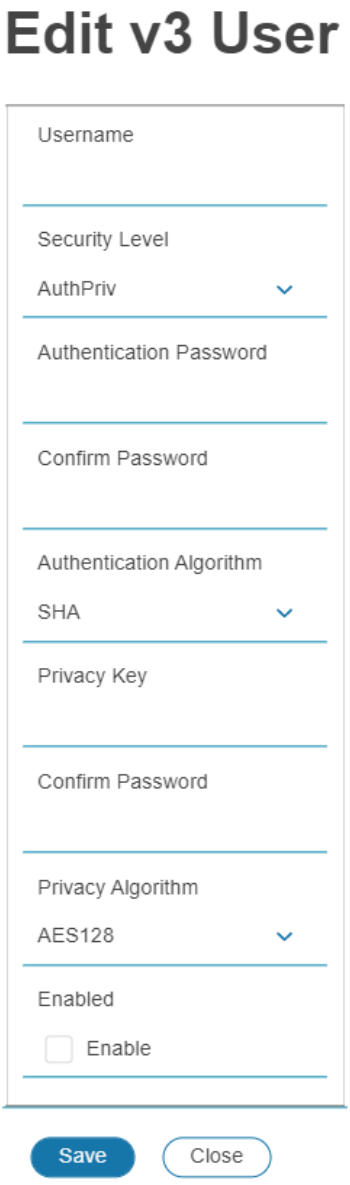


Figure 99: SNMP V3 Edit

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.

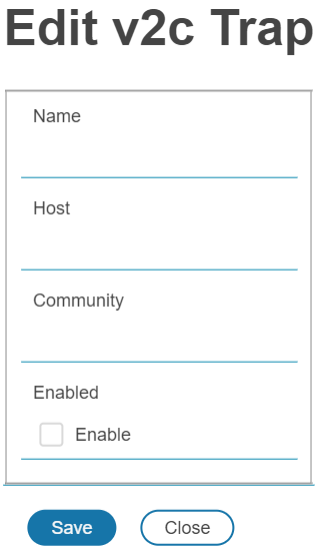


Figure 100: SNMPv2c Trap Receiver Configuration Information

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.

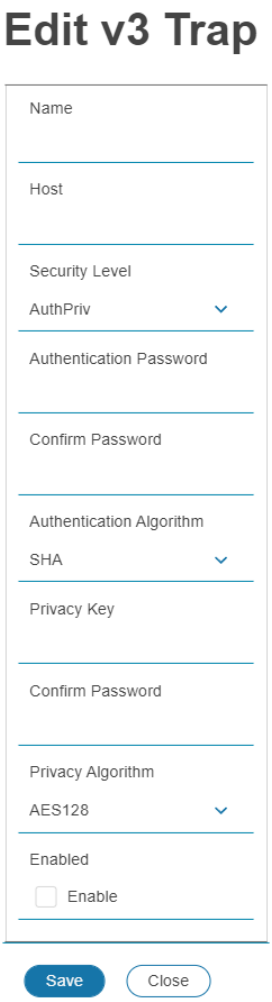


Figure 101: SNMPv3 Trap Server configuration Information.

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.

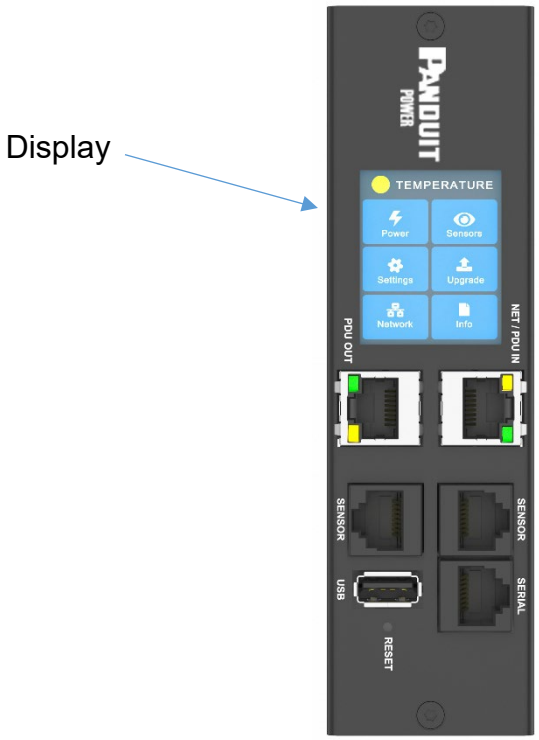


Figure 102: Network Controller

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

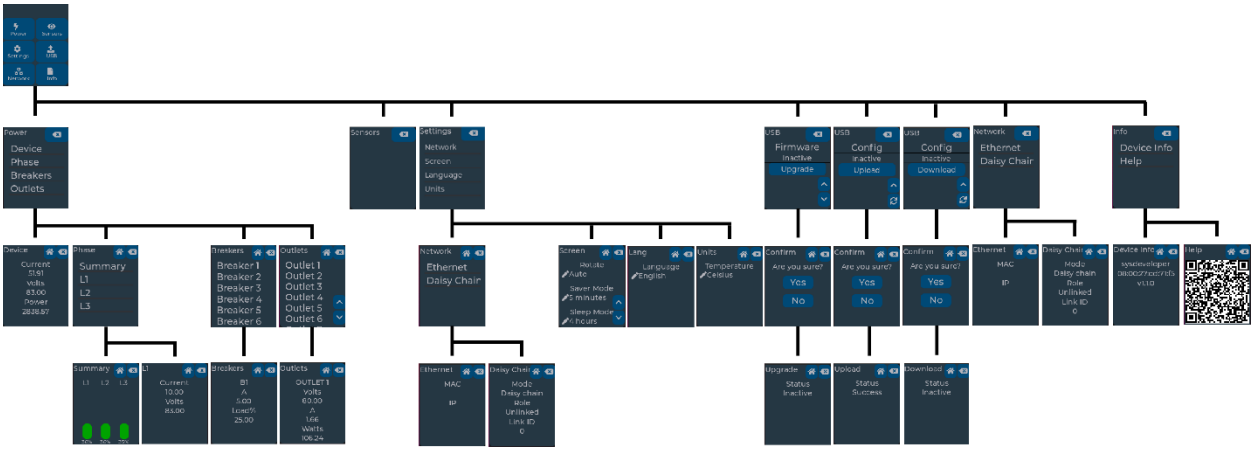


Figure 103: Network Controller Menu Structure

Main Menu Selections

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

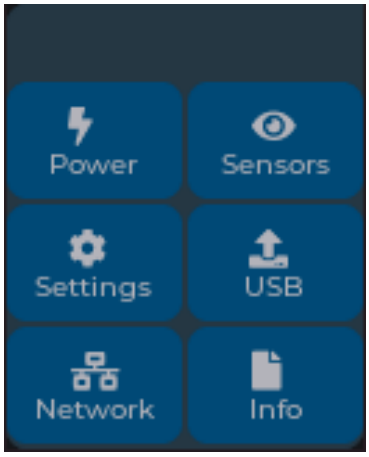


Figure 104: Main Menu Selections

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.

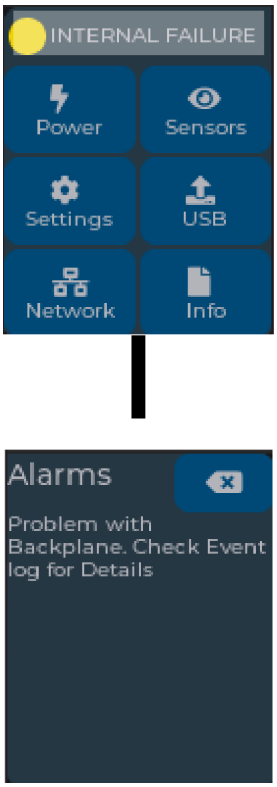


Figure 105: Alarms Menu

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.

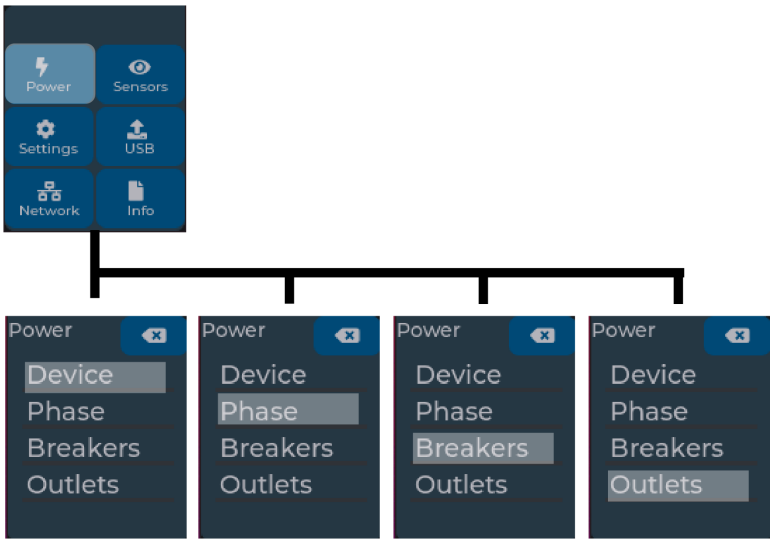


Figure 106: Power Menu

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.

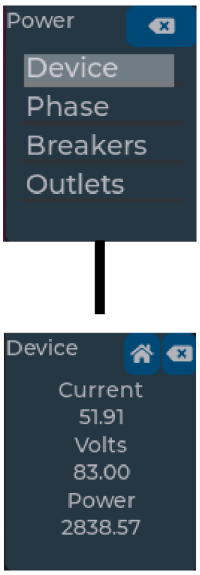


Figure 107: Device Submenu

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 108: 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.

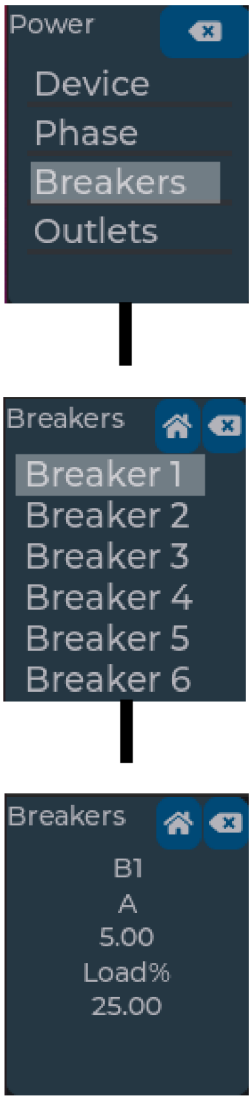


Figure 109: Breaker Submenu

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.

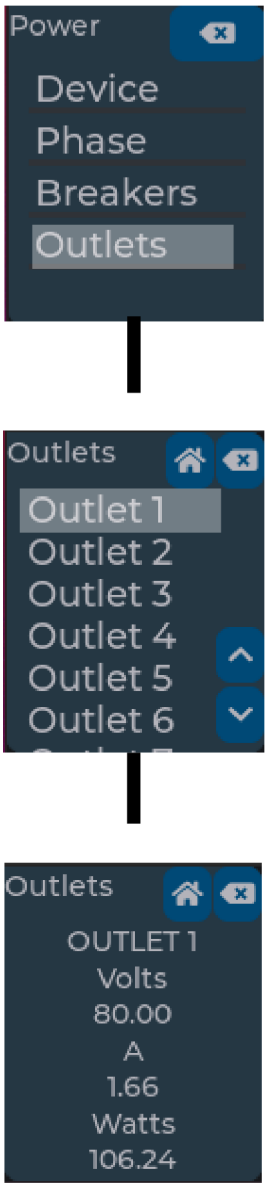


Figure 110: Outlet Submenu

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.

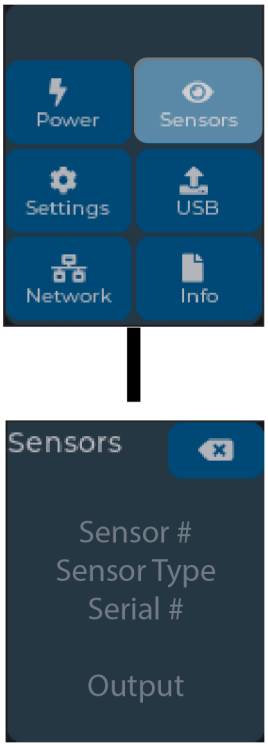


Figure 111: Sensors

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.

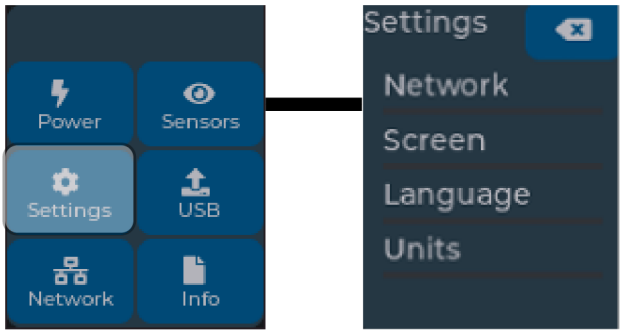


Figure 112: Setup Menu

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.

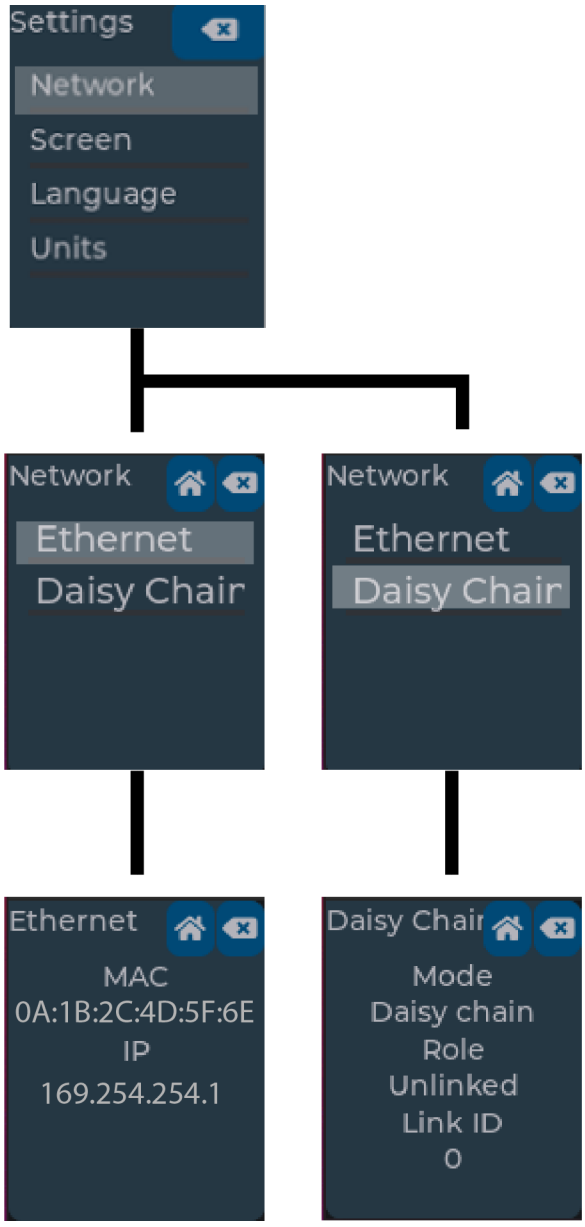


Figure 113: Network Submenu

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.

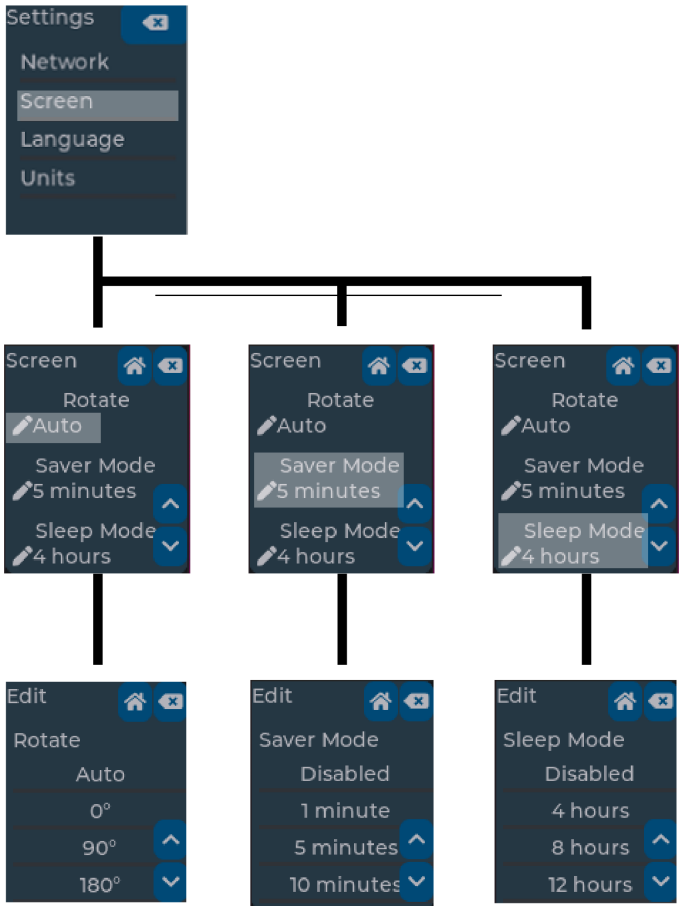


Figure 114: Screen Submenu

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.

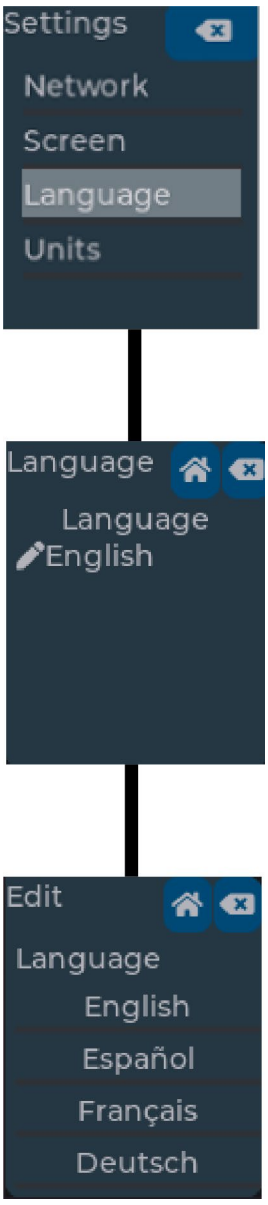


Figure 115: Language Submenu

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.

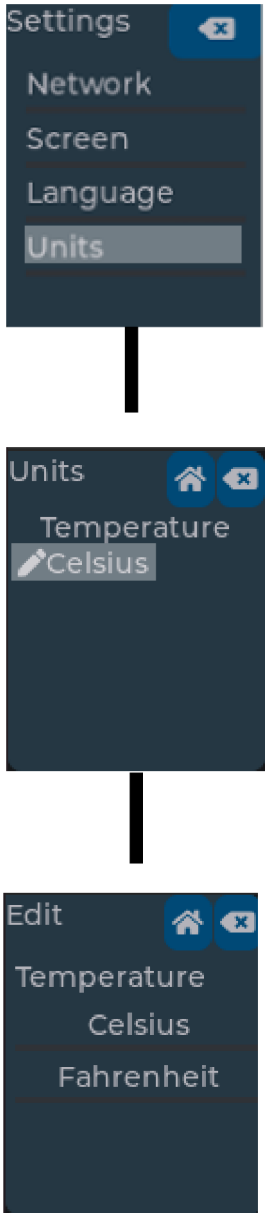


Figure 116: Units Submenu

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).

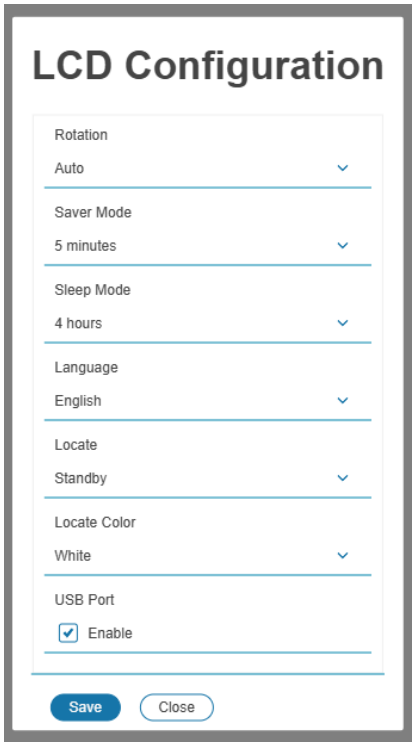


Figure 117: USB Enable

Firmware Update via USB

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

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.

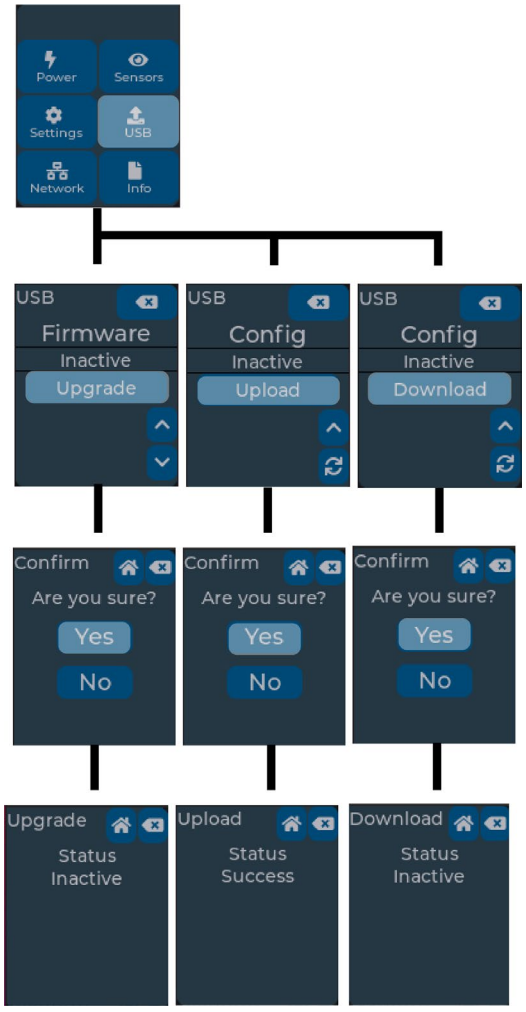


Figure 118: USB Submenu

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.

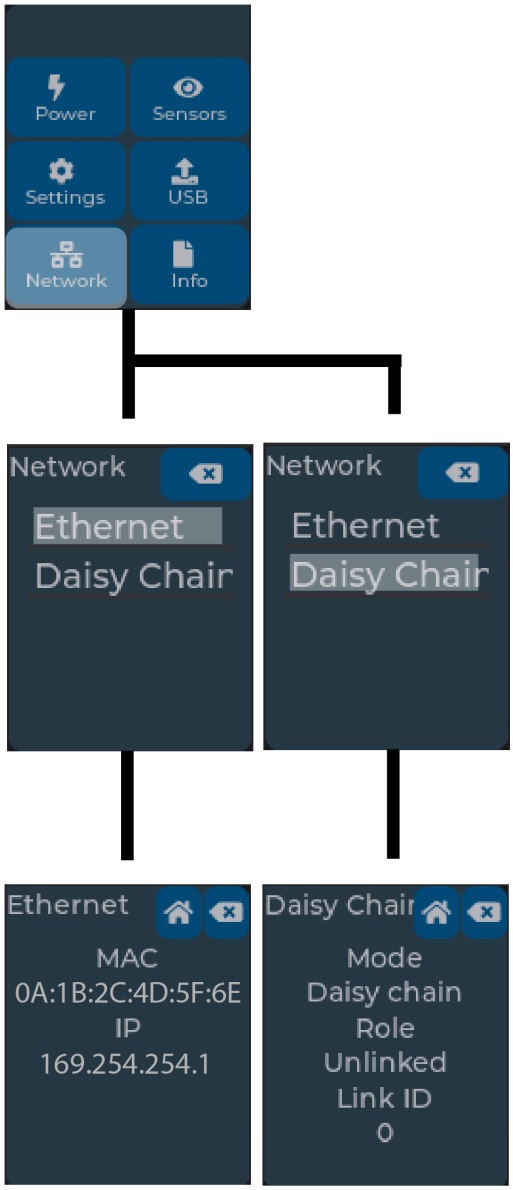


Figure 119: Network Menu

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.

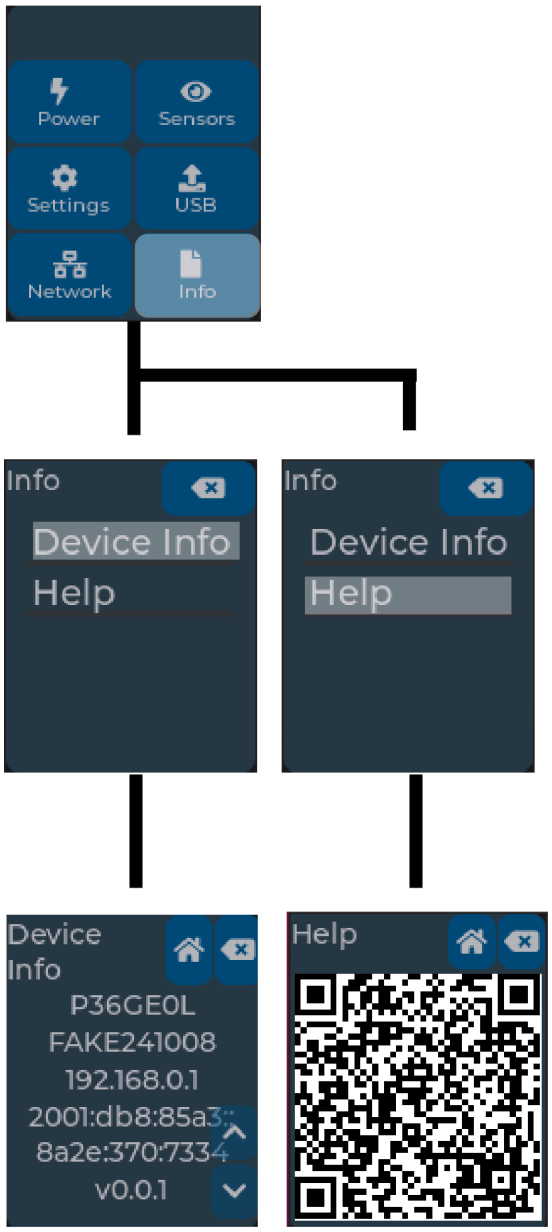


Figure 120: Info Menu

Help Menu

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

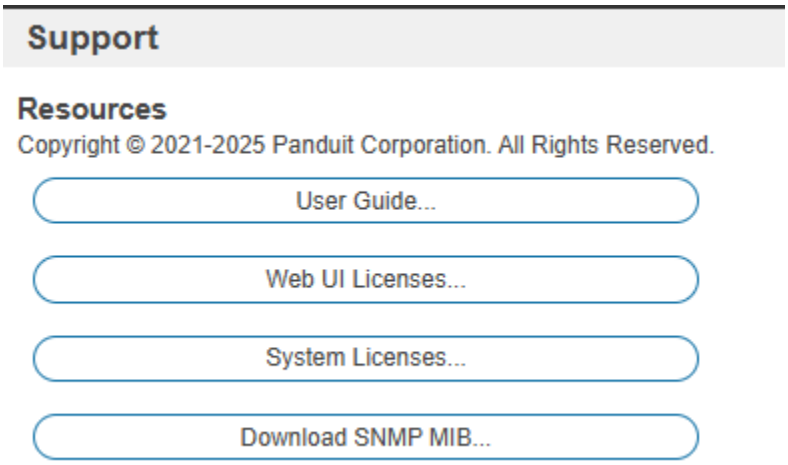


Figure 121: Help & Support

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"

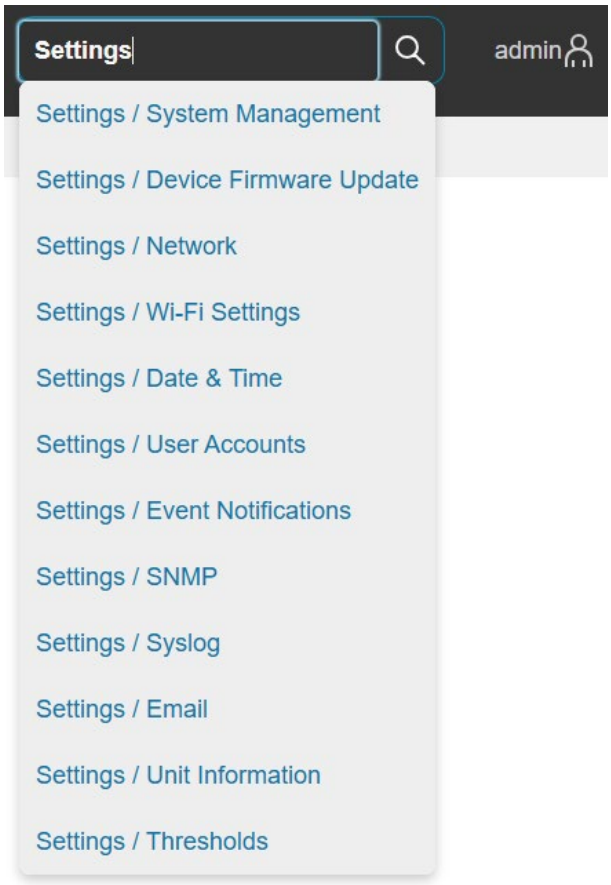


Figure 122: Example Search Box

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.

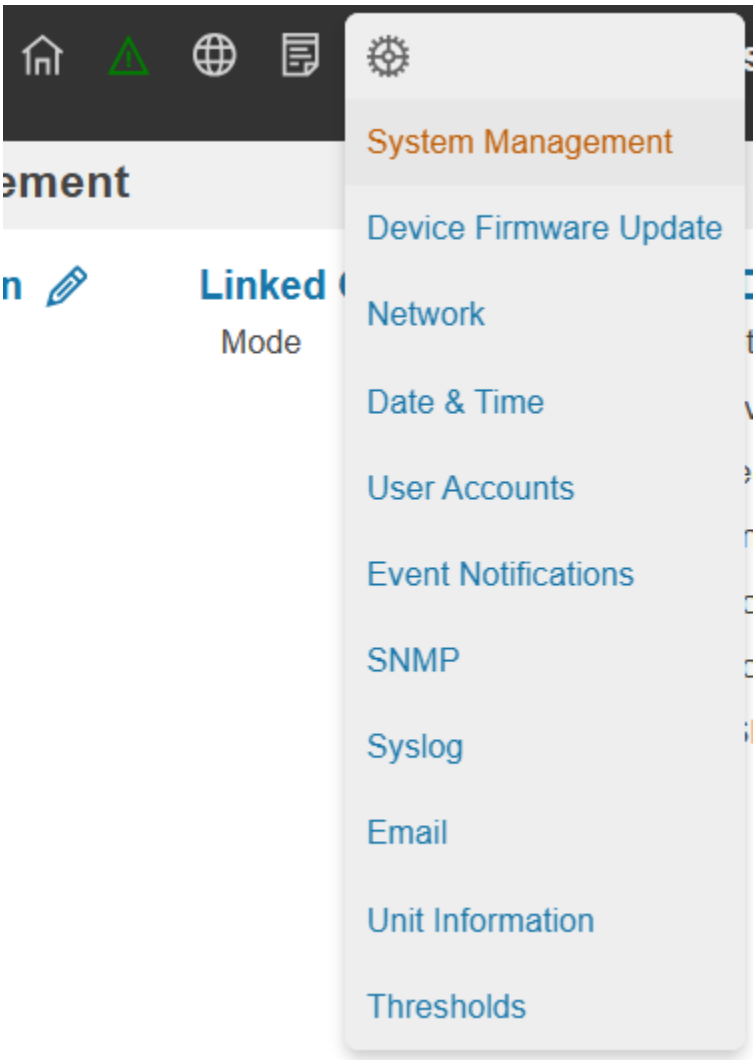


Figure 123: System Management

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

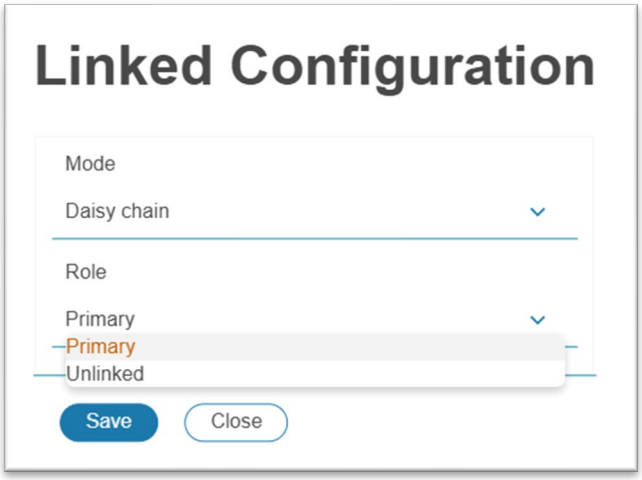


Figure 124: Linked Configuration

Daisy-Chain Overview

In standard daisy chain mode, multiple EL2P PDUs are connected in series and managed through a single IP address assigned to the primary PDU. The downstream PDUs do not receive individual network identities and are accessed indirectly through the primary unit's web interface.

Because all communication is aggregated through one management interface, this mode is subject to a fixed daisy chain limit, which constrains the maximum number of PDUs that can be connected and managed together.

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 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.

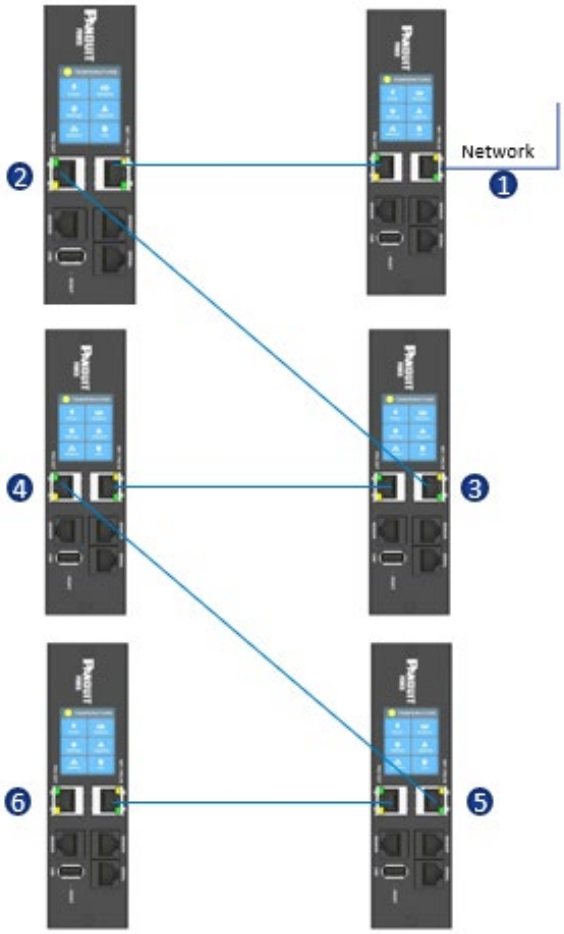


Figure 125: Connection Diagram 6 PDU Daisy Chain

Bridge Mode Daisy Chain

In bridge mode daisy chain, multiple EL2P PDUs are physically connected through a single network connection point and daisy chained together similar to standard daisy chain mode, but each PDU operates in Stand Alone mode at the network level.

In this configuration, every PDU is assigned its own distinct IP address, allowing each unit to be accessed, monitored, and managed independently—even though they share a common network uplink.

As a result, bridge mode effectively removes the daisy chain limit imposed by standard daisy chaining. Since each PDU is individually addressable and does not rely on a master unit for network access, scalability is driven by network capacity rather than daisy chain constraints.

Bridge Mode and Network Redundancy

Bridge mode can be used to implement a network redundancy configuration by connecting both ends of a daisy-chained group of EL2P PDUs to the network. In this topology, Spanning Tree Protocol (STP) is required to prevent network loops.

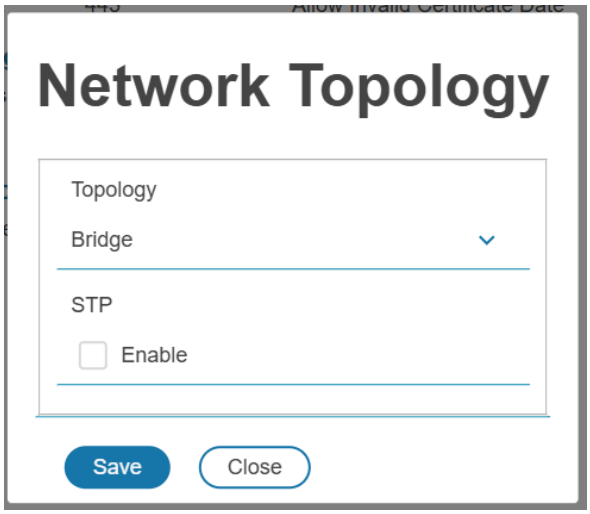
When both ends of the daisy chain are connected, STP actively manages the redundant paths to ensure only a single active forwarding path exists at any time. Without STP, this configuration will create a network loop, which can result in broadcast storms, degraded network performance, or network outages.

WARNING: Do not connect both ends of the daisy chain to the network unless STP is enabled and properly configured.

If STP is enabled, the corresponding configuration must also be applied on the connected network switches. Note that some network designs or switch policies may automatically disable ports if STP is detected unexpectedly or conflicts with existing network settings. Verify switch behavior and port configuration prior to deployment.

Bridge Mode Setup

Each PDU in the chain must be configured for Bridge mode. Starting with the PDU directly connected to the network, under Settings->Network, select Network Topology and change the configuration to Bridge.



If using STP, check enabled in the dialog box.

You should now be able to communicate with the next PDU in the chain. Repeat the

Network Topology configuration for each PDU.

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.

Power Share in Bridge Mode

Setting up a Bridge Mode Daisy Chain with Redundancy and Power Share involves a few simple CLI commands during configuration.

CLI Command for the UPLINK (U) PDU:

write config/powerShare/enUplink 0

write config/powerShare/enDownlink 1

CLI Command for the DOWNLINK (D) PDU:

write config/powerShare/enUplink 1

write config/powerShare/enDownlink 0

CLI Command for the internal PDUs (within the Daisy Chain):

write config/powerShare/enUplink 1

write config/powerShare/enDownlink 1

Refer to the figure below for a diagram illustrating how to set up Bridge Mode Daisy Chain with Redundancy and Power Sharing.

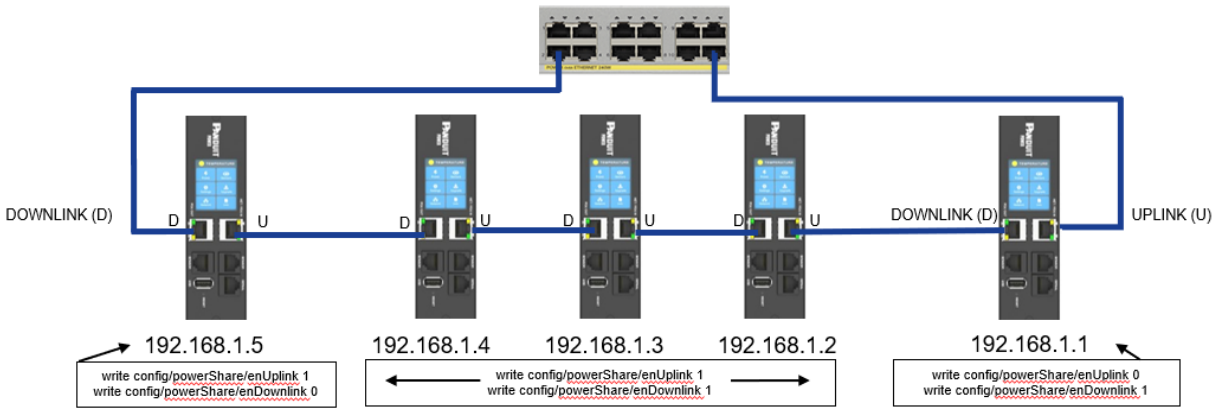


Figure 126: Bridge Mode Daisy Chain with Redundancy and Power Share

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 sensor accessories to the NMC controller or connecting EL2P PDU Sensors to 3rd party controllers may result in damage.

Note: The maximum number of sensors supported by each Panduit NMC controller depends on the number and type of logical sensing functions provided by the connected physical sensor accessories. A single physical sensor accessory may support multiple logical sensing capabilities. Physical sensor accessories can be installed while the NMC is powered on.

Logical Sensing Capability	Max Logical Sensors per NMC
Temperature	6
Humidity	4
Door	2
Rope	2
Spot	2
Dry	2
Auto Light Bar	2
Handle	2

The following table lists available physical sensor accessory products as well as the accessories' respective associated logical sensing capabilities:

Physical Sensor Accessory	Description	Logical Sensing Capability, Count
Temperature Sensor (EA001, EA001L)	Monitors the temperature in the rack.	Temperature, 1
Temperature + Humidity Sensor (EB001, EB001L)	Monitors the temperature and relative humidity in the rack.	Temperature, 1

Physical Sensor Accessory	Description	Logical Sensing Capability, Count
		Humidity, 1
Three Temperature + Humidity Sensor (EC001, EC001L)	Monitors the temperature in three areas using three separate probes and the relative humidity using one probe.	Temperature, 3 Humidity, 1
Door Sensor (ACA01, ACA01L)	Monitors intrusion when a door on which the sensor is installed has been opened greater than 10 mm.	Door, 1
Liquid - Rope Sensor (ED00, ED001L)	Monitors leak detection of liquid with a resistivity of less than 2 megaohms (including distilled water).	Rope, 1
Liquid – Spot Sensor (EE001, EE001L)	Monitors leak detection of liquid with a resistivity of less than 2 megaohms (including distilled water) in the monitored area.	Spot, 1
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.	Dry, 1
Auto Light Bar (ACD01L)	Remote control and automatic space illumination	Auto Light Bar, 1
Smart Rack Handle (ACF06L)	Smart Rack Access Handle	Handle, 1

Physical Sensor Accessory	Description	Logical Sensing Capability, Count
3-Temperature + Humidity, Door Switch Sensor (EHC01L)	Monitors the temperature in three areas using three separate probes, door intrusion, and the relative humidity using one probe.	Temperature, 3 Humidity, 1 Door, 1
1-Temperature, Humidity Door Switch Sensor (EHH01L)	Monitors the temperature in one area, door intrusion, and the relative humidity using one probe.	Temperature, 1 Humidity, 1 Door, 1
Smart Rack Handle (ACF05, ACF06)	Smart Rack Access Handle with humidity sensor	Handle, 1 Humidity, 1
Three Temperature + Door Sensor Harness (ACF11 requires ACF05 or ACF06)	Monitors the temperature in three areas using three separate probes and one door.	Temperature, 3 Door, 1
Temperature + Door Sensor Harness (ACF10 requires ACF05 or ACF06)	Monitors the temperature and one door in the rack.	Temperature, 1 Door, 1

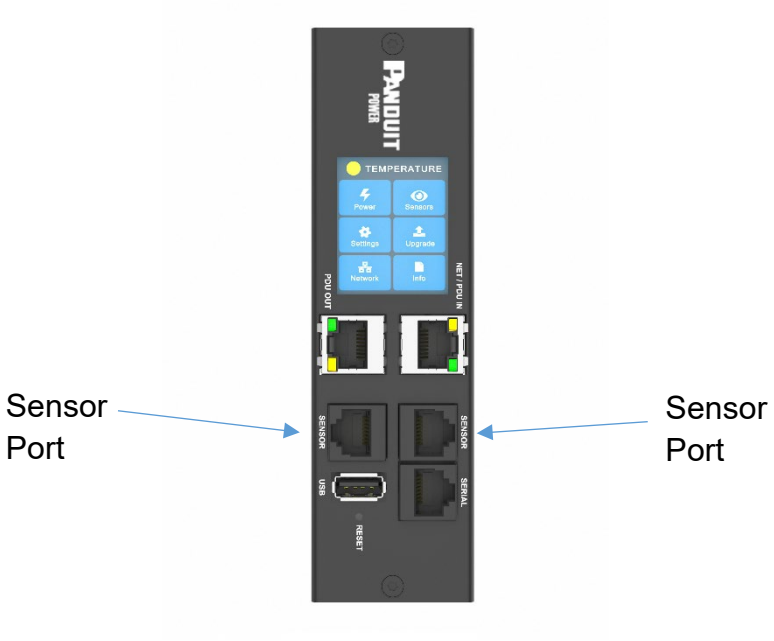


Figure 127: Sensor Ports

Configuring Temperature Scale

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

1. Go to **User Accounts.**

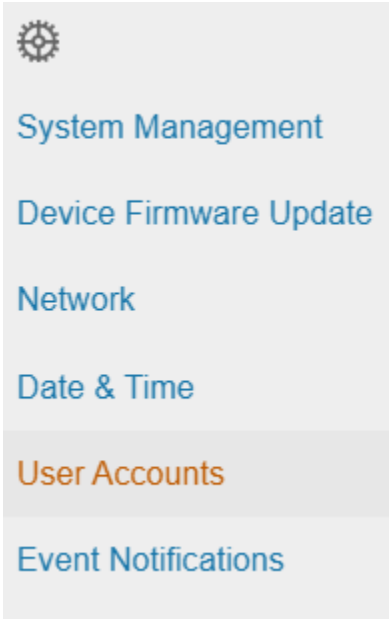


Figure 128: User Accounts

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

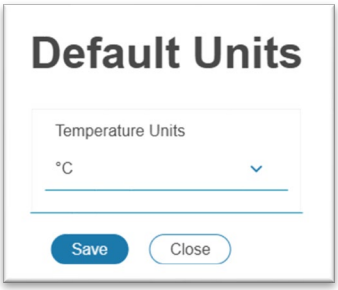


Figure 129: Temperature Units Setting

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.

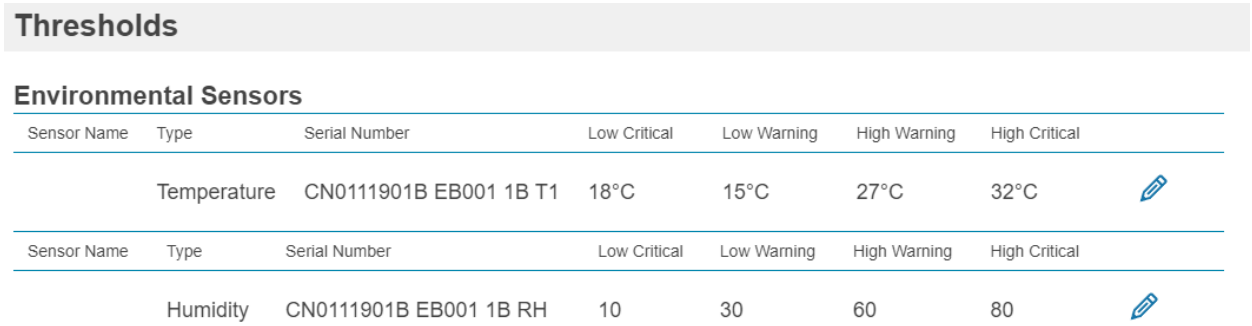


Figure 130: Environmental Sensor Threshold Configuration View

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

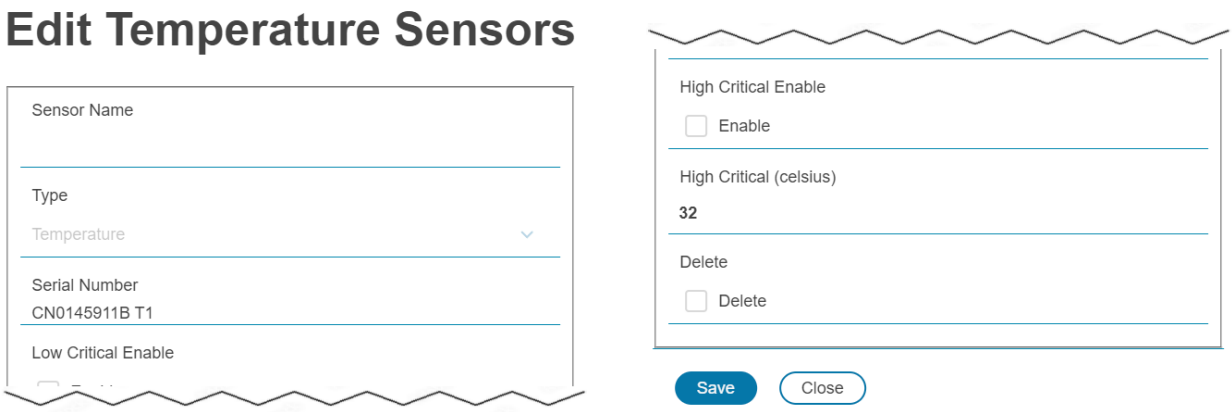


Figure 131: Temperature Sensor Edit dialog

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.

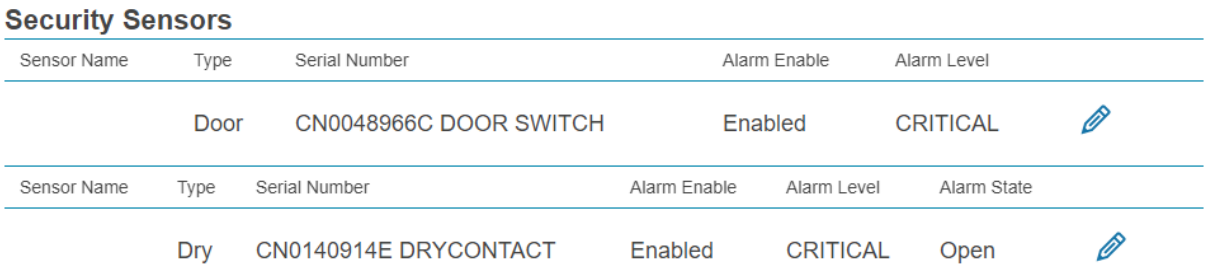


Figure 132: Security Sensor Alarm Configuration view

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

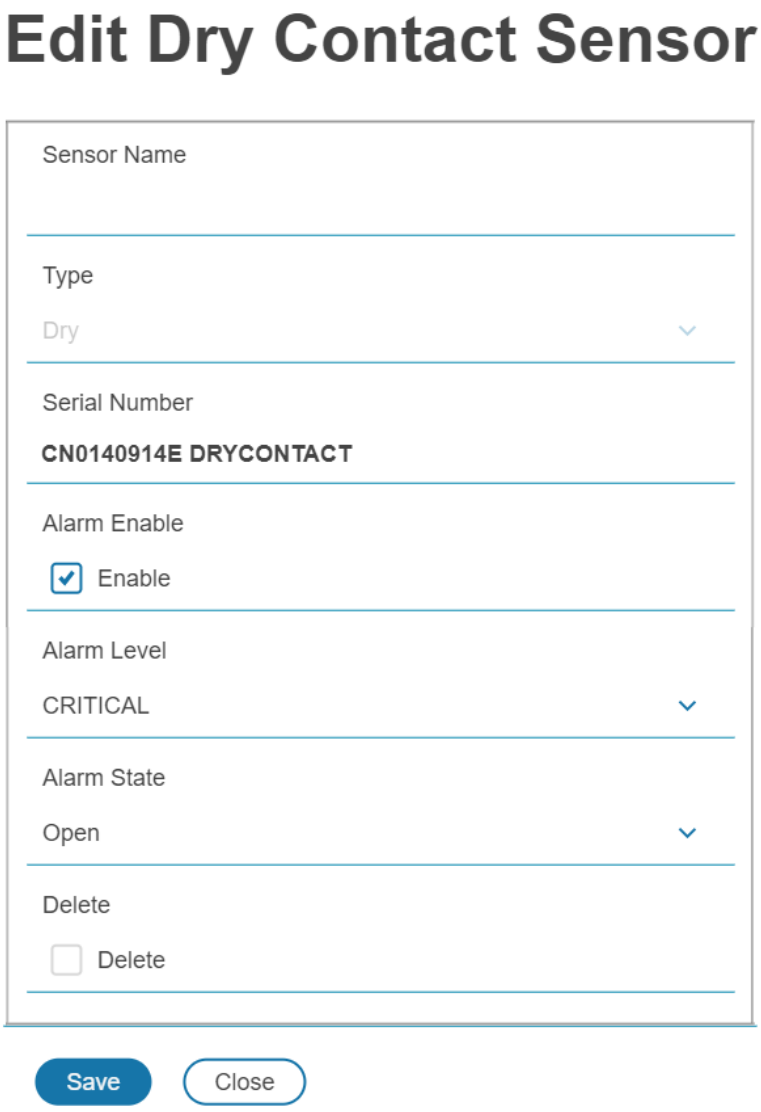


Figure 133: Dry Contact Sensor Edit dialog

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.

To prevent damage to the handle please refer to the below connection diagram and ensure you are implementing harness part numbers MA030 and ACF20.

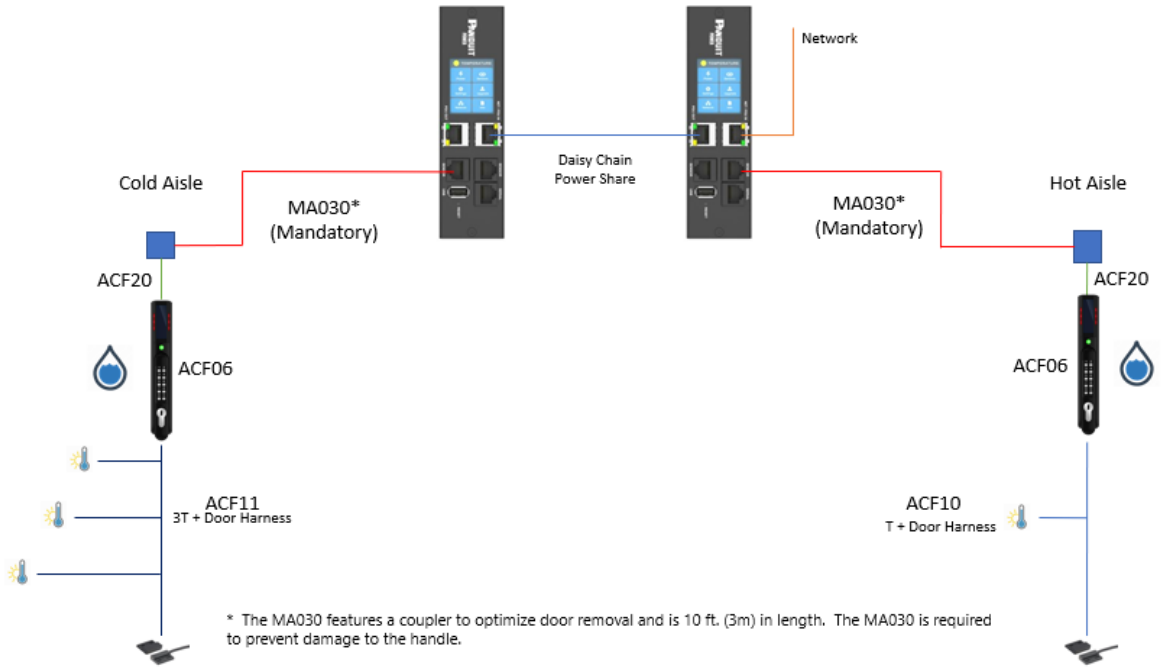


Figure 134: Connection Diagram

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 135: 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.

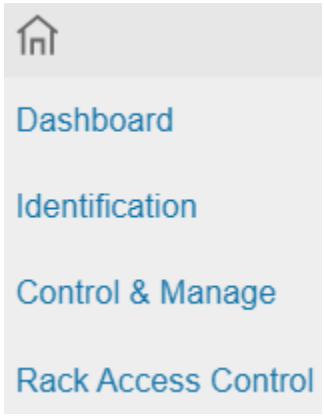


Figure 136: Rack Access Control

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.

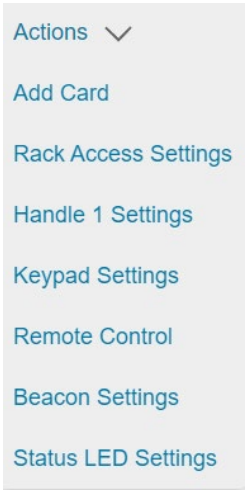


Figure 137: Rack Access Control Actions

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.

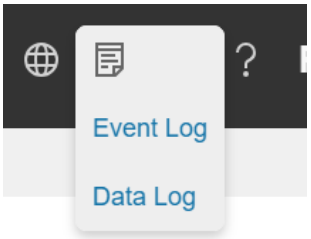


Figure 138: Event Log

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

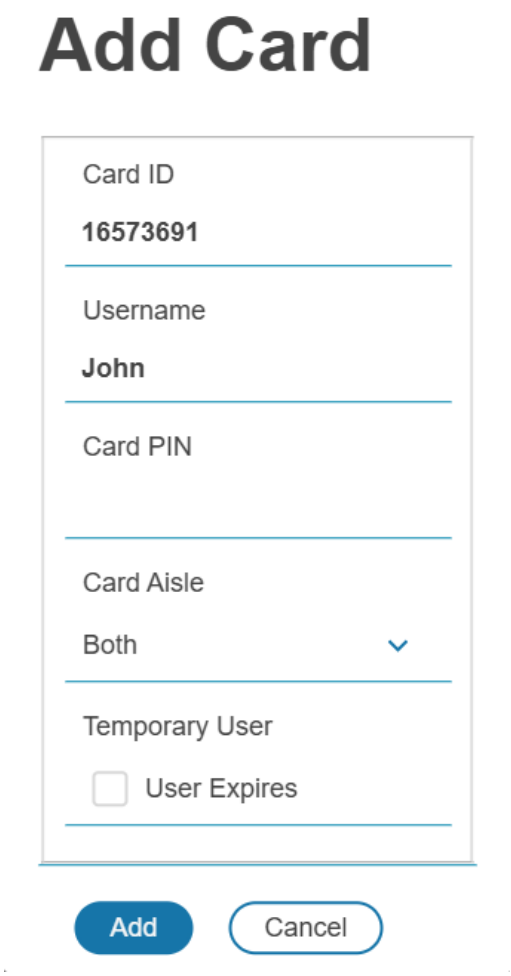


Figure 139: Add Card

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**.

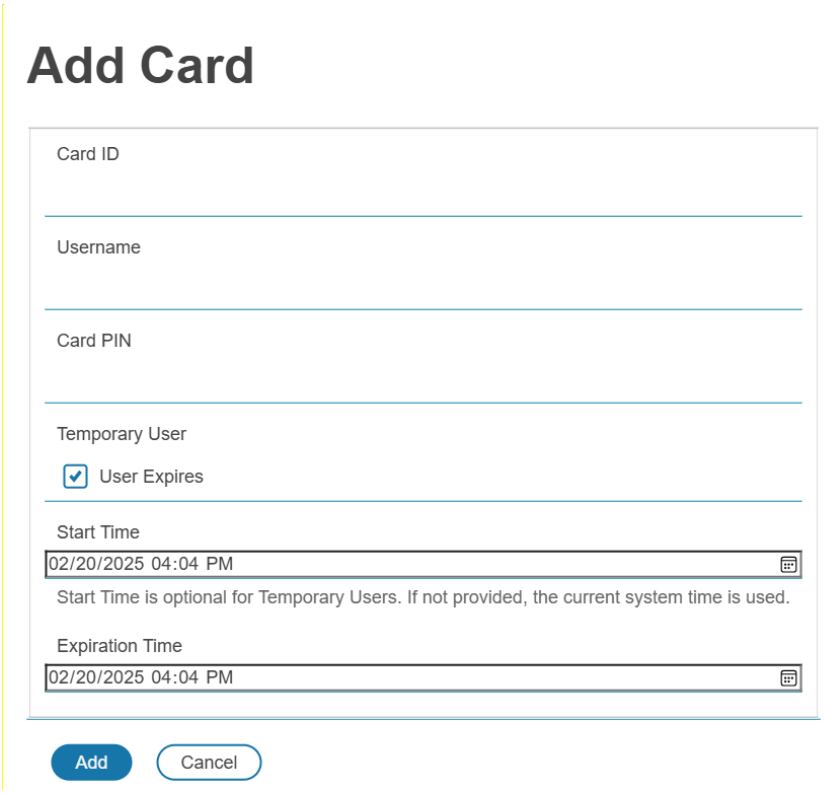


Figure 140: Add Card (Temporary User)

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.

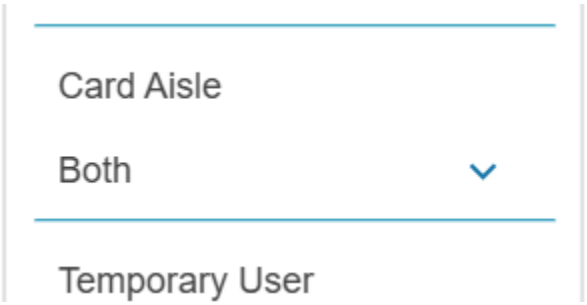


Figure 141: Add Card with Card Aisle

7. Click Add.

Editing an access user

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

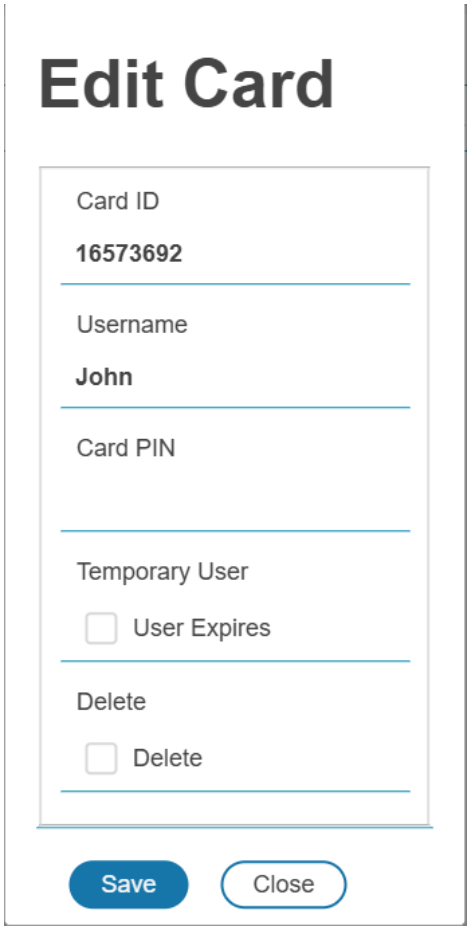


Figure 142: Edit Card

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**.

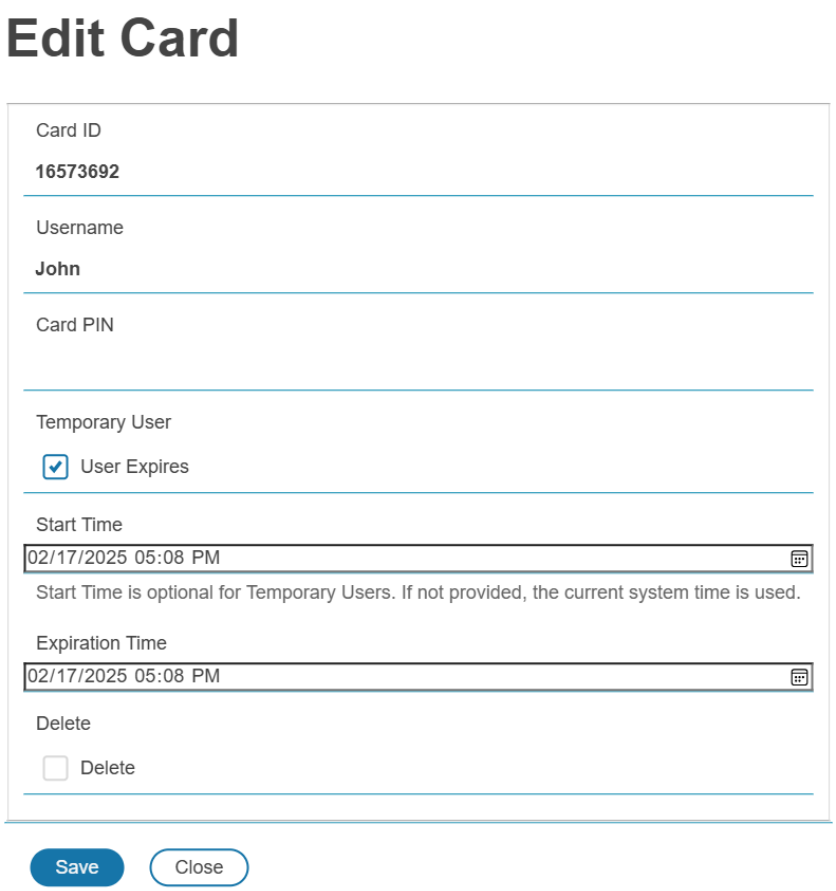


Figure 143: Edit Card (Temporary User)

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.

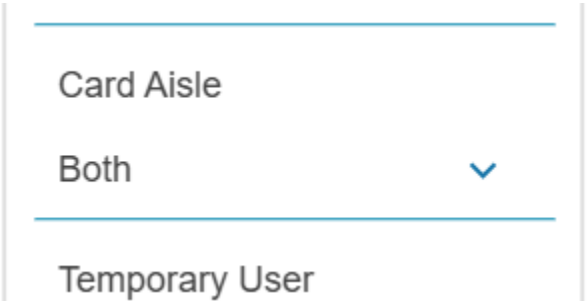


Figure 144: Add Card with Card Aisle

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.

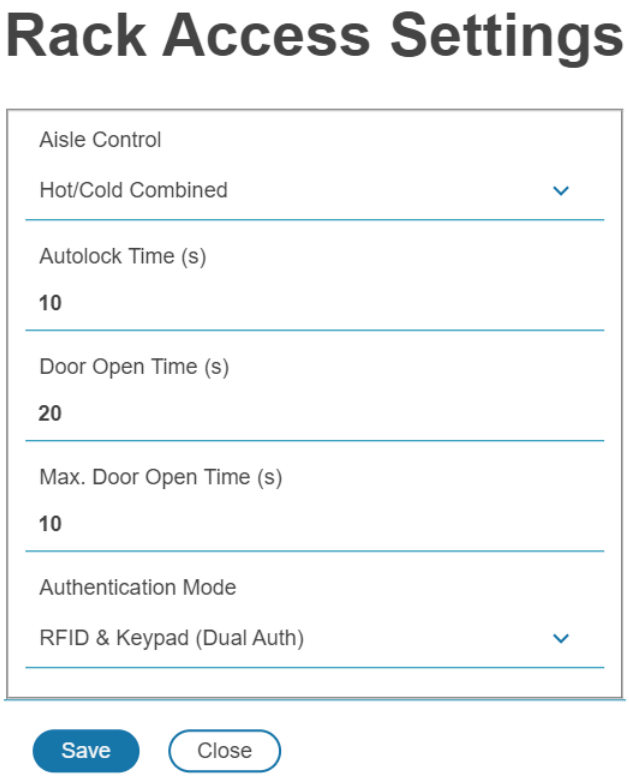


Figure 145: Rack Access Settings

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.

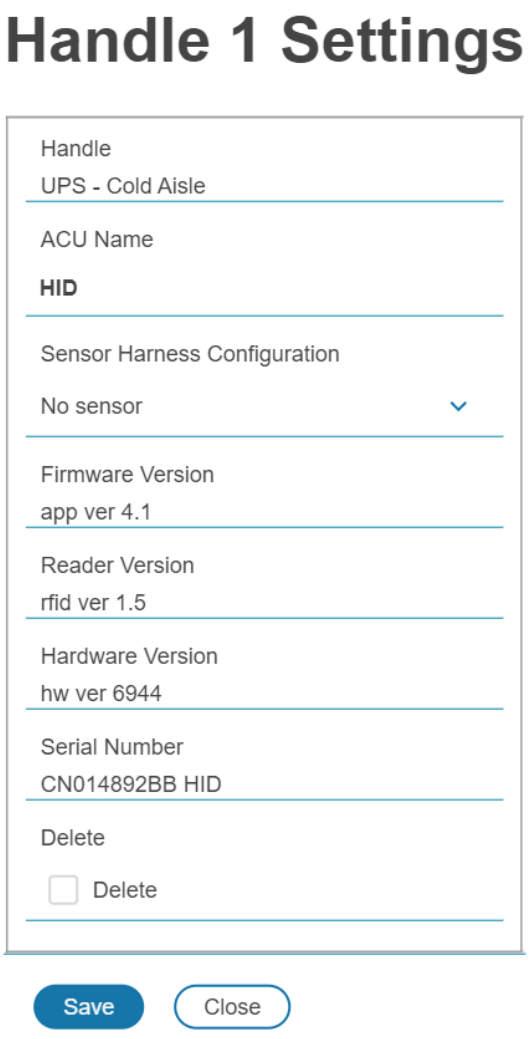


Figure 146: Handle Settings

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.

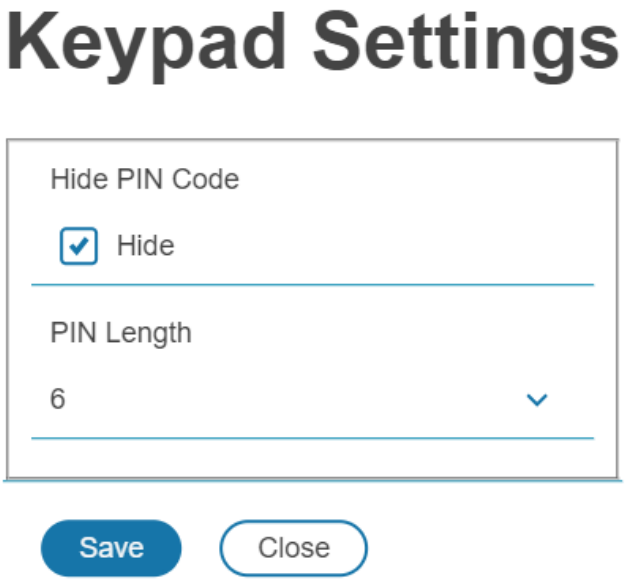


Figure 147: Keypad Settings

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.

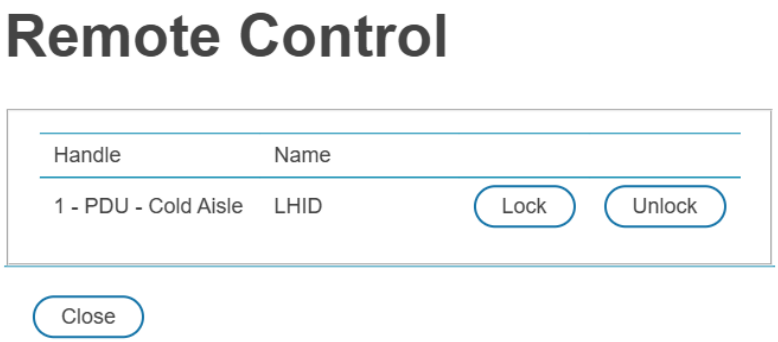


Figure 148: Remote Control

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 149: 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.

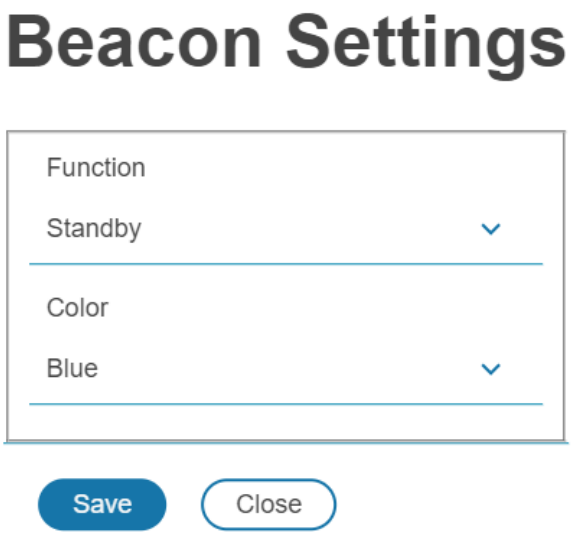


Figure 150: Beacon Settings

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.

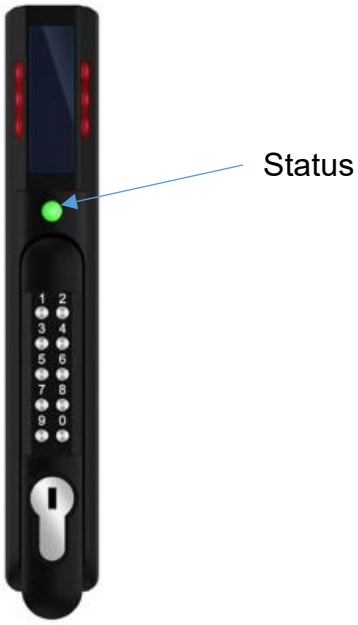


Figure 151: Status LED

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.

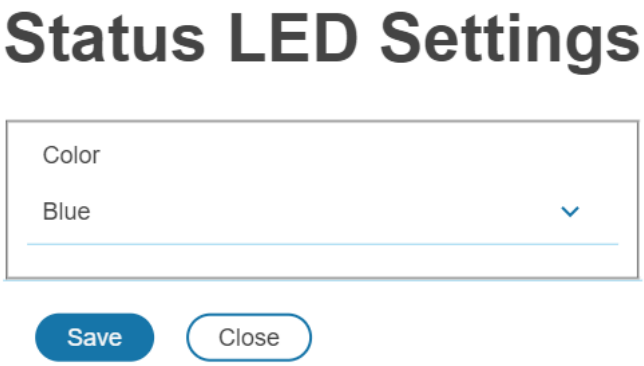


Figure 152: Status LED Settings

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.

Standards Compliance

- The product was evaluated and meets the requirements of the standard “UL 2900-1: 2023 Standard for Safety for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements, ANSI/CAN/UL 2900-1, Second Edition, Dated December 13, 2023.” Test Report Number: 4791828948-001.

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.
- The USB port provides API access to the Configuration Download, Configuration Upload and Firmware Upgrade features, triggered by button presses on the LCD screen.
- The USB Configuration Upload feature executes with Administrator Role permission.

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 reset to defaults feature deletes temporary files from a flash file system that is used to temporarily store firmware update uploads.
- The reset to defaults feature causes the SSH RSA 3072-bit private host key to be regenerated.
- The reset to defaults feature causes the SSH ED25519 256-bit private host key to be regenerated.
- If the disposed unit's “default settings” feature cannot be activated OR the user does not want event log or data log files from being extracted from the flash memory on the device THEN the device PCBAs must be physically destroyed.

Secure Erase — NIST SP 800-88 Media Sanitization

Overview

The device implements a user-triggered secure erase that sanitizes all user-provisioned data from non-volatile storage. The procedure targets two storage devices:

Storage	Location	Contents
eMMC (managed NAND)	NMC card	User configuration, logs, credentials
SPI NOR flash	PDU backplane	PDU configuration data

NIST SP 800-88 Rev. 1 Classification

NIST Special Publication 800-88 Rev. 1, *Guidelines for Media Sanitization*, defines three sanitization levels:

Level	Description
Clear	Overwrites with fixed data patterns. Protects against simple, non-invasive recovery (e.g. standard OS or file-recovery tools).
Purge	Uses media-specific commands or techniques that make recovery infeasible even with state-of-the-art laboratory techniques.
Destroy	Renders media physically unusable (shredding, incineration, etc.).

Target	NIST Level	Rationale
eMMC (NMC)	**Purge**	Uses eMMC Secure Erase + Sanitize command per Table A-8
SPI NOR (backplane)	**Clear**	No device-internal Sanitize command exists for SPI NOR; erase+overwrite is a host-level technique

A detailed explanation of each procedure and its classification follows.

eMMC Purge Procedure (NMC)

The eMMC erase uses commands defined by the JEDEC eMMC specification (JESD84-B51) which are specifically cited by NIST SP 800-88 §2.4 as appropriate for Purge-level sanitization of flash media with a flash translation layer (FTL).

Steps

1. **Device identification** — Manufacturer ID, model name, serial number, and CID are logged to create an auditable sanitization record per NIST §4.7.
2. **Secure Discard** (`blkdiscard -fs`) — Issues eMMC SECURE ERASE / SECURE TRIM commands to the flash controller. The controller marks the underlying NAND pages for physical erasure, including cells that the FTL may have remapped or reserved as spare blocks.
3. **Sanitize** (`mmc sanitize`) — Issues the eMMC SANITIZE command (CMD6, EXT_CSD[165]). This forces the controller to physically erase all blocks that were previously unmapped, discarded, or trimmed — including over-provisioned space not reachable by host reads. This is the critical step that elevates the procedure from Clear to Purge.
4. **Verification** — The entire partition is read back through the parent block device (bypassing partition alignment assumptions) and verified to be all zeros.

Why this qualifies as Purge

NIST SP 800-88 Table A-8 (Flash Memory-Based Storage Devices) states:

> *Purge: Use the device-internal Sanitize commands, if supported, or use block erase followed by the Sanitize command.*

The implementation follows this guidance exactly: secure discard followed by the eMMC Sanitize command, with post-erase verification.

SPI NOR Flash Clear Procedure (Backplane)

The backplane SPI NOR flash has no flash translation layer — host writes and erases reach the physical cells directly. There are no hidden spare blocks, wear-leveling remaps, or over-provisioned regions.

1. **Device identification** — MTD device name, JEDEC ID, manufacturer, part name, type, and size are logged.
2. **Initial erase** (`flash_erase`) — All erase blocks are set to `0xFF` (the NOR flash erased state). Verified by reading back.
3. **Random data overwrite** — A deterministic pseudorandom stream is generated using AES-256-CTR (via OpenSSL) seeded from `/dev/random`. The stream is written to the entire device, then verified by regenerating the identical stream and comparing byte-for-byte with the device contents. This pass ensures every cell has been programmed to a non-erased state, exercising the full program/erase cycle.
4. **Final erase** (`flash_erase`) — All erase blocks are erased again to `0xFF` and verified.

Why this is classified as Clear (not Purge)

NIST SP 800-88 Table A-8 defines Purge for flash storage as requiring *device-internal Sanitize commands* — firmware-level operations that reach areas the host cannot address (over-provisioned blocks, remapped sectors, etc.). SPI NOR has no such command; `flash_erase` and write operations are host-issued logical techniques that NIST classifies as Clear regardless of the number of passes.

However, the practical security posture is stronger than a minimal Clear:

- **No FTL means no hidden data.** The concern that motivates Purge for managed-NAND (eMMC, SSD) — data hiding in FTL-managed spare blocks — does not apply to SPI NOR. Every physical cell is directly addressable by the host.
- **Three verified passes.** The erase → random-overwrite → erase cycle exercises every cell through a full program/erase cycle with verification, exceeding the minimum Clear requirement of one fixed-pattern overwrite.
- **Residual charge recovery is not practical.** For modern NOR flash geometries, recovering prior cell states after a full erase cycle using laboratory techniques (e.g., scanning electron microscopy of floating-gate charge) is not considered feasible.

To achieve a formal NIST Purge classification for SPI NOR, the flash part would need to expose a vendor-specific chip-erase or security-erase command at the SPI command level (e.g., JEDEC-defined Security Register erase), which common SPI NOR parts do not implement.

Trigger and Execution Flow

```
User sets /control/mgmtModuleCtrl/secureErase
        │
        ▼
secureErase
  ├── Writes target partitions to wipe flag file
  └── Reboots device
        │
        ▼
```

```
init  (initramfs)
  ├── Detects wipe flag file
  ├── Reads partition list from configuration
  ├── Runs erase_partition.sh for each partition
  └── Logs result
```

Log and Audit Record

Each erase produces a timestamped log (`/tmp/secure-erase.log`) containing:

- Device identification (manufacturer, model, serial / JEDEC ID)
- Each erase step and its pass/fail status
- Verification results

These fields satisfy the NIST SP 800-88 §4.7 recommendation to record sufficient detail to verify that sanitization was performed correctly and to identify the specific media instance.

Limitations

- **Firmware / boot partitions are not erased** — The procedure targets user-data partitions only. The NMC boot partitions and the backplane factory area are intentionally preserved so the device remains bootable.
- **Wear-leveled spare blocks (eMMC)** — The eMMC Sanitize command is designed to cover spare/over-provisioned blocks, but ultimate coverage depends on the controller implementation.

References

- NIST SP 800-88 Rev. 1, *Guidelines for Media Sanitization*, December 2014. https://doi.org/10.6028/NIST.SP.800-88r1
  - §2.4 — Trends in sanitization (flash-specific considerations)
  - §4.7 — Verification and documentation
  - Table A-8 — Flash Memory-Based Storage Devices (Clear / Purge / Destroy)
- JEDEC JESD84-B51 — eMMC Electrical Standard, §6.6.40 (Sanitize), §6.6.10 (Secure Erase / Secure Trim)

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.

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, TACACS+) 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
- TACACS+

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 3072-bit private host key the first time the product starts up.
- The product generates a random SSH ECDSA 256-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 openssl AES password encryption formats.
- If the private key is contained in a .pfx or .p12 file, you may convert that to the password encrypted PEM format using openssl. Please review the openssl documentation for more information. Example:
  - openssl pkcs12 -in [yourfile.p12] -nocerts -nodes -passin pass:[input_password] | openssl rsa –aes256 -out [privatekey.pem] -passout pass:[new_password]
- The product uses TLS 1.2 or TLS 1.3 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_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
  - Cipher Spec: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
  - Cipher Spec: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
  - Cipher Spec: TLS_AES_256_GCM_SHA384 (0x1302)
  - Cipher Spec: TLS_AES_128_GCM_SHA256 (0x1301)
- The product uses TLS 1.2 or TLS 1.3 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_RSA_WITH_AES_128_CBC_SHA (0x002f)
  - Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
  - Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)
  - Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
  - Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
  - Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
  - Cipher Suite: TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)
  - Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
  - Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
  - Cipher Suite: TLS_AES_128_CCM_SHA256 (0x1304)
  - Cipher Suite: TLS_AES_128_CCM_8_SHA256 (0x1305)

- Cipher Suite: TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004)
- Cipher Suite: TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005)
- Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
- Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
- Cipher Suite: TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e)
- Cipher Suite: TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f)
- Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
- Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
- Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)
- Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)
- Cipher Suite: TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (0xc025)
- Cipher Suite: TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026)
- Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)
- Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
- Cipher Suite: TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 (0xc029)
- Cipher Suite: TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 (0xc02a)
- Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
- Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
- Cipher Suite: TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02d)
- Cipher Suite: TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02e)
- Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
- Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
- Cipher Suite: TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 (0xc031)
- Cipher Suite: TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 (0xc032)
- Cipher Suite: TLS_RSA_WITH_ARIA_128_CBC_SHA256 (0xc03c)

- Cipher Suite: TLS_RSA_WITH_ARIA_256_CBC_SHA384 (0xc03d)
- Cipher Suite: TLS_ECDHE_ECDSA_WITH_ARIA_128_CBC_SHA256 (0xc048)
- Cipher Suite: TLS_ECDHE_ECDSA_WITH_ARIA_256_CBC_SHA384 (0xc049)
- Cipher Suite: TLS_ECDH_ECDSA_WITH_ARIA_128_CBC_SHA256 (0xc04a)
- Cipher Suite: TLS_ECDH_ECDSA_WITH_ARIA_256_CBC_SHA384 (0xc04b)
- Cipher Suite: TLS_ECDHE_RSA_WITH_ARIA_128_CBC_SHA256 (0xc04c)
- Cipher Suite: TLS_ECDHE_RSA_WITH_ARIA_256_CBC_SHA384 (0xc04d)
- Cipher Suite: TLS_ECDH_RSA_WITH_ARIA_128_CBC_SHA256 (0xc04e)
- Cipher Suite: TLS_ECDH_RSA_WITH_ARIA_256_CBC_SHA384 (0xc04f)
- Cipher Suite: TLS_RSA_WITH_ARIA_128_GCM_SHA256 (0xc050)
- Cipher Suite: TLS_RSA_WITH_ARIA_256_GCM_SHA384 (0xc051)
- Cipher Suite: TLS_ECDHE_ECDSA_WITH_ARIA_128_GCM_SHA256 (0xc05c)
- Cipher Suite: TLS_ECDHE_ECDSA_WITH_ARIA_256_GCM_SHA384 (0xc05d)
- Cipher Suite: TLS_ECDH_ECDSA_WITH_ARIA_128_GCM_SHA256 (0xc05e)
- Cipher Suite: TLS_ECDH_ECDSA_WITH_ARIA_256_GCM_SHA384 (0xc05f)
- Cipher Suite: TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256 (0xc060)
- Cipher Suite: TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384 (0xc061)
- Cipher Suite: TLS_ECDH_RSA_WITH_ARIA_128_GCM_SHA256 (0xc062)
- Cipher Suite: TLS_ECDH_RSA_WITH_ARIA_256_GCM_SHA384 (0xc063)
- Cipher Suite: TLS_RSA_WITH_AES_128_CCM (0xc09c)
- Cipher Suite: TLS_RSA_WITH_AES_256_CCM (0xc09d)
- Cipher Suite: TLS_RSA_WITH_AES_128_CCM_8 (0xc0a0)
- Cipher Suite: TLS_RSA_WITH_AES_256_CCM_8 (0xc0a1)
- Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CCM (0xc0ac)
- Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CCM (0xc0ad)
- Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8 (0xc0ae)

    - Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8 (0xc0af)
- The product provides a SSH server with these algorithms to communicate with SSH clients:
    - Key exchange algorithms:
        - curve25519-sha256
        - curve25519-sha256@libssh.org
        - ecdh-sha2-nistp521
        - ecdh-sha2-nistp384
        - ecdh-sha2-nistp256
        - diffie-hellman-group14-sha256
        - kexguess2@matt.ucc.asn.au
        - kex-strict-s-v00@openssh.com
    - Host key algorithms:
        - rsa-sha2-256 (2048-bit)
    - Encryption algorithms:
        - chacha20-poly1305@openssh.com
        - aes128-ctr
        - aes256-ctr
    - MAC algorithms:
        - hmac-sha2-256

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.

Logging

- Event log messages and alarm messages sent to the Event Log, Email and SNMP trap may contain containing the IP address and username of the user performing the action.
- The data log and event log produce a “Log is downloaded by user” message each time the log has changed and a new viewer has accessed it.

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.
- The TACACS+ 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 that 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.

Protocols

- The product provides mDNS (UDP port 5353) and LLMNR (UDP port 5355) to enable MacOS and Windows to easily connect to the device via “pdu-<macaddress>.local”. If a hostname is configured, the hostname is used instead of “pdu-<macaddress>”.

Secure deployment

To maintain the highest level of security, Panduit recommends:

- Deploy the product in a physically secured location, preferably within a locked cabinet inside a secured datacenter.
- Do not run Serial, Sensor or USB cables through insecure areas as these interfaces do not provide confidentiality (encryption).

Configure the NMC regarding the following settings:

NTP

Configure a trusted Network Time Protocol server to allow accurate time stamps to be used in the Event Log and Notifications.

Upload HTTPS Certificate and Private Key

Certificates ensure authenticity of the confidential encrypted connection to the device’s HTTPS server. It is recommended that an X.509 Server 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**

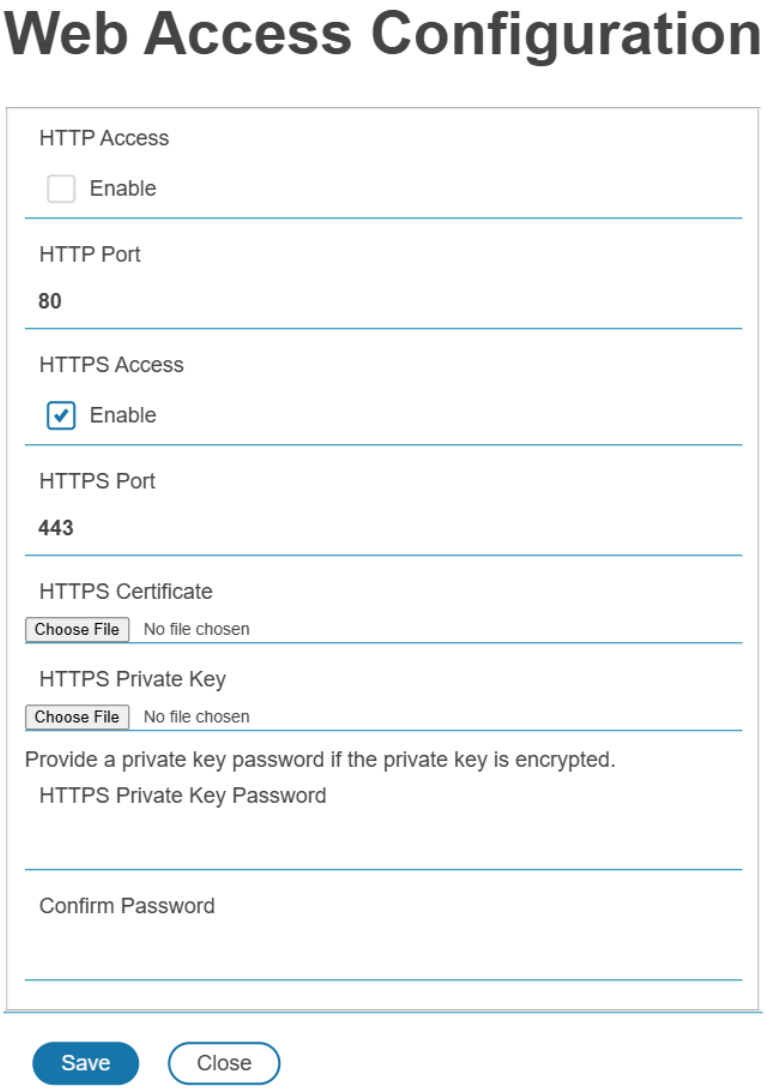


Figure 153: SSL Certificate Load Screen

Use SNMPv3c

The 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-512 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.

The default setting is to have the USB port enabled. Using the USB port management operations require two physical operations: inserting a USB flash drive and choosing the requested operation on the LCD screen interface. The customer may disable the USB configuration upgrade, downgrade and firmware upgrade features if these are not desired. To disable:

- serial CLI or SSH: login and then “write config/screen/usbScreen 0”.
- web UI: navigate to Settings / System Management / LCD Configuration, click the pencil icon, remove the checkbox from USB Port Enable, and click the Save button.

Review Session management

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

Automatic Firmware Upgrade

Panduit updates the firmware for our products. Refer to the “Appendix A: Firmware Update Procedure”. Configure Automatic Firmware Upgrade to point to a local server to automate keeping PDUs up to date. Refer to the “Auto Update” chapter for more details. Ensure only authorized personnel can update the resources stored at the configured Firmware URI and Config URI.

TLS Server Certificate Verification

Protocols implemented by the product may include optional TLS server certificate verification. Make sure the TLS configuration meets your security requirements. It is best practice to configure a “Server Certificate” (the server’s certificate or a trusted certificate authority) and to enable the appropriate "Verify Certificate", "Verify Server Certificate", or "Verify Server" option. Server certificate verification allows the NMC to verify the authenticity of the configured server.

TLS Client Certificate and Client Private Key

Protocols implemented by the product may include the ability to present an optional TLS client certificate. Make sure the TLS configuration meets your security requirements. It is best practice to configure a “Client Certificate” and “Client Private Key” and enable the associated “Provide Client Certificate” option. Presenting a certificate allows the configured server to verify the authenticity of the configured NMC.

Security Response

To report security incidents, please contact “Technical Support” as described in the Support chapter.

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 Receivers
- **Return Material Authorizations (RMAs)**

Email (**preferred**): SystemSupport@panduit.com
Ph (Americas): 1-866-721-5302
Ph (EMEA): +44-1291-674661

To expedite your experience when **Global Post Sale Support** please include (or have ready on the phone call) the following information in your request (mandatory):

Purchase Order Number:
Distributor Name (if applicable):
Invoice Date:
End User Company Name:
Site Contact Full Name:
Site Contact Phone Number:
Site Contact E-mail address:
Site Delivery Address:

Complete Panduit Part #:
Total Quantity Affected:
Fault Description (be as detailed as possible):

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

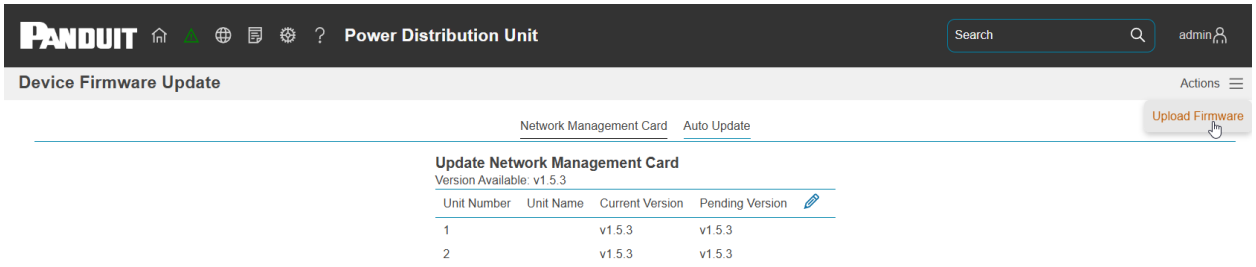
Watts

Appendix A: Firmware Update Procedure

Manual Update

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'.

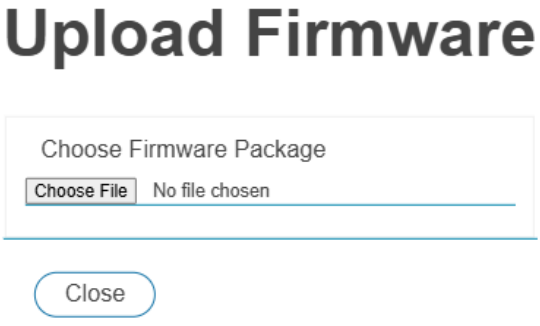


Figure 154: Upload

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.

Auto Update

The Auto Update feature simplifies in-field maintenance by enabling periodic updates to both configuration files and firmware. Unlike SZTP, which provisions devices only once during initial startup, Auto Update operates continuously during runtime.

It checks the configured HTTPS URIs for updated firmware and configuration files based on the defined update frequency. For the PDU to detect changes, the HTTPS server must update the HTTP Last-Modified header associated with the file—this signals that a new version is available.

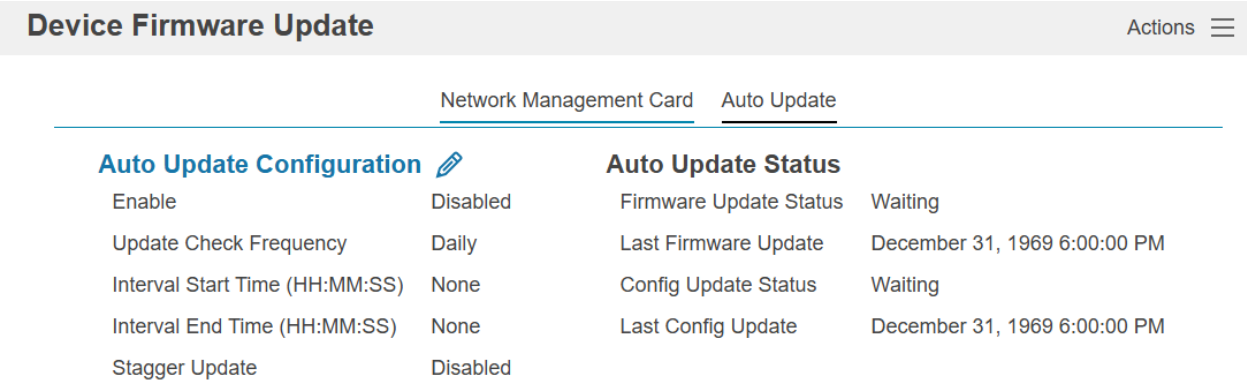


Figure 155: Auto Update

Auto Update Configuration

The Auto Update Configuration includes settings for enabling SZTP and setting network locations, server verification, and update patterns. Follow the steps below to set up Auto Update:

1. Select the pencil icon next to Auto Update Configuration.
2. Click the box next to **Enable**.
3. Enter the HTTPS URI of the firmware file into **Firmware URI**.
4. Enter the HTTPS URI of the configuration file into **Config URI**.
5. Click on the dropdown menu under **Update Check Frequency** to set how often Auto Update checks for new files.

6. To enable authentication of a specific server, click the checkbox under **Verify Certificate**, then click on the Server Certificate and add the certificate for the https server.
7. Configure the window of time each day when Auto Update should check for updates. Enter the start of the window under **Interval Start Time**. Enter the end of the window under **Interval End Time**.
8. Click the box next to **Stagger Update** to perform the update at a random time between the interval start and interval end times. This will help with network traffic and server loading bursts if you have many PDUs.
9. If you would like to check for updates at once, check the **Update Now** box.

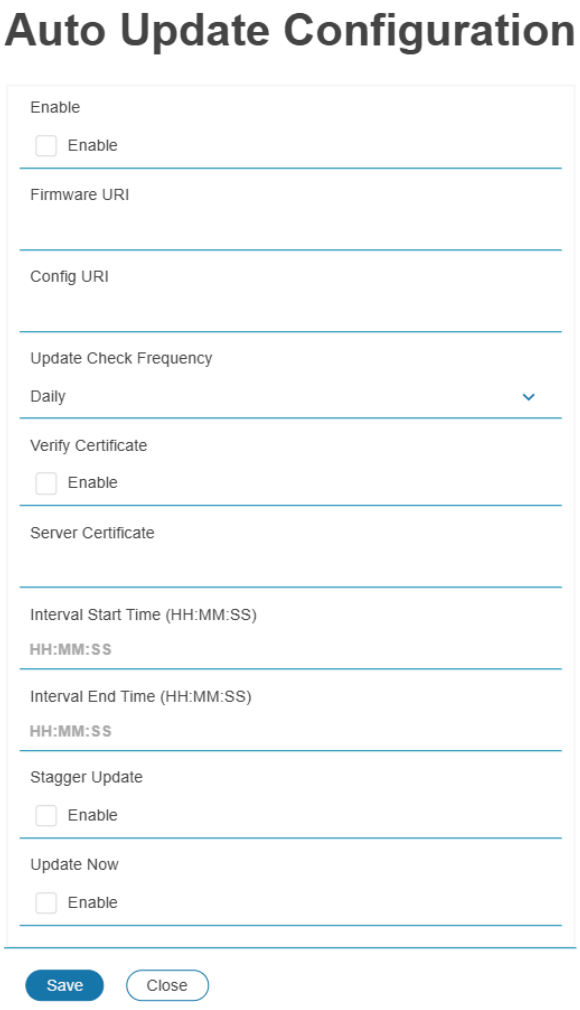


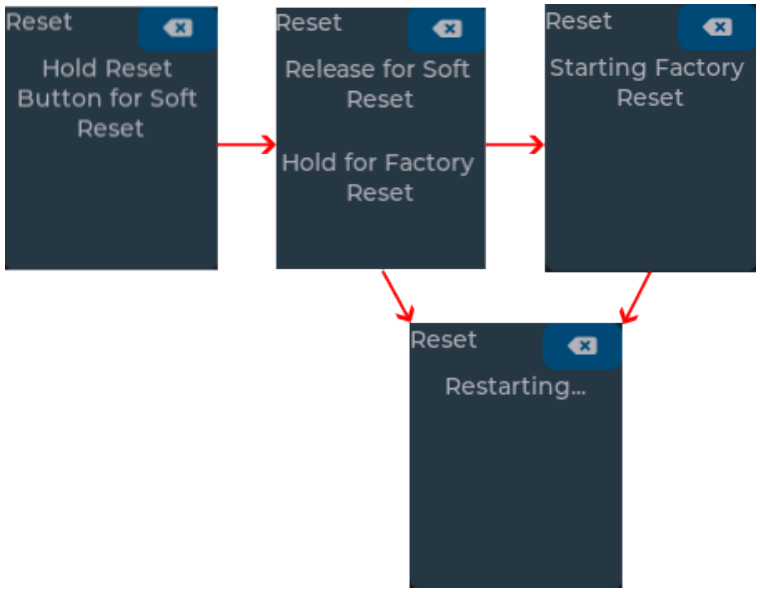
Figure 156: Auto Update Configuration

Appendix B: System Reset or Password Recovery

The EL2P Controller supports three reset levels, each providing a different degree of system recovery.

Level 1 – Soft Reset (NMC Reboot)
Press and hold the **RESET** button on the front of the NMC for **2 seconds**.
This performs a soft system reset when the button is released, rebooting the NMC controller while **retaining all existing configurations**.

Level 2 – Factory Reset (NMC Default)
Press and hold the **RESET** button for **at least 8 seconds, but no longer than 20 seconds**. The factory reset begins at the 8 second mark not at the release of the button. This restores the NMC controller to factory default settings, **erasing all configurations**, including usernames and passwords. The NMC will automatically restart upon completion. See section Logging in to the Web Interface for default credentials.



Level 3 – Full System Reset (NMC)
In a rare case, if a controller is fully locked up (unresponsive); Press and hold the **RESET** button for **30 seconds**. This forces a **reset to the NMC's internal microcontroller**, providing a potential recovery path.

User Password Recovery:

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**.

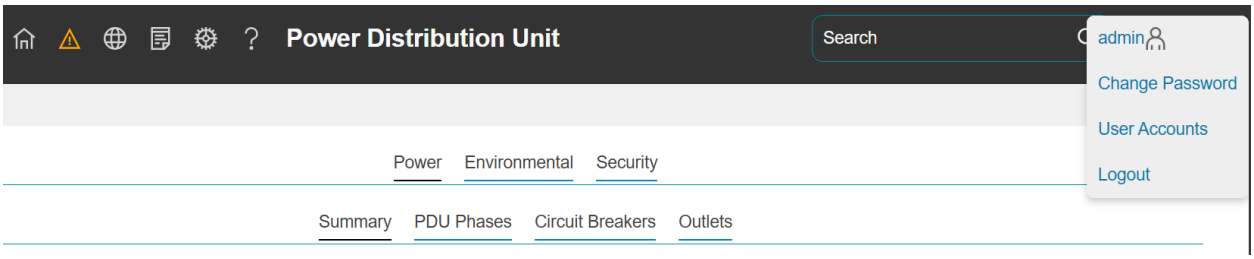


Figure 157: User Accounts from the User Icon

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

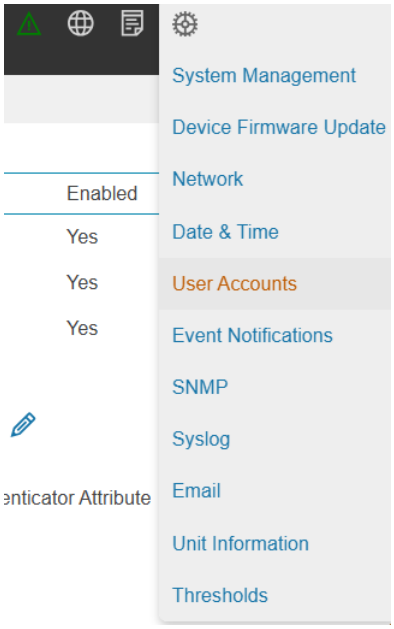


Figure 158:User Accounts from Gear Icon

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.

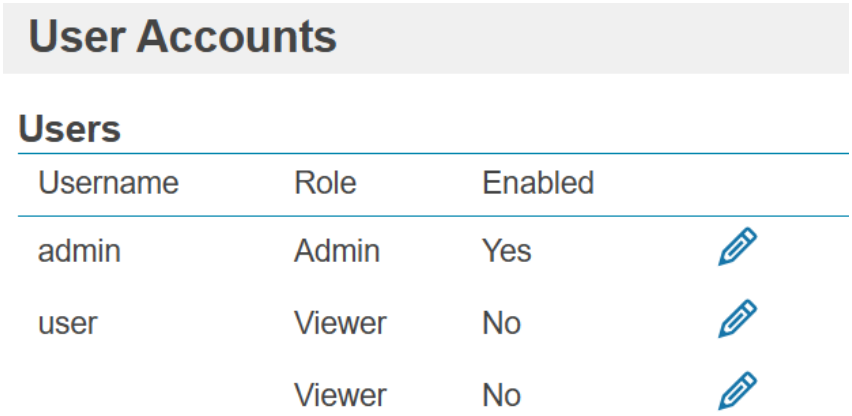


Figure 159: Users Table

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.

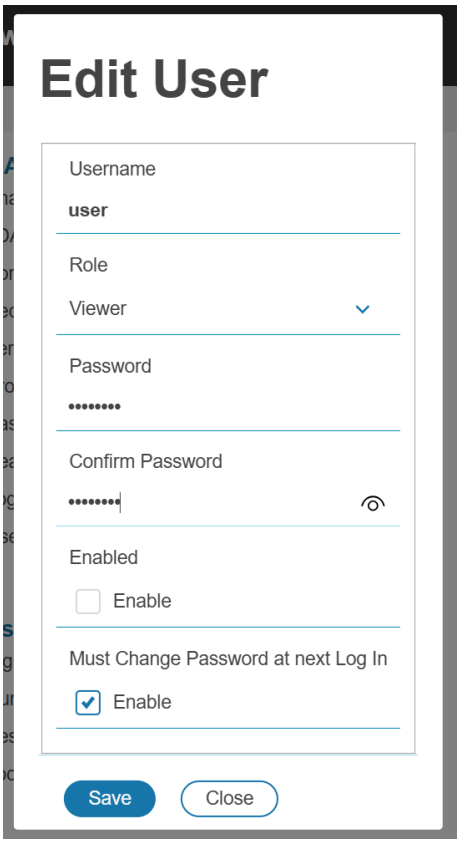


Figure 160: Edit User Screen

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**.

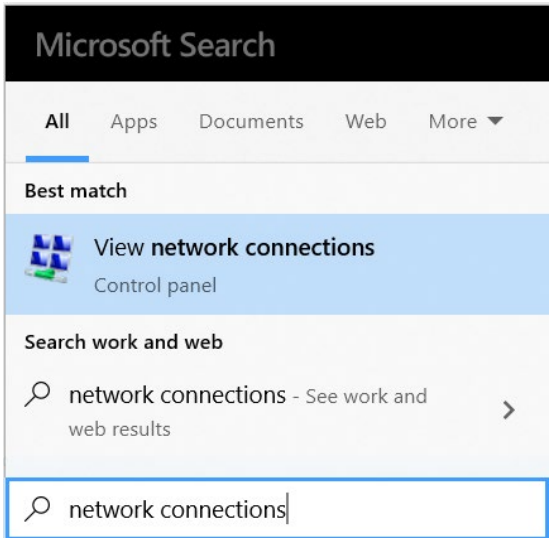


Figure 161: View network Connections

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

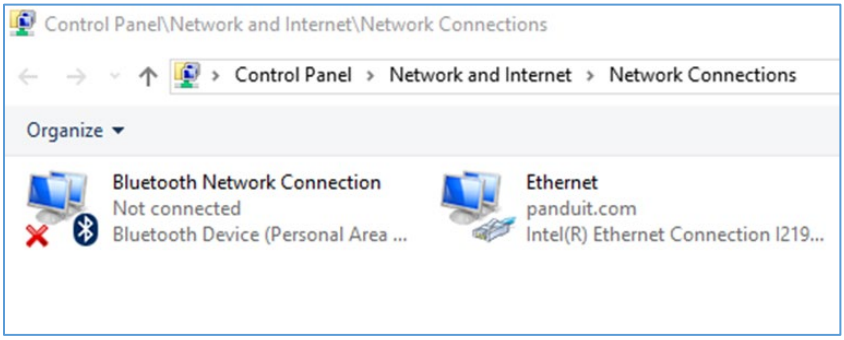


Figure 162: Properties

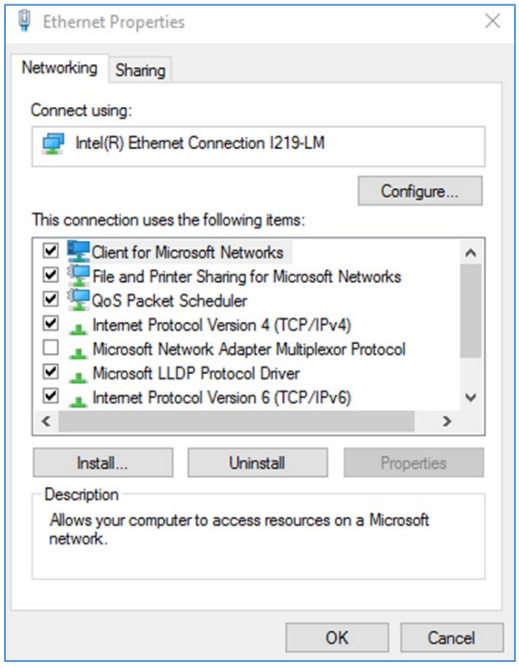


Figure 163: Ethernet Properties

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

Figure 164: 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

Below is an *example* of an industry standard USB console cable:

- 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

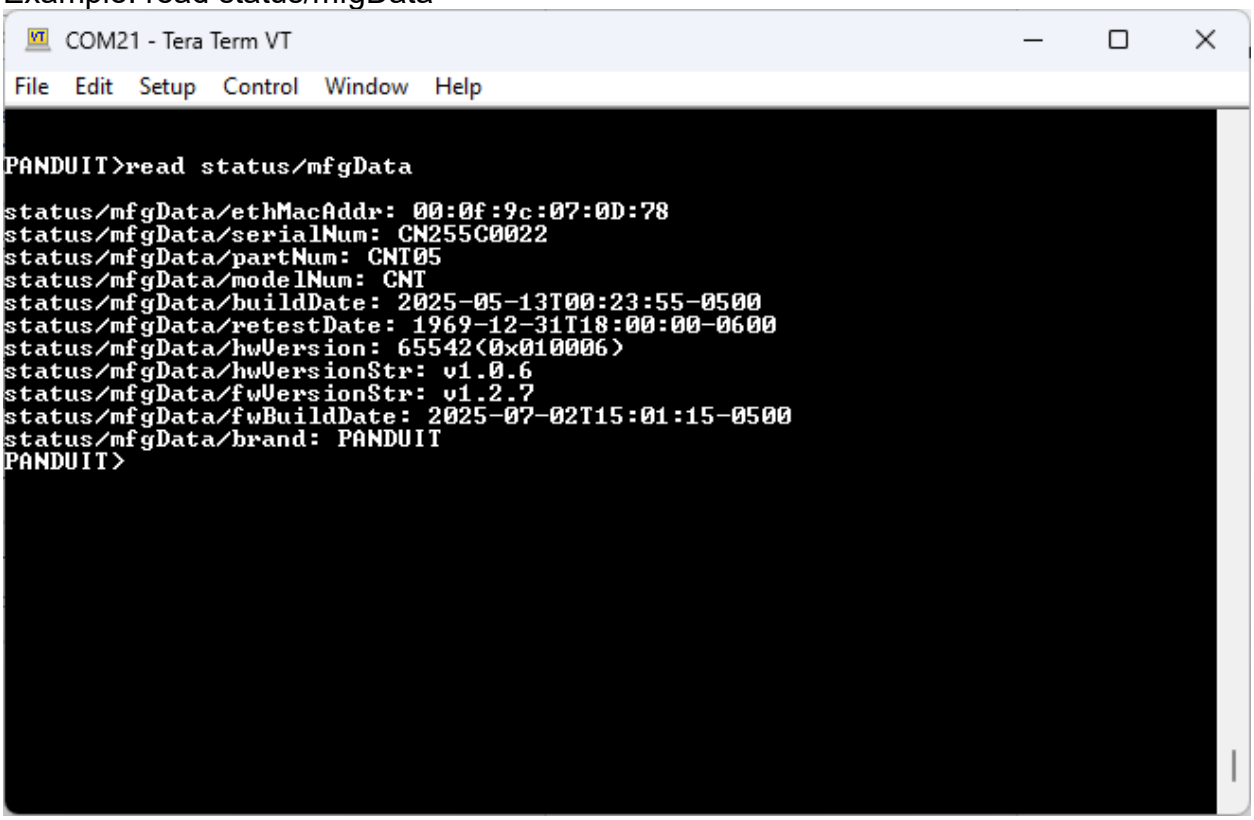


Figure 165: Reading from CLI

- **write**

  Set a value to an individual item in the data model

  Example: write config/systemInfo/systemName DC1-PDUA1

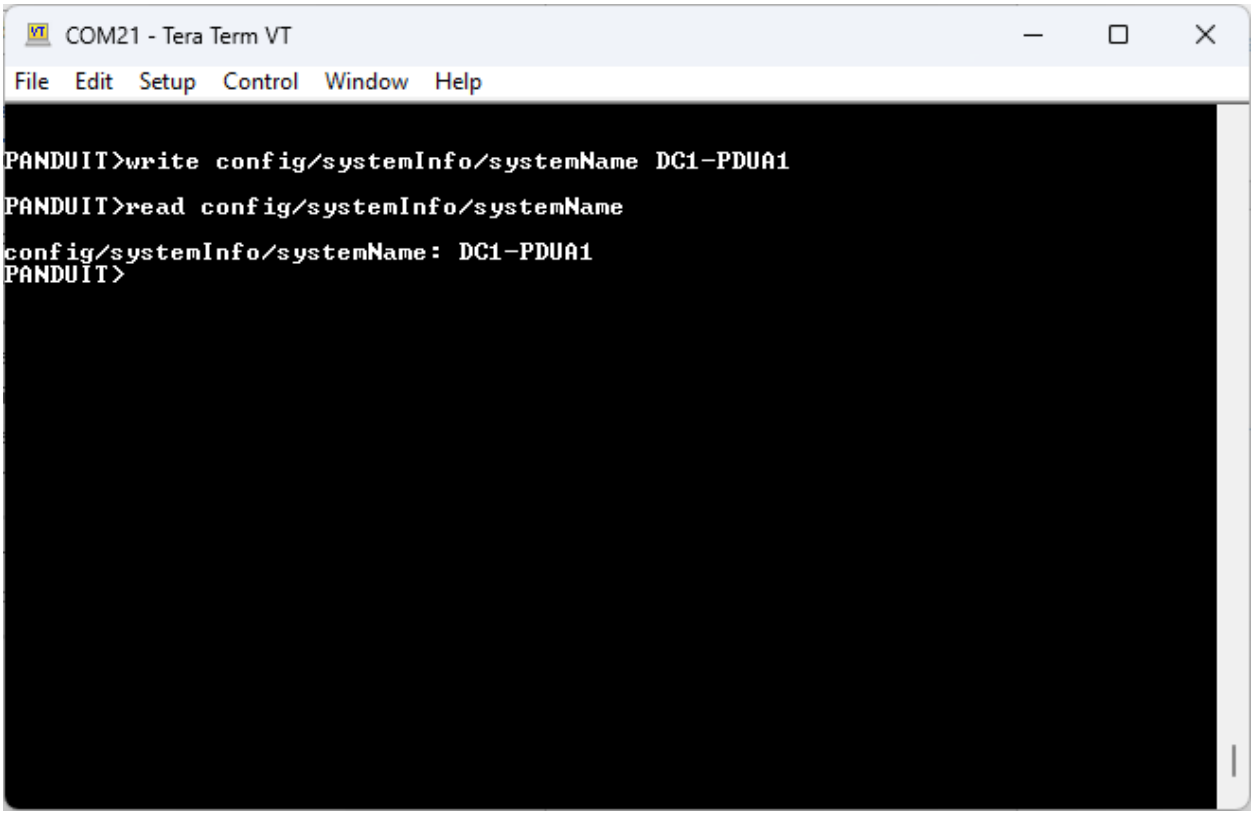


Figure 166: Writing from CLI

- **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. To remedy this, the PDU supports Secure Zero Touch Provisioning (SZTP), which is 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.

Getting Started with SZTP

SZTP requires the following:

1) A Windows server to run the bootstrap software.
2) Network configuration changes for DHCP and DNS for non-local network use.
3) Certificates for SZTP.
4) SZTP Vouchers from Panduit.
5) EL2P Firmware version 1.4.1 or higher.

Summary of SZTP Setup

Step 1: Create or obtain a CA certificate and a server certificate / private key. Make sure the server certificate contains a name that is resolvable with DNS to the Windows server.

Step 2: Request Signed Vouchers from systemsupport@panduit.com.

Step 3: Install the Panduit SZTP Bootstrap software on a Windows Server.

Step 4: Configure your network DHCP server to provide the SZTP DHCP option.

Step 5: Create configuration files for each PDU.

Step 6: Connect new PDUs to the network. SZTP will automatically update and configure each PDU that has a voucher on the server. If the PDU was previously connected or logged into, default the settings to initiate SZTP.

Certificate creation and network configuration will require the assistance of your network administrator. For detailed explanation of SZTP configuration steps, read the sections below and refer to Appendix J: SZTP Bootstrap Server Installation and Appendix I: SZTP Server Discovery (via DHCP or mDNS) for more information.

Certificate Configuration
SZTP requires configuration of at least a single CA certificate that will function as a trust anchor for authentication of the bootstrap server. You must send the trust anchor certificate to Panduit as part of a voucher request.

- The trust anchor may be a root CA or an intermediate CA certificate, not the bootstrap server certificate itself.
- An existing corporate root of trust, or intermediate CA may be used.
- The bootstrap server certificate must include a chain back to the trust anchor.
- The “Trust Anchor” is referred to as the “pinned-domain-cert" once it has been embedded in the voucher.

Voucher Request
Vouchers provided by the bootstrap server to the Panduit PDU prove ownership of the PDU. Provide the following items when requesting vouchers from Panduit:

- PDU serial numbers
- Proof of ownership of PDUs
- Trust anchor certificate

Request SZTP ownership vouchers from systemsupport@panduit.com

SZTP Operation
An out-of-the-box Panduit PDU with a voucher and configuration on the SZTP bootstrap server will now auto-provision itself when powered on and plugged into the network.

SZTP is designed to be run once on each PDU and will disable itself if any of the following happens:

- Successful bootstrapping occurs (via SZTP)
- There is login activity.

- The PDU becomes a Linked Unit in a Daisy Chain.

If you would like to use SZTP after the PDU has disabled it, you must factory reset the PDU. For periodic firmware updates, use the Auto Update feature.

Appendix H: Zero Touch Provisioning (1-Touch ZTP)

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. To remedy this, the PDU supports Zero Touch Provisioning (ZTP), which is a bootstrapping strategy enabling devices to obtain bootstrapping data with no installer action beyond physical placement and connecting network and power cables.

To maintain the highest level of security, Panduit Zero Touch Provisioning (ZTP) is now 1-Touch provisioning. For secured networks where servers can be trusted, 1-Touch provisioning is an automated method that does not require vouchers from Panduit. To enable ZTP, the user must make a physical acknowledgement on the local display.

Panduit's 1-Touch Provisioning follows the RFC 8572 except for the manufacturer voucher requirement.

Getting Started with 1-Touch ZTP

ZTP requires the following:

1) A Windows server to run the bootstrap software.
2) Network configuration changes for DHCP and DNS for non-local network use.
3) EL2P Firmware version 1.5.3 or higher

Summary of 1-Touch ZTP Setup

Step 1: Install the Panduit SZTP Bootstrap software on a Windows Server.

Make sure to enable 1-Touch in the configuration. See Appendix J: SZTP Bootstrap Server Installation for more information.

Step 2: Configure your network DHCP server to provide the SZTP DHCP option.

See Appendix I: SZTP Server Discovery (via DHCP or mDNS) for more information.

Step 3: Create configuration files for each PDU.

See Appendix J: SZTP Bootstrap Server Installation for more information.

Step 4: Connect new PDUs to the network. If the PDU was previously connected or logged into, default the settings to initiate SZTP.

Step 5: Enable ZTP in each PDU

1) Touch the settings icon on the LCD
2) Touch the “Enable ZTP” Button

The PDU will now auto-provision itself.

Appendix I: SZTP Server Discovery (via DHCP or mDNS)

The PDU will discover the SZTP bootstrap server either via a DHCP option, or via mDNS (locally).

mDNS

If the PDU and SZTP bootstrap server are on the same local network, you can configure the bootstrap server to advertise itself to the PDU via an mDNS service, without needing to modify your DHCP configuration. To do so, during installation of the bootstrap server, check “Enable mDNS”, and fill in the hostname of the server.

This method requires EL2P Firmware version 1.6.x or higher.

Note that it may take up to 6 minutes for the PDU to detect the bootstrap server via mDNS and connect to it.

DHCP Option

In all other cases, DHCP is used to provide a redirect URI to the bootstrap server. Redirect information may be provided either via DHCPv4 (option 143) or DHCPv6 (option 136). The bootstrap information must be provided as a “URI” structure, per RFC8572 sections 8.2 and 8.3.

uri-length	URI

- uri-length: 2 octets long; specifies the length of the URI data.
- URI: URI of the SZTP bootstrap server.

The URI provided by DHCP must be in the form "https://<bootstrap hostname>[:<port>]".

Depending on your DHCP server software, setting up the SZTP URI option using the correct format may involve writing the option value in hex. For example, a boot strap server with the default HTTPS port 443 at sztpbootstrap.panduitlabs.com would have the following URI:

https://sztpbootstrap.panduitlabs.com

which encoded in ASCII hexadecimal is:

68 74 74 70 73 3A 2F 2F 73 7A 74 70 62 6F 6F 74 73 74 72

61 70 2E 70 61 6E 64 75 69 74 6C 61 62 73 2E 63 6F 6D

There are 37 bytes which is 0x0025 in hexadecimal, giving us the option value of:

00 25 68 74 74 70 73 3A 2F 2F 73 7A 74 70 62 6F 6F 74 73 74

72 61 70 2E 70 61 6E 64 75 69 74 6C 61 62 73 2E 63 6F 6D

On a Windows DHCP Server:

1) Open the DHCP Console.
2) Right click on IPv4 and select Set Predefined Options
3) Click Add and enter the configuration information:
    a. Name: SZTP
    b. Data type: Binary
    c. Code: 143
    d. Description: SZTP Redirect URI
4) Click OK to save the new option.
5) Navigate to the desired scope under the IPv4 tree.
6) Right-click Scope Options and select Configure Options
7) Check the box on the 143 SZTP option.
8) Enter the hexadecimal data for the URI of the server where you will run the Panduit Bootstrap software.

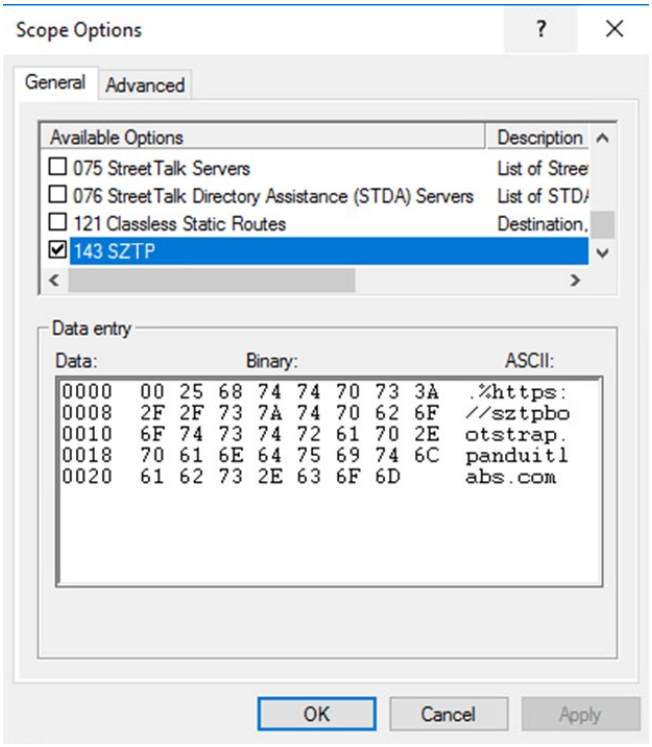


Figure 167: Windows DHCP Config

Appendix J: SZTP Bootstrap Server Installation

Panduit Bootstrap software runs on a Windows computer. It provides bootstrapping information and firmware images for Panduit PDUs using SZTP.

1) Extract the Panduit Bootstrap software from the PDU firmware package found under support at https://www.panduit.com/pdu-support
2) Double click on the installer.
3) Read and accept the Panduit EULA

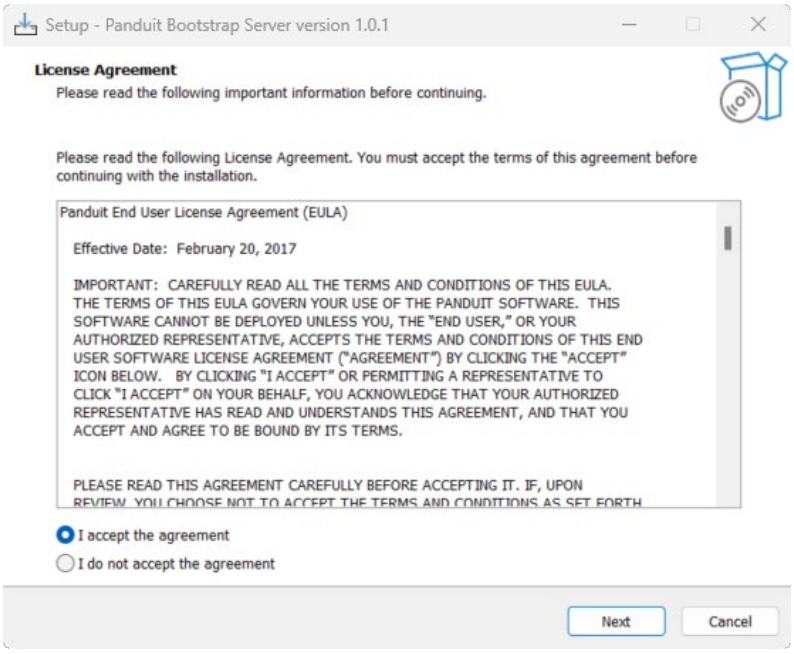


Figure 168: SZTP License

4) Choose the software installation folder, the default is recommended.

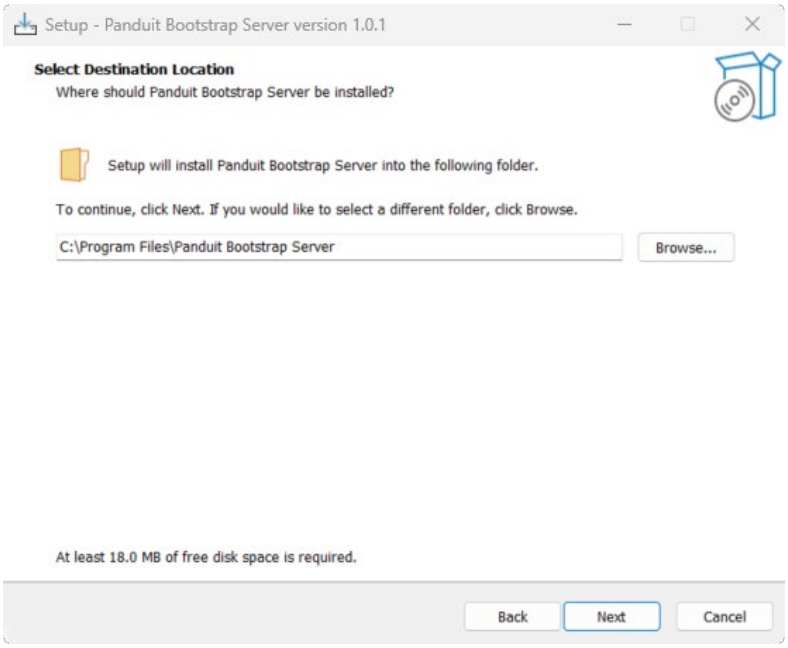


Figure 169: Install Folder

5) Choose the start menu folder.

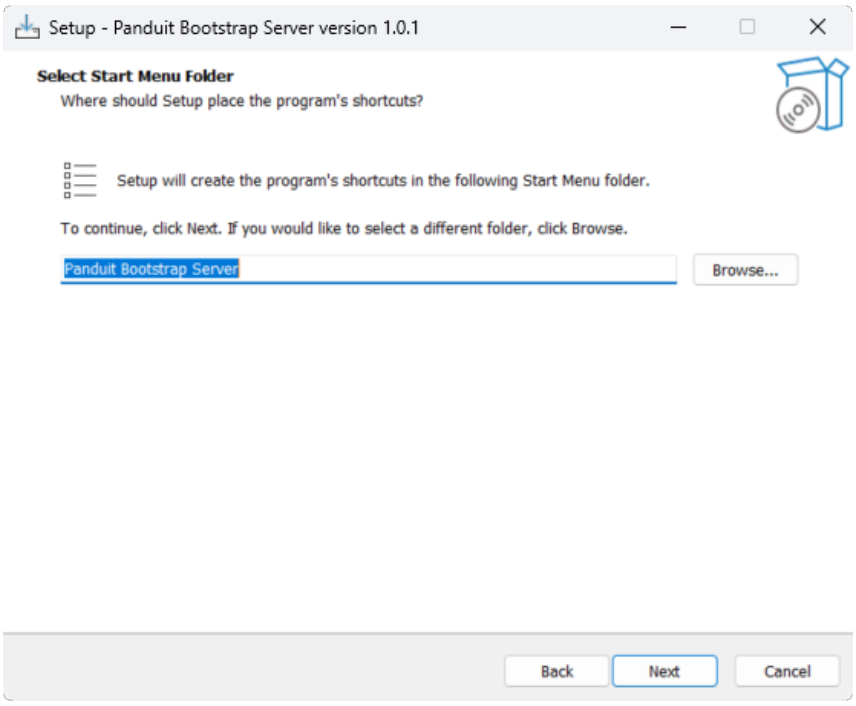


Figure 170: Start Menu Location

6) Click “Install” to start the software installation.

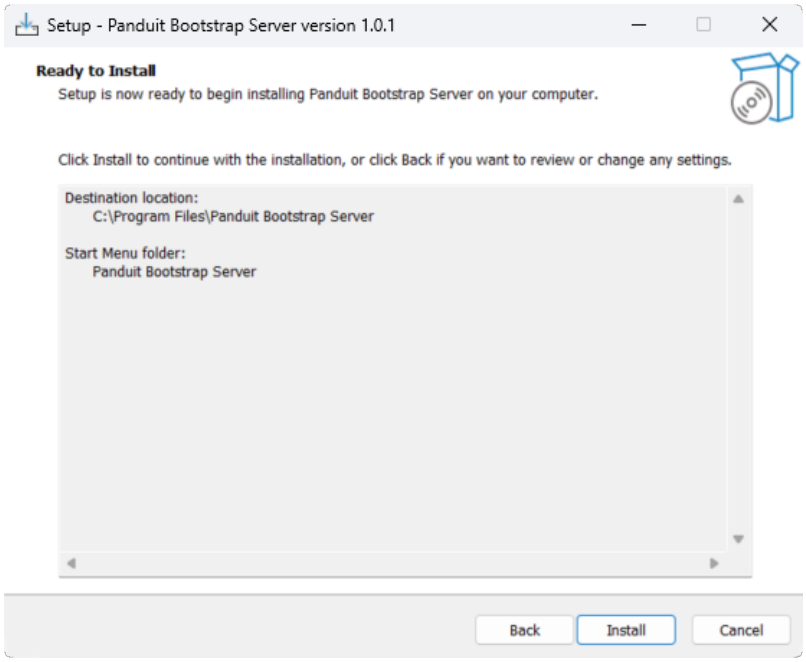


Figure 171: Installation Review

7) Set bootstrap server configuration options, the defaults are recommended for SZTP. These options can be changed after installation by editing server.cfg.

   For 1-Touch provisioning:
   - Check “Allow 1-Touch ZTP”
   - Delete text in Certificate/Key Path and provide ZTP Hostname to automatically generate a self-signed Certificate for the bootstrap server.

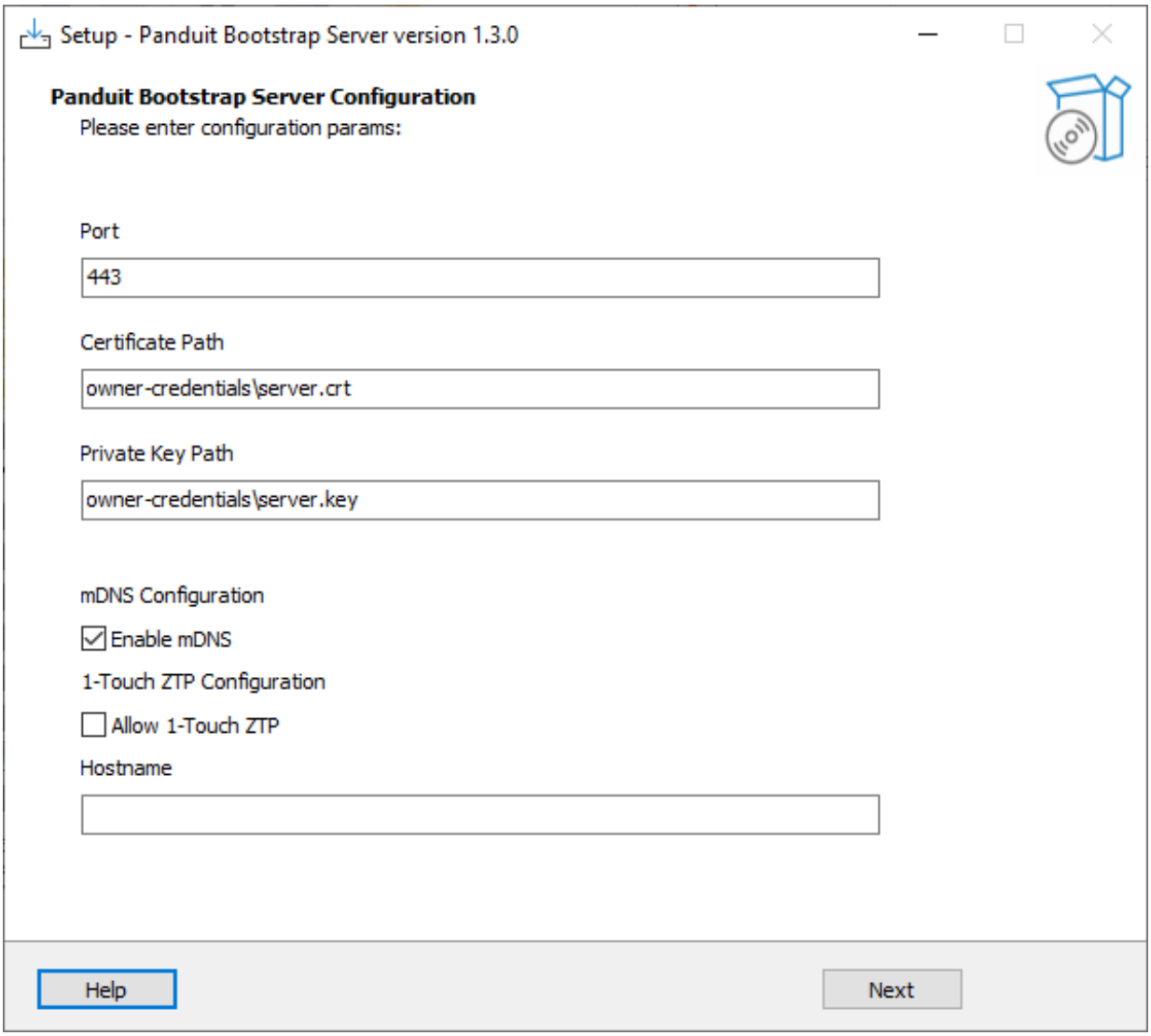


Figure 172: Bootstrap Server Configuration

8) Select post installation options.

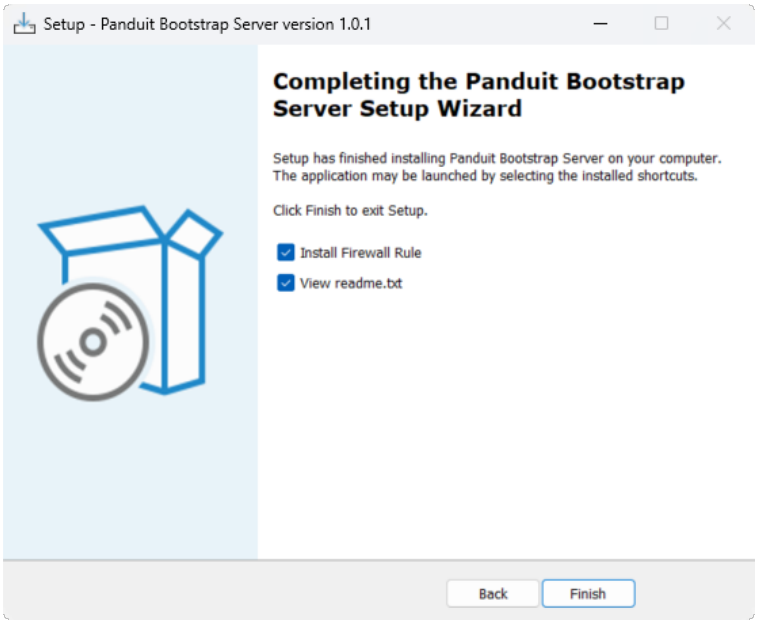


Figure 173: Post Install Options

Note: SZTP will not work if a firewall on the server blocks the port selected earlier in the installation process. Leave “Install Firewall Rule” checked to have the installer to add a Windows firewall rule that allows devices on the network to communicate with the bootstrap server. You may uncheck this option if you are not running Windows firewall or will configure the rule manually.

Bootstrap Server Configuration

1) Copy vouchers from Panduit into the "ownership-vouchers" folder in the installation folder. There is one voucher file per PDU. If the PDU’s serial number is ABC123, name its voucher file "ABC123.vcj".
(Skip this step for 1-Touch)

2) Copy bootstrap server certificate and key into the owner-credentials folder and name as specified in your server.cfg.

- The commonName (or subjectAltName DNS field) field in the Server Certificate MUST MATCH the bootstrap server address.
- Both commonName and subjectAltName must be present.

- Your Server Certificate cannot be the same as the pinned-domain-cert. Your Server Certificate must be signed by the pinned-domain-cert or signed by any number of intermediate entities leading back to the pinned-domain-cert.

- The Server Certificate must be in PEM format, and must include certificates for all intermediate entities leading back to the pinned-domain-cert. The order is: Server Certificate first, and then intermediates toward the pinned-domain-cert.

3) Download latest EL2P firmware package and copy into the "boot-image" folder.

4) Create configuration files for each PDU.
   - Configuration files may be created using a web UI on a Panduit PDU of the same type.
   - Download the configuration file from Settings -> System Management -> Actions -> Download Configuration

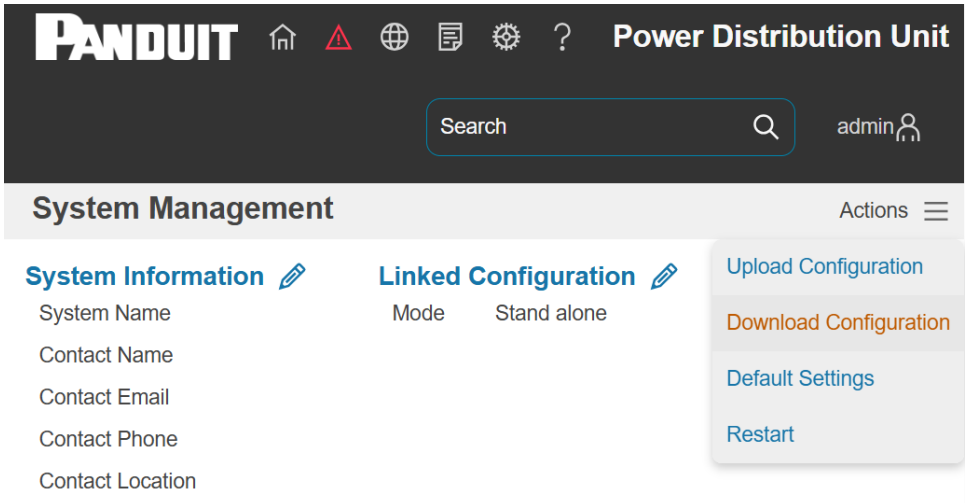


Figure 174: Configuration Download

5) Copy configuration files for each PDU into the "configurations" folder.

   There is one configuration file per PDU, named using with the PDU's serial number. If the PDU's serial number is ABC123, name its configuration file "ABC123.json".

6) Run services.msc and start "Panduit SZTP Bootstrap Service"

By default, the server is automatically started on reboot. This behavior can be modified

with services.msc.

Troubleshooting SZTP

1) Open the Windows Event Viewer

2) Under Event Viewer -> Windows Logs -> Application, review all "PanBootstrapService" events

   You can filter like so:

   Filter Current Log... -> Event sources: -> select "PanBootstrapService".

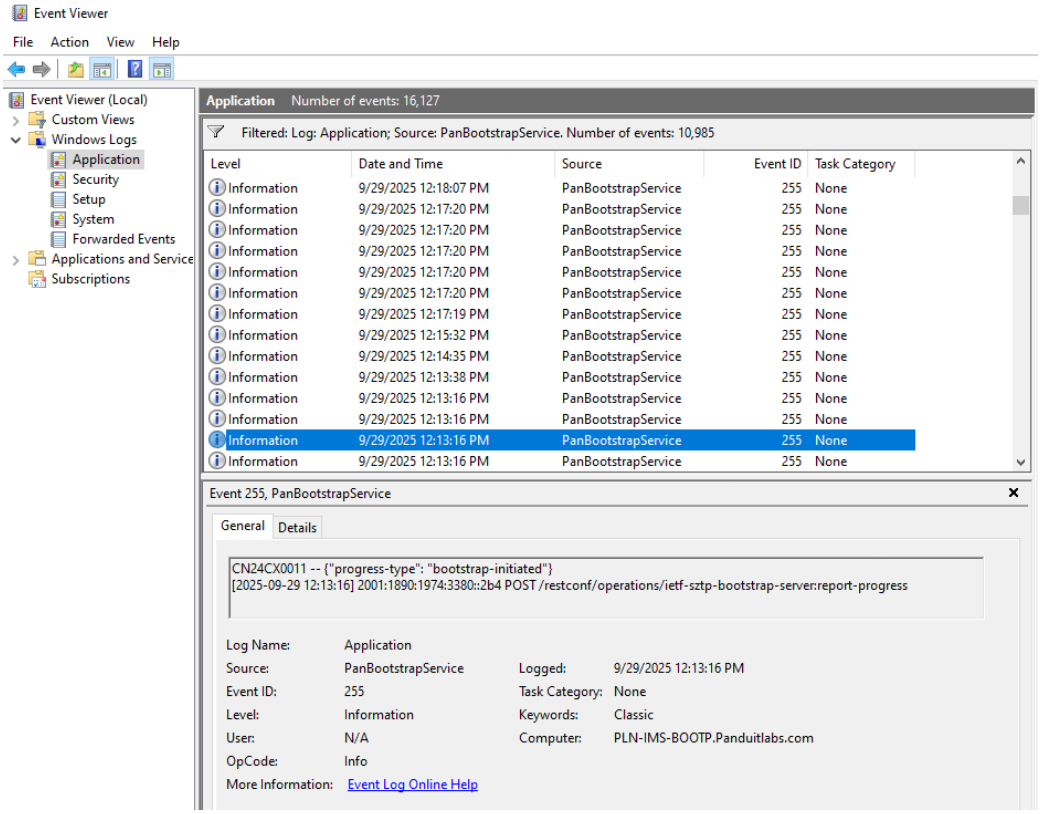


Figure 175: Windows Event Viewer

3) All vouchers are verified at startup, and any issues will be logged.

4) SZTP progress is logged for all SZTP clients that connect.

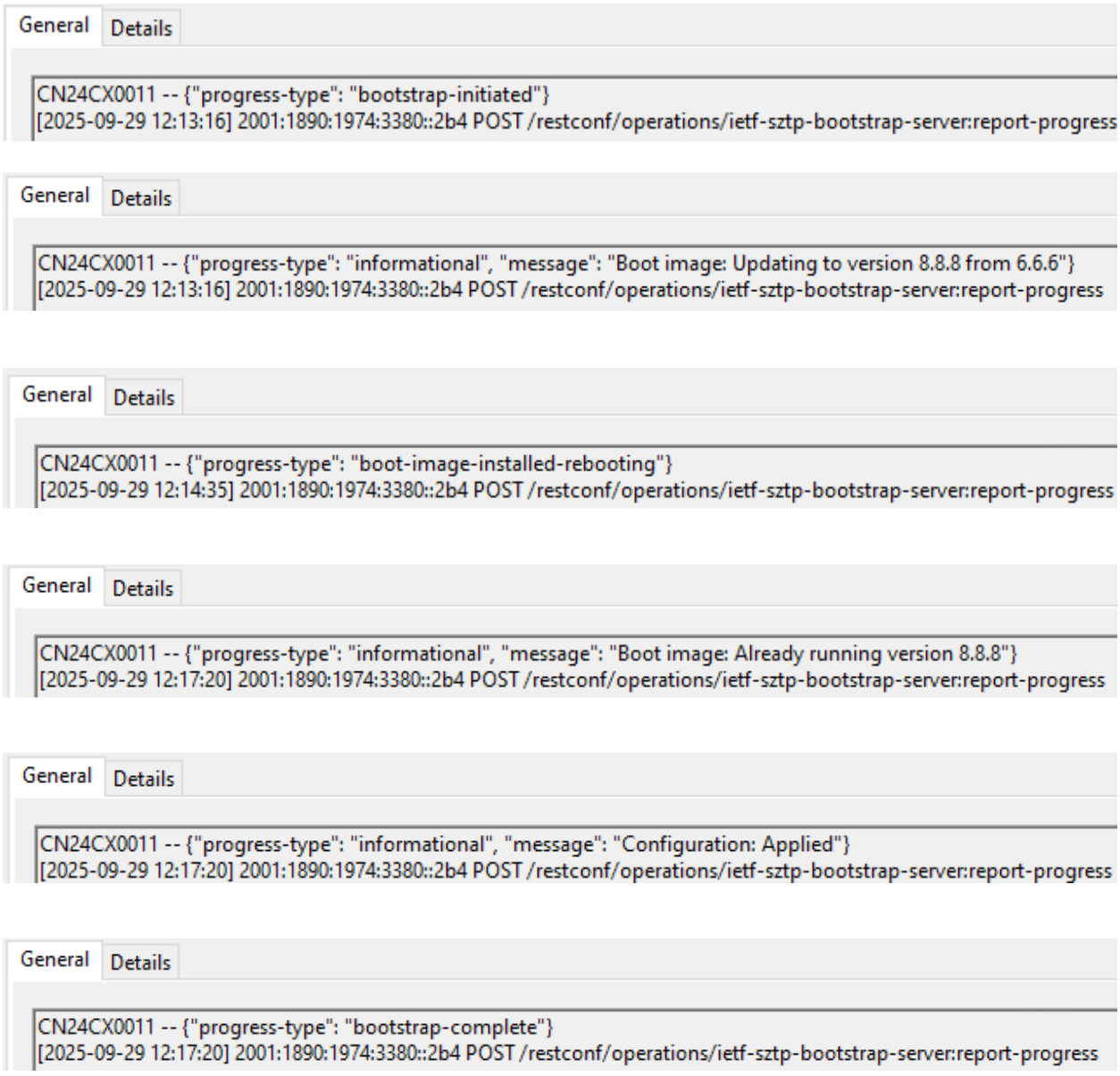


Figure 176: SZTP Event Examples

Appendix K: Onboard Data Collector Configuration

The Onboard Data Collector allows Panduit's EL2P PDUs to be monitored through the Cisco Nexus Dashboard. The Onboard Data Collector provides the functionality of the Panduit Data Collector on the EL2P PDU firmware. The "Collector" PDU collects metrics from "Device" PDUs by polling configured devices every 15 minutes. A Collector PDU can also collect its own metrics.

Requirements

Requirements for utilizing the Onboard Data Collector:

1) EL2P firmware version 1.6.4 or higher.
2) PDUs involved in the collection process have static IPs or fixed DHCP leases.
3) Cisco Nexus Dashboard version 4.1.1 or higher.

Collector PDU Setup

To set up the Onboard Data Collector, the user must configure an admin user account on the PDU designated to be a "Collector." This account must be a local account. To set up this user account:

1) Log in to a PDU, to configure as a Collector PDU, through the WebUI.
2) On the WebUI, go to Settings->User Accounts.

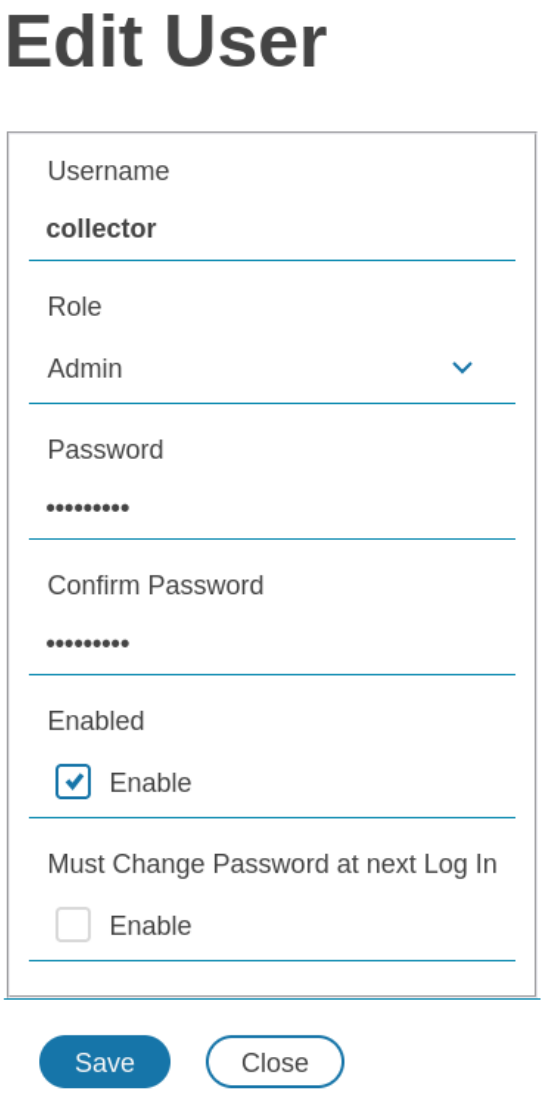


Figure 177: Example Admin User for Collector PDU

3) Create a user account at “Users” by clicking the pencil icon to the right of the final user account in the list, labeled “Add User.” This user must have the “Admin” role, have “Enabled” checked, and have “Must Change Password at next Log In” unchecked.

Now, the Onboard Data Collector must be configured on the WebUI:

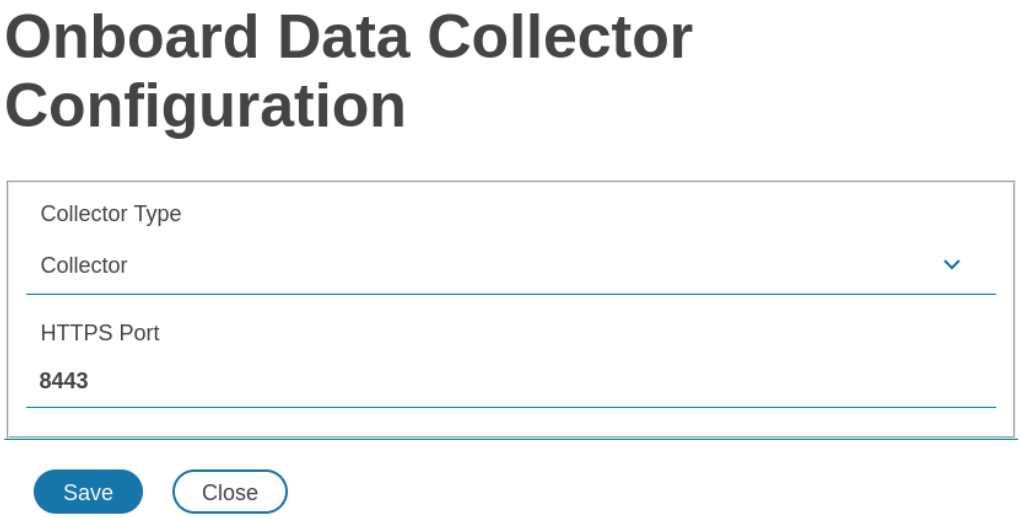


Figure 178: Onboard Data Collector Configuration for Collector PDU

1) On the WebUI, go to Settings->Network->Onboard Data Collector Configuration.
2) Set the “Collector Type” to “Collector.” This will enable the Onboard Data Collector HTTPS webserver, which shares its HTTPS certificate & private key with the HTTPS webserver.
    a. The “HTTPS Port” must be set to 8443 for communication with the Cisco Nexus Dashboard. This port number must not conflict with another port number.
    b. This also enables the Device REST API on the HTTPS server that the WebUI is hosted on, so a Collector PDU’s metrics can be polled.

Device PDU Setup

Once a Collector PDU has been set up, the user may now set up the Device PDU(s) to have its metrics collected. Note that a Collector PDU may also be registered to itself or another Collector PDU.

Like the Collector PDU setup, the user should create a user account:

1) Log in to the PDU to configure as a Device through the WebUI.
2) On the WebUI, go to Settings->User Accounts.

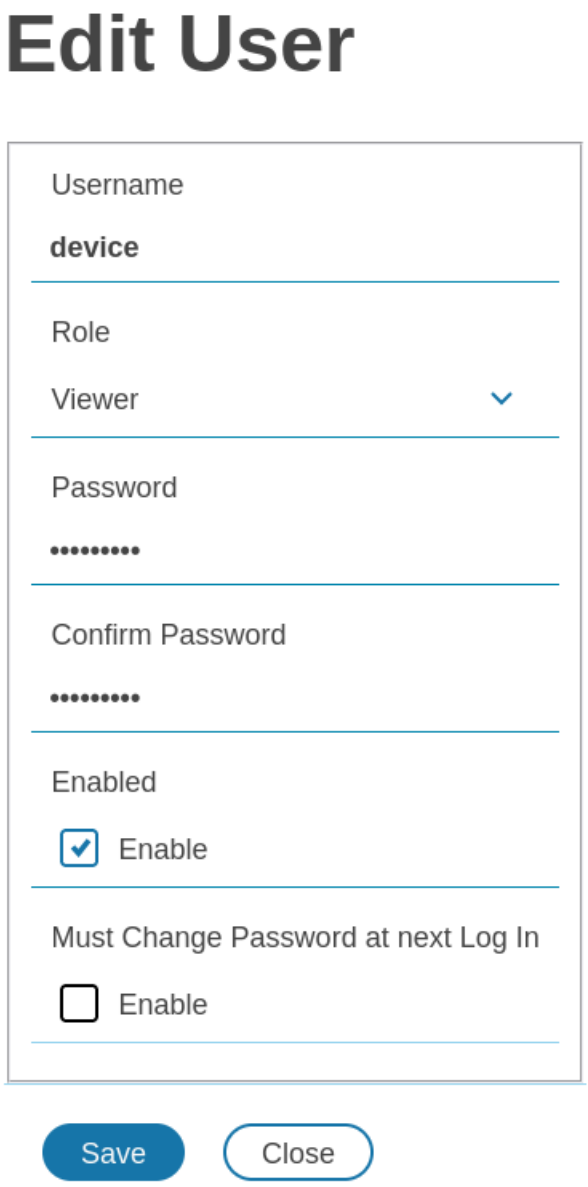


Figure 179: Example Viewer User for Device PDU

3) Create a user account at “Users” by clicking the pencil icon to the right of the final user account in the list, labeled “Add User.” This user is recommended to have the “Viewer” role. It must have “Enabled” checked and “Must Change Password at next Log In” unchecked.

    a. This account should be configured with the “Viewer” role, to separate the data collection account from system administration accounts. The device account may be a Controller or Administrator, but it will not benefit from

those additional permissions.

Next, the PDU may be configured as a Device (note: if the user is configuring a Collector PDU and wishes to register it to itself or another Collector PDU, this step may be skipped):

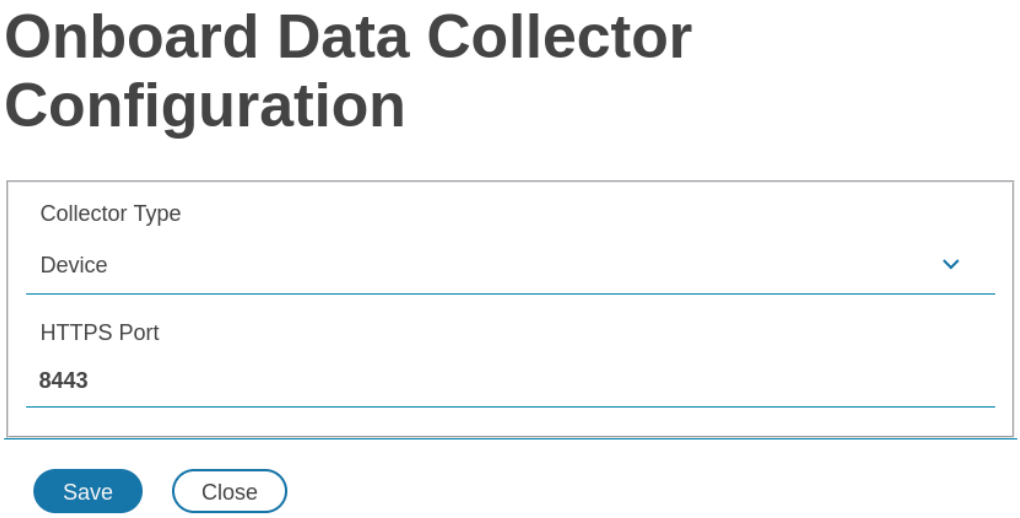


Figure 180: Onboard Data Collector Configuration for Device PDU

1) On the WebUI, go to Settings->Network->Onboard Data Collector Configuration.
2) Set the “Collector Type” to “Device.” This will enable the Device REST API on the HTTPS webserver.
    a. This does not enable the Onboard Data Collector HTTPS webserver, so “HTTPS Port” can be ignored.
    b. The “HTTPS Port” in Settings->Network->Web Access Configuration must have the value “443.” In other words, the HTTPS port which the WebUI is hosted on must be port 443. This allows a Collector PDU to communicate with a Device PDU.

Registering PDUs to Cisco Nexus Dashboard

Now, the user should have the Collector PDU(s) and Device PDU(s) set up. The user may now register the Collector PDU to the Cisco Nexus Dashboard. On the Cisco Nexus Dashboard WebUI:

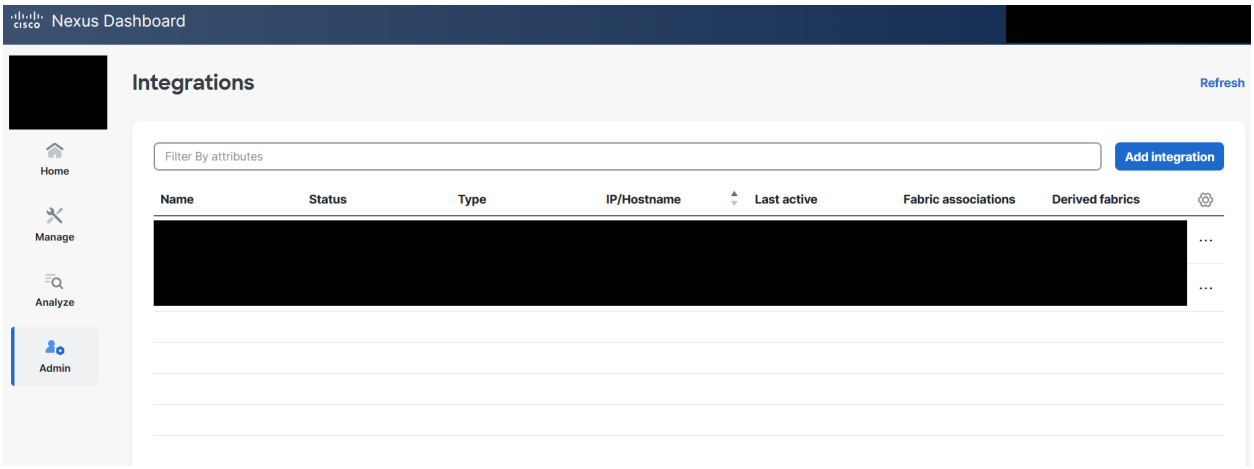


Figure 181: Cisco Nexus Dashboard Integrations

1) From the “Home” page, go to Admin->Integrations and click on “Add integration.”

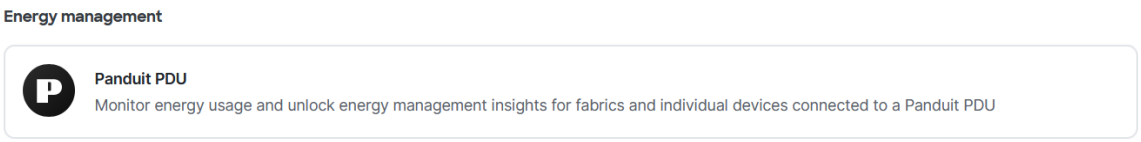


Figure 182: Cisco Nexus Dashboard Panduit PDU Integration

2) Scroll down and select “Panduit PDU.”

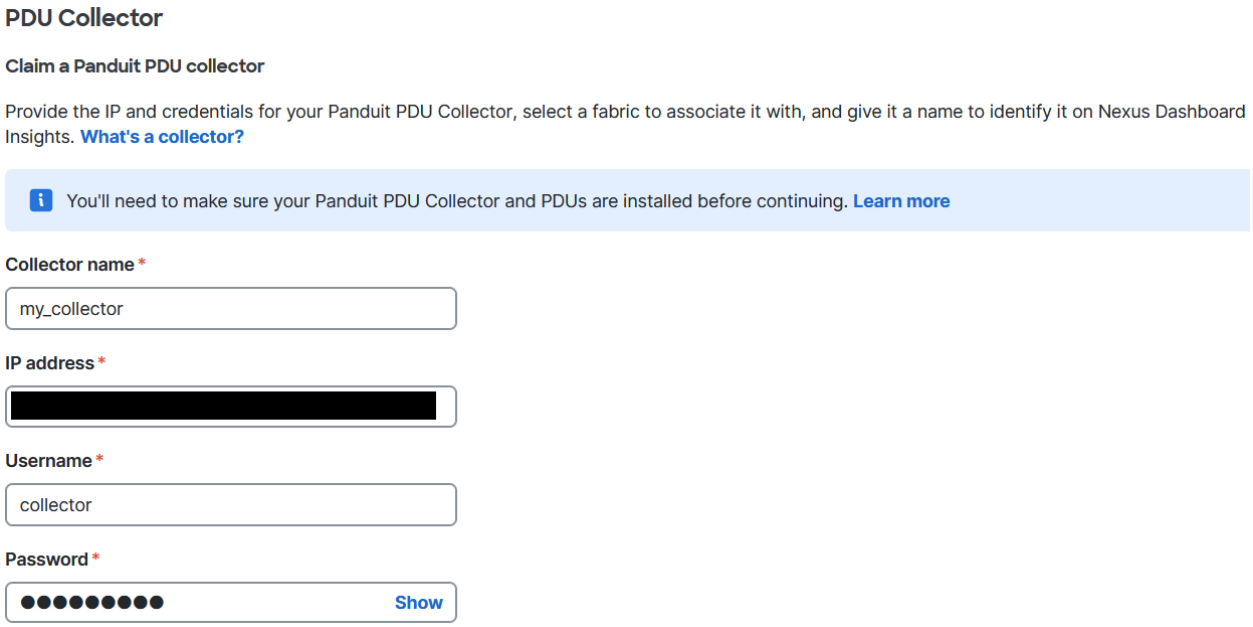


Figure 183: Registering Collector PDU to Cisco Nexus Dashboard

3) Input the “Admin” role credentials of the Collector user, created during Collector

PDU setup, into the “Username” and “Password” fields. Input the “IP address” of the Collector PDU and enter a “Collector name” for it.

Figure 184: Selecting Fabric

4) Associate the PDU with a Fabric and click “Save.”

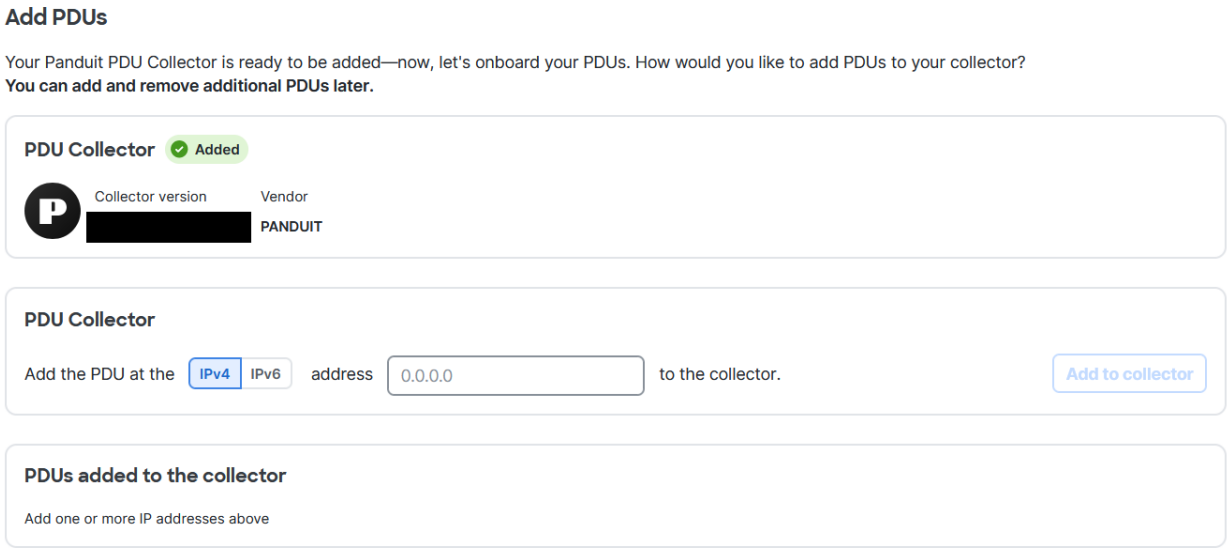


Figure 185: Registered Collector PDU

5) The Collector PDU should be registered successfully. The user may now add Device PDUs to the Collector. Input the IP address of the Device PDU to register and click “Add to collector.” The user will now be prompted for credentials.

    a. Note that the user may input the IP address of the Collector PDU to collect its own metrics.

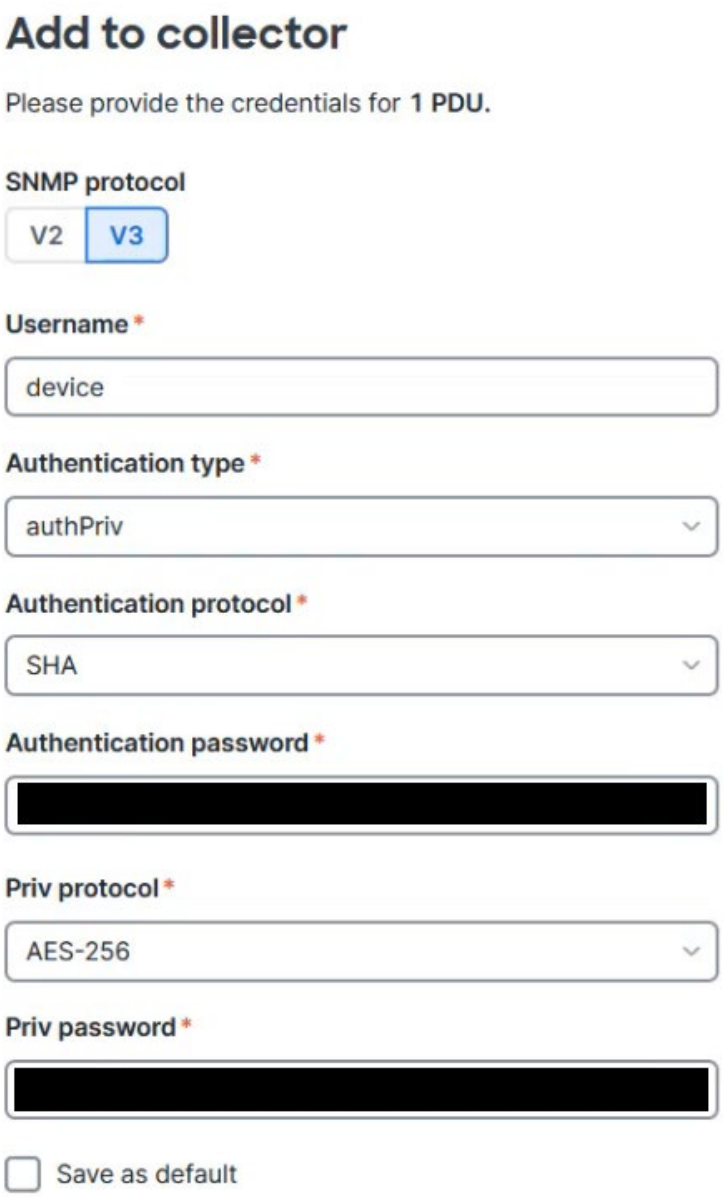


Figure 186: Example Credentials for Device PDU

6) Select “SNMP protocol” and choose “V3.”

    a. Note that the Onboard Data Collector utilizes HTTPS rather than SNMP and requires these settings to be configured in this way.

7) Select “Username” and enter the device username for the “Viewer” role user which was created during Device PDU setup.

8) Select “Authentication type” and set it to “authPriv.”

9) Select “Authentication protocol” and set it to “SHA.”

10) Select “Authentication password” and enter the device password for the “Viewer” role user.

11) Select “Priv protocol” and select “AES-256.”

12) Select “Priv password” and enter the device password for the “Viewer” role user.

Repeating steps 1-4 for each Collector PDU and steps 5-12 for each Device PDU, the user should have successfully registered the PDUs they wish to monitor. Some data will take at least 15 minutes to appear on the Cisco Nexus Dashboard after registration.

Notes

- If the user changes the password of the “Admin” role account on a Collector PDU via the Cisco Nexus Dashboard UI, the new password must meet the NMC’s requirements for a strong password.

Security

To reduce login events, the refresh endpoint for the Onboard Data Collector generates a new refresh token, when given a valid refresh token. If a user is logging in for the first time, they must use the login endpoint first to obtain an access token.

- Rebooting the NMC will expire all access and refresh tokens immediately.
- Disabling a user for the access token duration (5 minutes) will prevent that user from logging in and will expire any issued access tokens for that user.
- Disabling a user for the refresh token duration (30 minutes) will prevent that user from logging in and will expire any issued access & refresh tokens for that user.

Communication Diagrams

The following diagrams illustrate the communication between the Cisco Nexus Dashboard, Collector PDU, and polled Device PDUs.

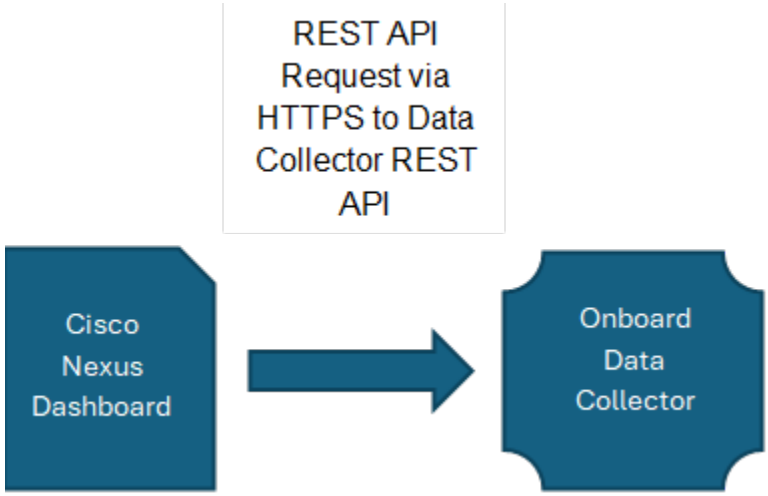


Figure 187: Cisco Nexus Dashboard to Onboard Data Collector Communication

The figure above illustrates general communication between the Onboard Data Collector and the Cisco Nexus Dashboard.

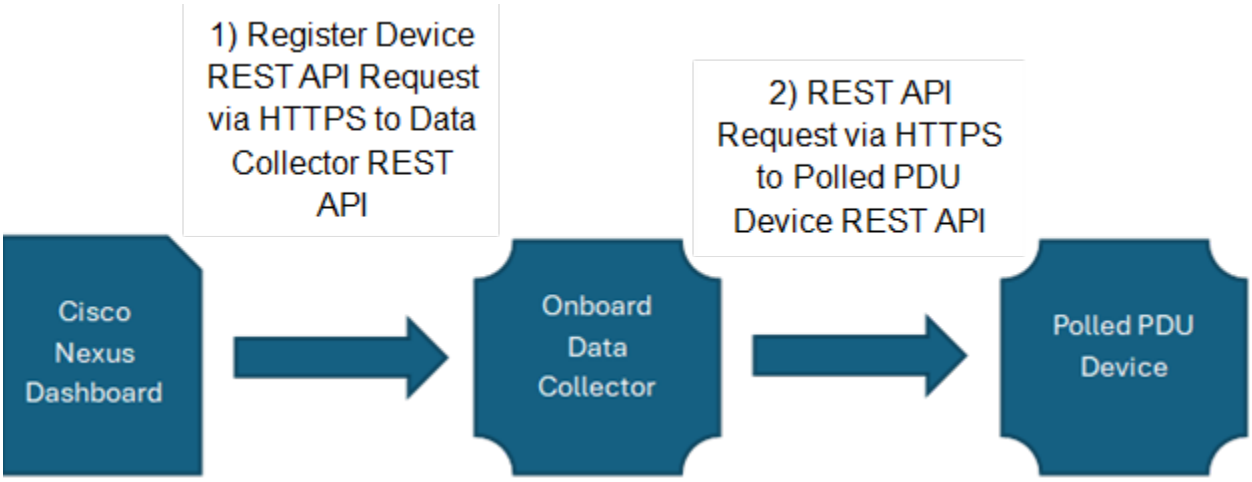


Figure 188: Register Device Communication

The figure above demonstrates communication when the Cisco Nexus Dashboard registers a Device PDU.

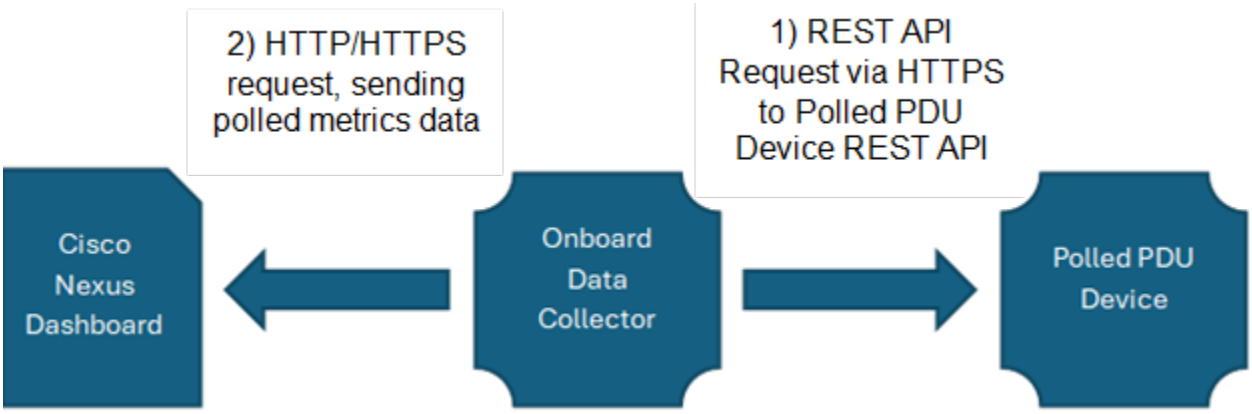


Figure 189: Onboard Data Collector Communication when Polling

The figure above demonstrates communication when a Collector PDU polls Device PDUs and sends that polled data to the Cisco Nexus Dashboard.

Appendix L: Bulk Management with SiteCommand Utility

SiteCommand Utility is a free, lightweight software tool provided by Panduit to simplify bulk configuration and firmware management across multiple Panduit EL2P PDUs.

SiteCommand Utility is designed for deployment, commissioning, and maintenance activities optimizing managing multiple Panduit EL2P PDUs.

For the latest version of SiteCommand Utility please visit: panduit.com → Support → Download Center → PDU

1. Download SiteCommand Utility from the web page.
2. Unzip the downloaded file.
3. Double click / run SiteCommand Utility installer file.
4. Follow the instructions to complete the installation process.
5. After installing the software, double click the launch icon that was added to your desktop or type in your web browser: https://localhost:8557/

Note: For additional information please download SiteCommand Utility User Manual at: panduit.com → Support → Download Center → PDU

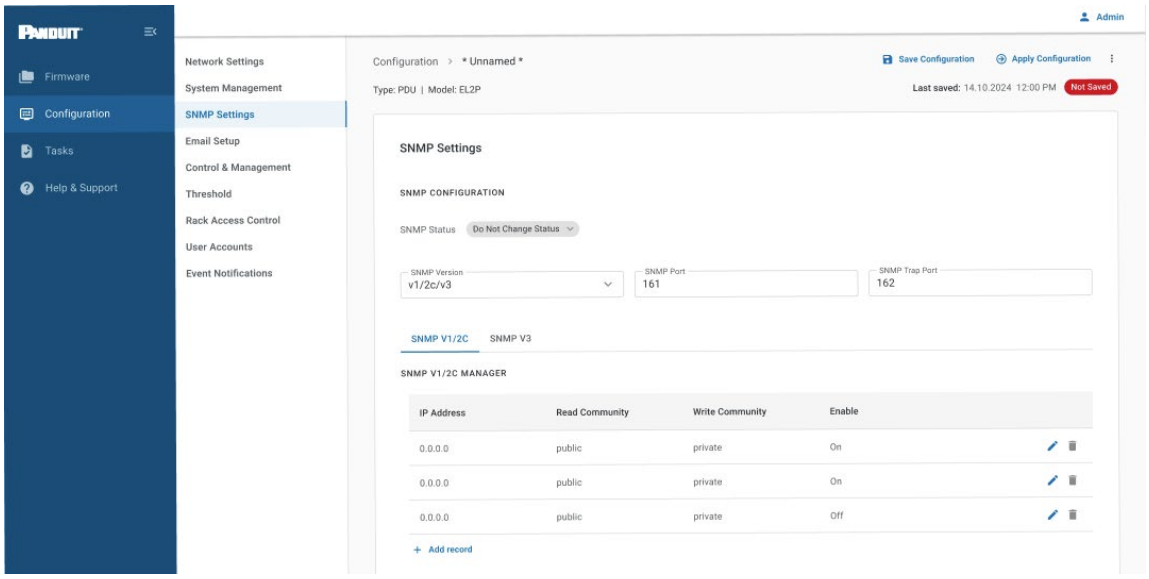


Figure 190: SiteCommand Utility

Appendix M: Frequently Asked Questions (FAQ)

Question:
Can PDUs operating in Bridge Mode be connected to the same switch when STP is enabled, or should they be connected to separate switches to avoid potential network loops?

Answer:
STP is designed to prevent network loops, so PDUs can be connected to either the same switch or to multiple switches, provided the switches support STP and operate within the same subnet. When STP is enabled and functioning correctly, connecting PDUs to the same switch will not create loops.

Question:
Can Bridge Mode be used in network environments where STP is not permitted, such as certain spine-and-leaf architectures?

Answer:
Yes. Bridge Mode can operate in environments where STP is not allowed. In these cases, STP should be disabled, and the final device in the chain must not be reconnected back into the network, as this would create a loop.

Question:
When connected to a network, is the PDU identified by the switch as another switching device?

Answer:
If STP is enabled, the PDU participates in STP processes, but it does not use LLDP and therefore is not fully recognized as a standard network switch. It engages in basic loop-prevention behavior but does not advertise or exchange switch-level information.

Question:
Does Power Share still work in Bridge Mode?

Answer:
Yes. Power Share works in Bridge Mode but requires CLI configuration. This is necessary because enabling Power Share on links connected to customer equipment may cause negotiation issues.

Ideally, Power Share should be enabled only between PDUs, not at the endpoints.
In Standalone mode, Power Share is disabled by default because PDUs are typically connected directly to customer equipment.

Question:
In Bridge Mode, does the WebGUI display neighboring PDUs, or do they behave as standalone units?

Answer:
PDUs in Standalone mode have no awareness of their neighbors.

Question:
How would the WebGUI behave if only the 1st and 3rd PDUs in the chain had Bridge Mode enabled?

Answer:
It is best practice to choose a single topology and apply it consistently across all PDUs. Mixing modes within the same chain is not recommended.