PANDUIT®
infrastructure for a connected world

Panduit UPS

User Manual

UPS Network Management Card

Version 1.8.3

Table of Contents

Section 1 – System Overview 8
NMC Controller 8
Connecting the NMC via Ethernet Port 8
Connecting the NMC via Wi-Fi 9
Connecting the NMC to a Computer Serial Port 9
Section 2 – Web Graphical User Interface (GUI) 11
Internet Protocol (IP) Addressing 11
Web Connection 11
Introduction to the Web GUI 14
Introduction to the Dashboard 16
System Management Information 19
Network Settings 22
Setting Time and Date on the NMC 25
Control & Manage 28
Panduit's Smart Load Shedding 43
Email Setup 50
Event Log 53
Data Log 54
Web Interface Access 55
Setting Up the System for RADIUS Authentication 57
Configuring the system with LDAP Server Settings 59
Wi-Fi Settings 61
Section 3 – Simple Network Management Protocol (SNMP) 67
SNMP Management Configuration 67
Configuring Users for SNMP V1/V2c 69
Configuring Users for SNMP v3 70

Configuring SNMP Traps 73
Section 4 – Network Management Controller 77
Status LED 77
Network LED 77
Section 5 – G5 PDU Accessories 78
Hardware Overview 78
Configuring Temperature Scale 79
Configuring Environmental Sensors 80
Configuring Security Sensors 81
Deleting Sensors 83
Section 6 – Security Handle 84
Configuring Cabinet Access Control 84
Adding a User for Local Rack Access 85
Configuring Rack Access Settings 88
Configuring Handle Settings 89
Configuring Keypad Settings 91
Remote Controlling the Handle 91
Controlling the Beacon 92
The Status LED 94
Setting Status LED State 95
Handle and Compatible Card Types 96
Section 7 – Security 97
API Access to Primary Features 97
Primary Features 97
Security Implications of Configuration Changes 97
Secure Disposal Features 99
Non-volatile Storage 99
Authentication Data 100
Authentication Priority 100

Network Transport Security 101
Wireless Communication 105
Network Configuration Data 106
Logging 106
External Authentication Mechanisms 106
Secure Boot Protection 106
Firmware Update Protection 107
Other Features 107
Protocols 107
Intended Use Security Context 107
Secure deployment 108
Secure Operation Summary 110
Defense-in-Depth Strategy Summary 111
Security Response 114
Warranty and Regulatory Information 115
Warranty Information 115
Regulatory Information 115
Panduit Support and Other Resources 116
Accessing Panduit Support 116
Acronyms and Abbreviations 117
Appendix A: Firmware Update Procedure 118
Appendix B: System Reset or Password Recovery 119
Appendix C: Direct connect to the UPS via Ethernet without Bonjour 120
Appendix D: Command Line Interface 124
Appendix E: RADIUS Server Configuration 127
Appendix F: POSIX Time Zone Information 129
Appendix G: Consolidated Network Interface and Protocol Inventory 130

Table of Figures

Figure 1: Ethernet Port for Network Connection 8
Figure 2: Reset button 9
Figure 3: Serial In Port 10
Figure 4: Network information from + ... 10
Figure 5: Refused Connection Example 11
Figure 6: Certificate Warning 12
Figure 7: Login Page 12
Figure 8: Changing Your Password 13
Figure 9: After Login 13
Figure 10: Landing Page/Dashboard 14
Figure 11: Power Summary Page 16
Figure 12: UPS Monitoring Page 17
Figure 13: Environmental Monitoring Page 18
Figure 14: Security Monitoring Page 18
Figure 15: System Management 19
Figure 16: System Information Configuration 20
Figure 17: Rack Location Configuration 21
Figure 18: Power Panel & Core Location 22
Figure 19: Ethernet Interface Configuration 23
Figure 20: DNS Configuration 24
Figure 21: Web Access Configuration 25
Figure 22: SSH Configuration 25
Figure 23: Control & Manage 29
Figure 24: Audible Alarm Configuration 29
Figure 25: Start Shutdown Example 30
Figure 26: Cancel Shutdown Example 31
Figure 27: Enter Bypass Example 31
Figure 28: Exit Bypass Example 32
Figure 29: UPS Manual Test Configuration 33
Figure 30: Start Test Example 33
Figure 31: Start Test Confirmation 34
Figure 32: Cancel Test Example 34
Figure 33: Cancel Test Confirmation 34
Figure 34: Battery Test Configuration 35
Figure 35: UPS Output Mode 36
Figure 36: UPS Main Input Setting 37

Figure 37: UPS Bypass Voltage Limit configuration 37
Figure 38: Battery Information configuration 39
Figure 39: Edit Outlet Group 40
Figure 40: Outlet Group Control 41
Figure 41: Edit Outlets 42
Figure 42: One Delay Time 43
Figure 43: Shutdown Group Configuration 45
Figure 44: Smart Load Configuration 47
Figure 45: Shutdown Schedule Configuration 49
Figure 46: Email Setup 50
Figure 47: SMTP Account Settings 51
Figure 48: Email Recipient 53
Figure 49: Event log 53
Figure 50: Event log Actions menu 54
Figure 51: Data Log 54
Figure 52: Data Log Configuration 55
Figure 53: Data Log Configuration Panel 55
Figure 54: User Accounts 58
Figure 55: RADIUS Configuration 58
Figure 56: LDAP Configuration 60
Figure 57: Enable Role Privileges 61
Figure 58: Wi-Fi Settings screen 62
Figure 59: Wi-Fi Radio Configuration 62
Figure 60: Wi-Fi Direct Connect Configuration 63
Figure 61: Wi-Fi Personal security Network configuration 64
Figure 62: Wi-Fi Enterprise security Network configuration 65
Figure 63: Wi-Fi Interface Configuration 66
Figure 64: SNMP Management 67
Figure 65: SNMP General 68
Figure 66: SNMP Port 68
Figure 67: Setup SNMP Port and Trap Port 69
Figure 68: Define SNMP V1/V2c User 69
Figure 69: Edit V1/2c Manager 70
Figure 70: SNMP v3 Manager 71
Figure 71: SNMP V3 Edit 72
Figure 72: SNMPv2c Trap Receiver Configuration Information 74
Figure 73: SNMPv3 Trap Server configuration Information. 75
Figure 74: Sensor Port 79

Figure 75: User Accounts 80
Figure 76: Temperature Units Setting 80
Figure 77: Environmental Sensor Threshold Configuration View 81
Figure 78: Temperature Sensor Edit dialog 81
Figure 79: Security Sensor Alarm Configuration view 82
Figure 80: Dry Contact Sensor Edit dialog 83
Figure 81: Security Handles 84
Figure 82: Rack Access Control 85
Figure 83: Rack Access Control Actions 85
Figure 84: Add Card 86
Figure 85: Edit Card 87
Figure 86: Rack Access Settings 88
Figure 87: Handle Settings 90
Figure 88: Keypad Settings 91
Figure 89: Remote Control 92
Figure 90: Beacon 93
Figure 91: Beacon Settings 94
Figure 92: Status LED 95
Figure 93: Status LED Settings 96
Figure 94: SSL Certificate Load Screen 109
Figure 95: Upload Firmware 118
Figure 96: View network Connections 120
Figure 97: Properties 120
Figure 98: Ethernet Properties 121
Figure 99: Internet Protocol Version 4 121
Figure 100: IP Address Calculation 123
Figure 101: Reading from CLI 125
Figure 102: Writing from CLI 126

Section 1 – System Overview

NMC Controller

All Panduit Intelligent NMCs feature a Hot Swappable NMC Controller. This centralized piece of intelligent hardware receives an IP address, contains a Graphical Web Interface and is addressable over the network.

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).

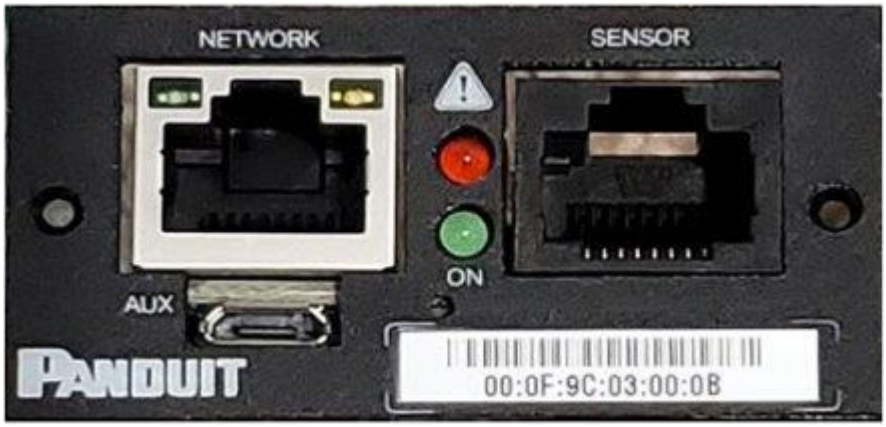


Figure 1: Ethernet Port for Network Connection

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 to the UPS via Ethernet without Bonjour. The NMC supports mDNS to discover the DHCP IP or the Auto IP. The mDNS address format is “panduit-ups-nmc-<macaddress>.local”. For example, the mDNS address for Figure 1 corresponds to “panduit-ups-nmc-000F9C03000B.local” The address is a unique address based on the NMC MAC address.

Connecting the NMC via Wi-Fi

Mobile devices can access the NMC via Wi-Fi.

1. Push and quickly release the reset button on the back of the NMC. The green LED will flash if Wi-Fi Direct Connect successfully started.
2. Connect the NMC from a mobile device. Network id is Panduit-ups-nmc-MAC and the default password is adminadmin

   Note. The wireless access is only available for 10 minutes by default
3. 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
4. Refer to web connection in Section 2 to accessing the web page.
5. Navigate to Identification page to examine the Ethernet IP address.
6. Navigate to Wi-Fi Settings page to set up Wi-Fi network

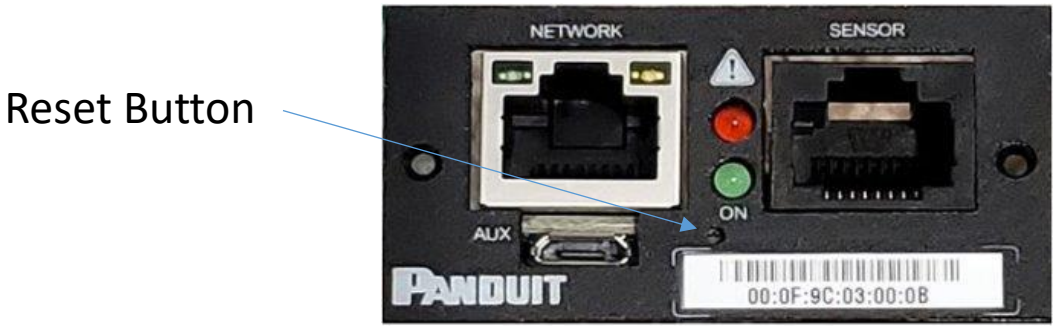


Figure 2: Reset button

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 USB 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

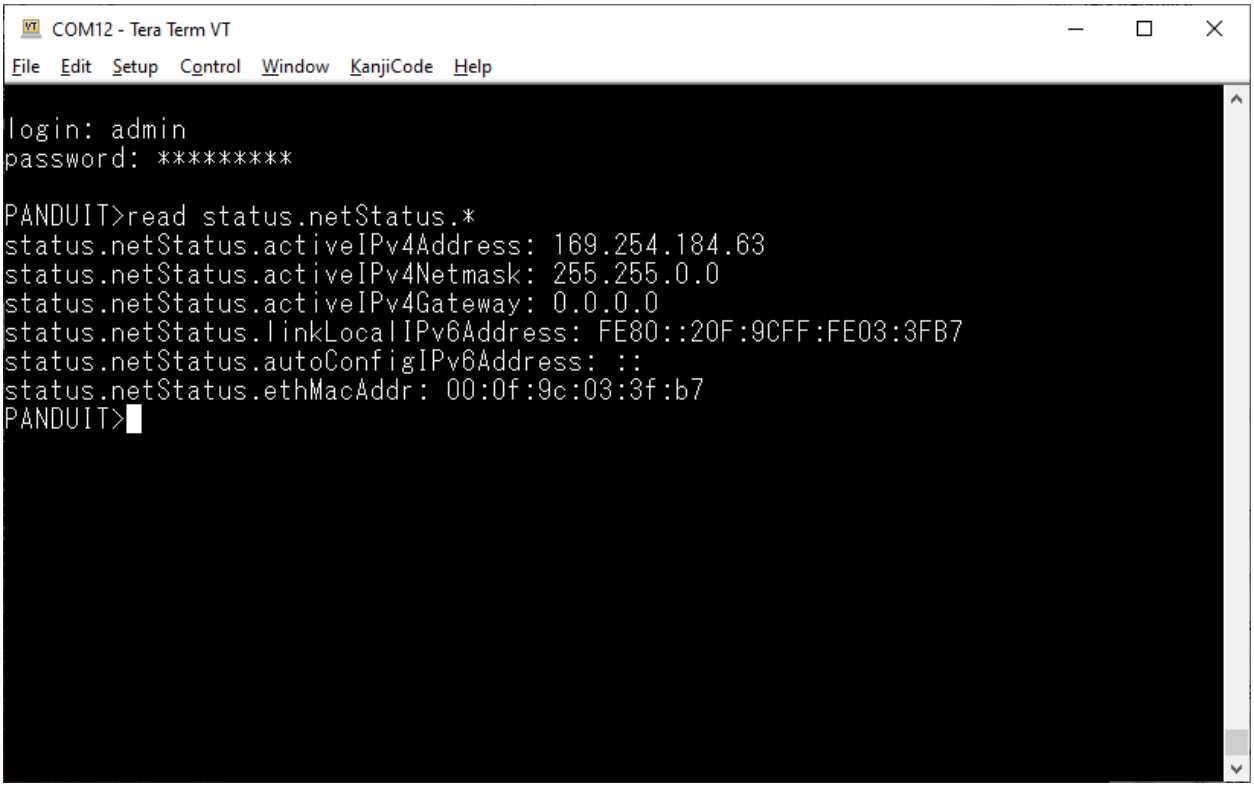


Figure 4: Network information from +

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://”

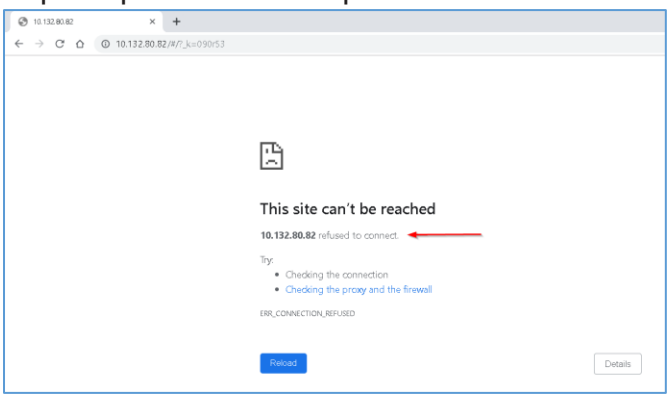


Figure 5: Refused Connection Example

- 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.

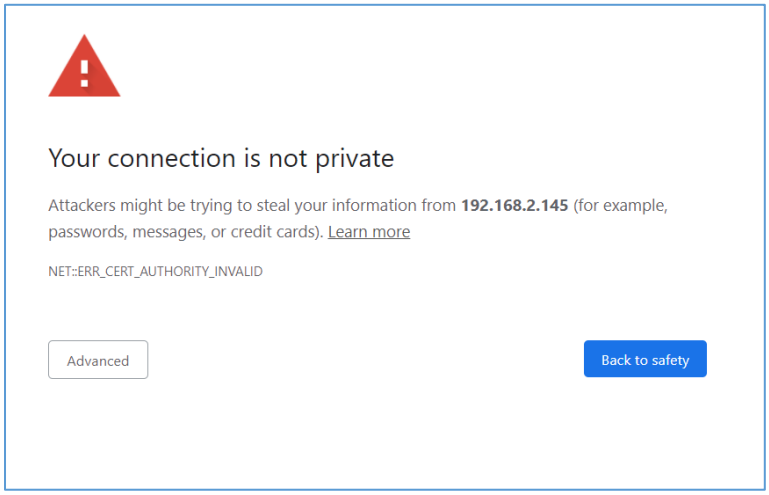


Figure 6: Certificate Warning

- 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.

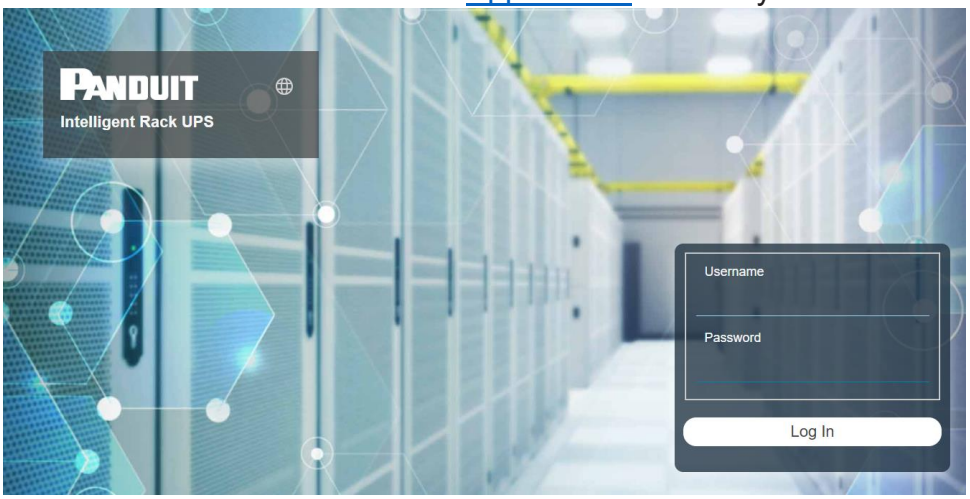


Figure 7: Login Page

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.

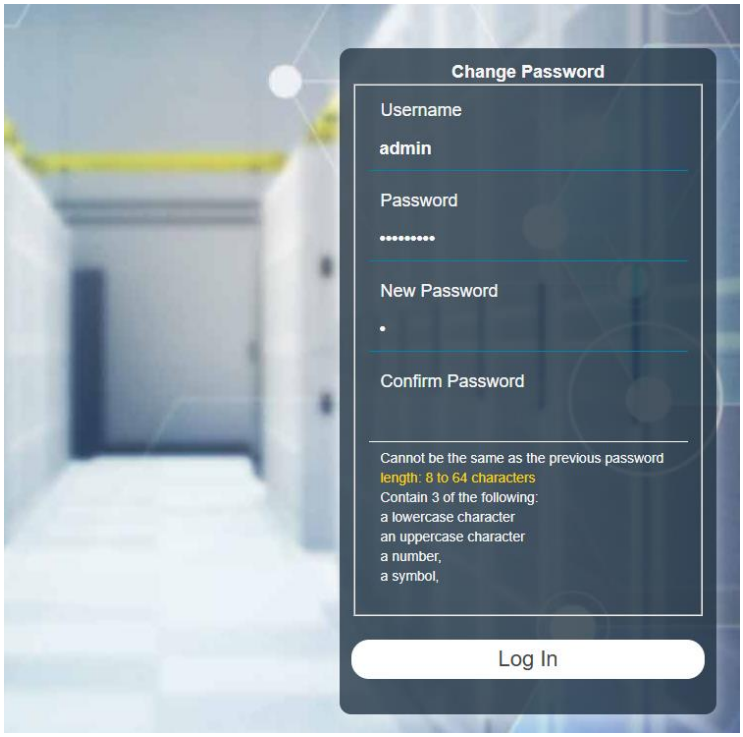


Figure 8: Changing Your Password

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**.

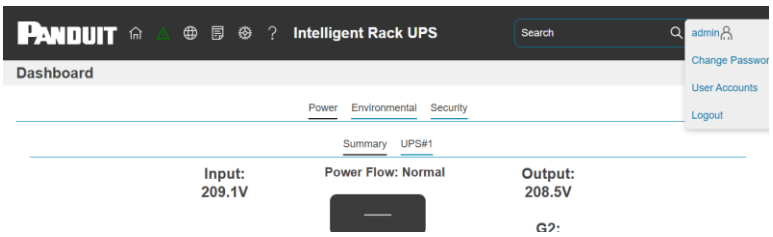


Figure 9: After Login

2. The **Change Password** window opens.
3. Follow the previous instructions in **Changing Your Password** and Figure 8: Changing Your Password

Introduction to the Web GUI

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

Landing Page/Dashboard

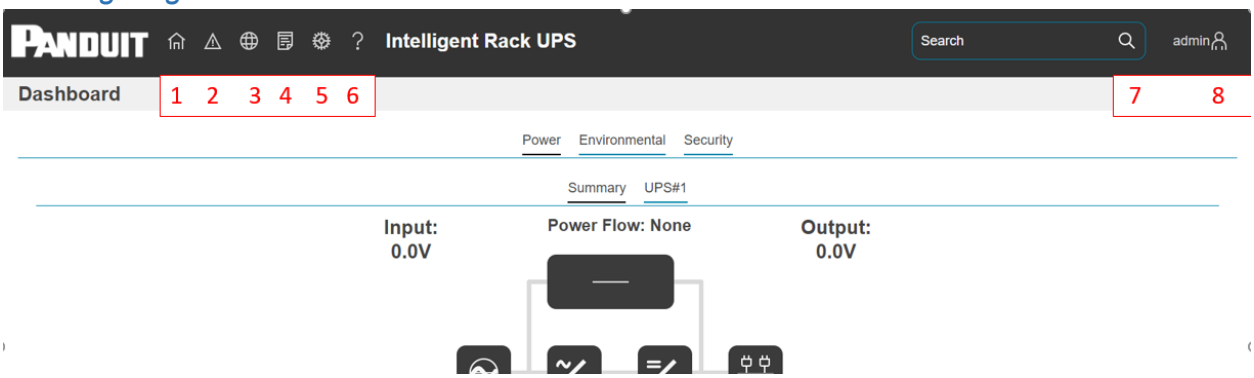


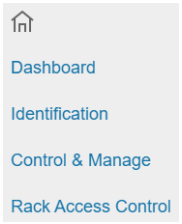
Figure 10: Landing Page/Dashboard

Number	Icon	Description
1		The home icon provides an overview of the UPS with access to the Dashboard, Identification, and Control & Manage.
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 UPS, which can be viewed and downloaded.
5		The settings icon allows a user to setup the Network Settings, System Management, SNMP Manager, Email Setup, Trap Receiver, User Accounts and Thresholds.
6		Information about the UPS can be found using this icon. You also can also click user guide and license to ask for help.

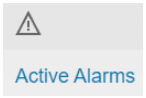
Number	Icon	Description
7		The search icon allows you to input key words and search for the related results.
8		This icon shows who is logged in (user or admin). Account passwords can be changed, and user accounts managed through this page.

Menu Dropdowns

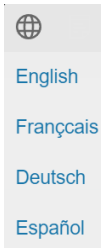
Overview



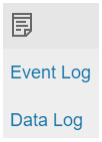
Alarms



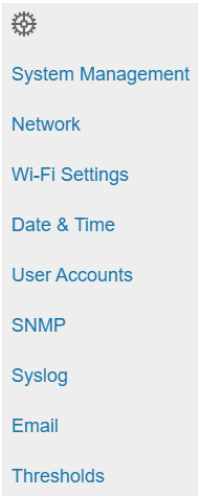
Language



Logs



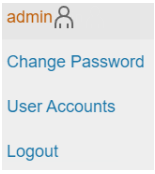
Setting



Help



User



Introduction to the Dashboard

Power Summary Page

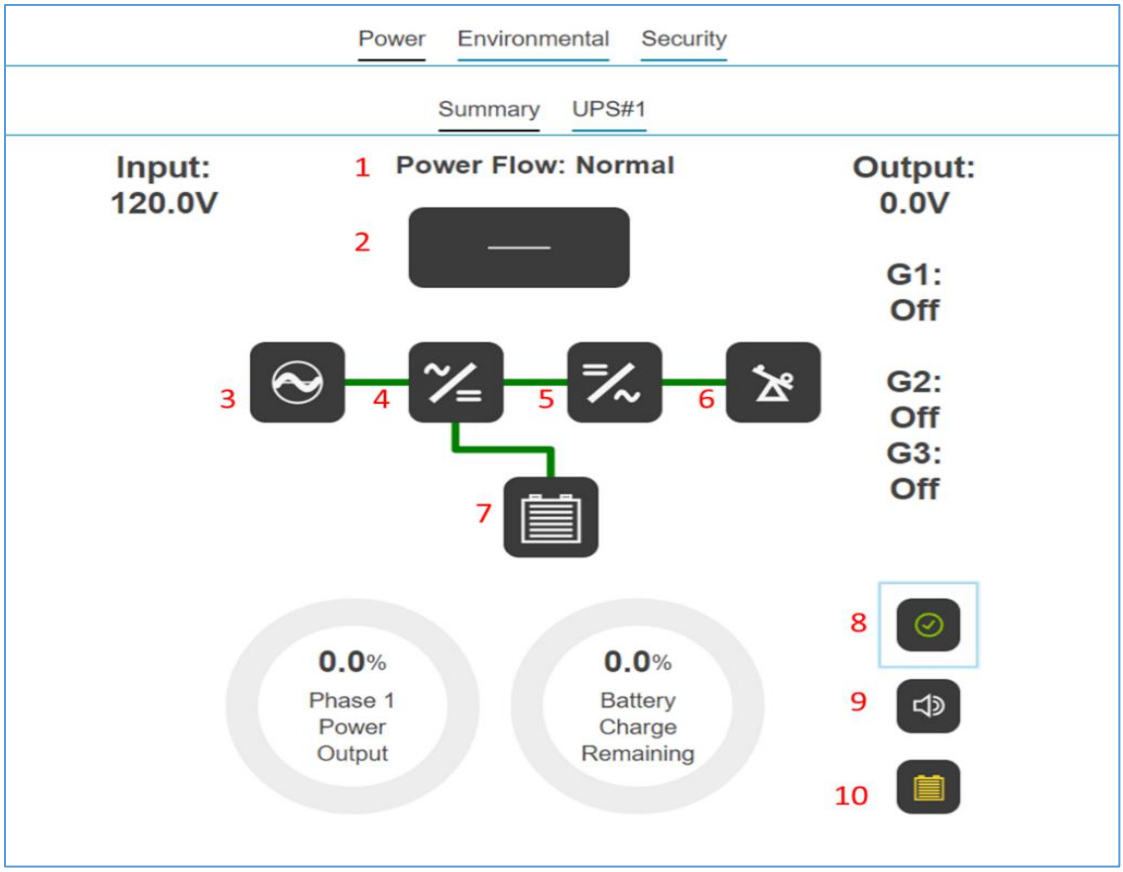


Figure 11: Power Summary Page

NUMBER	DESCRIPTION
1	Power flow of the system. The state will be Normal, Bypass or On Battery, None
2	The bypass component of the UPS
3	The AC input source
4	The AC to DC converter (Rectifier)

5	The DC to AC converter (Inverter)
6	The Output Load
7	The Battery
8	Alert Summary. Clicking on the icon will give a summary of the system.
9	Speaker Status. If the audible alarm is enabled.
10	Battery Status

UPS Monitoring Page

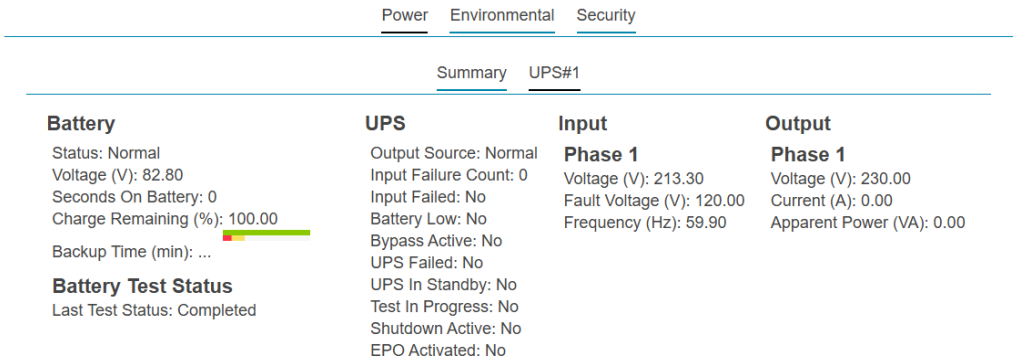


Figure 12: UPS Monitoring Page

Environmental Monitoring Page

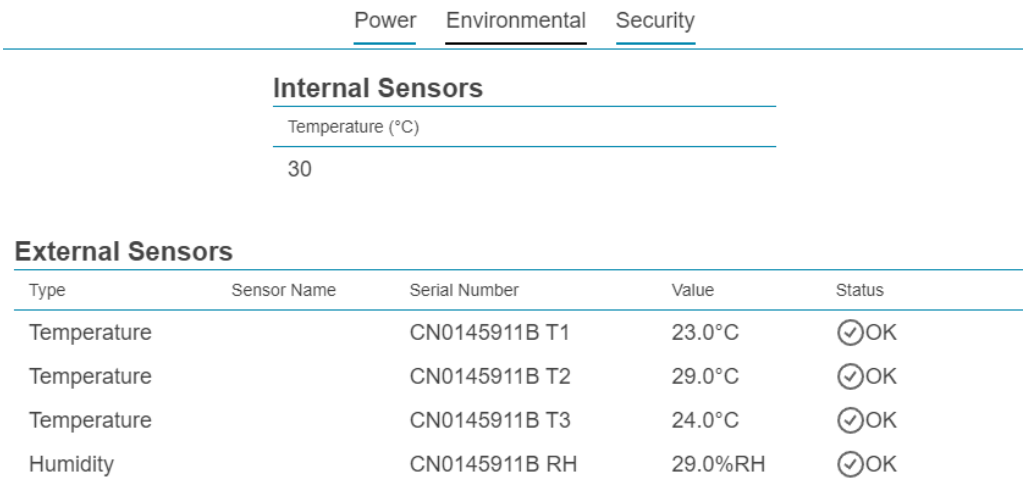


Figure 13: Environmental Monitoring Page

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

Security Monitoring Page

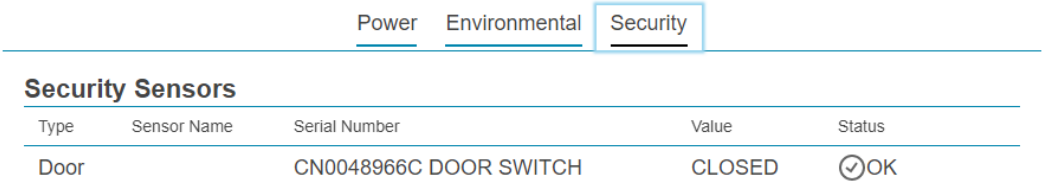


Figure 14: Security Monitoring Page

System Management Information

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

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

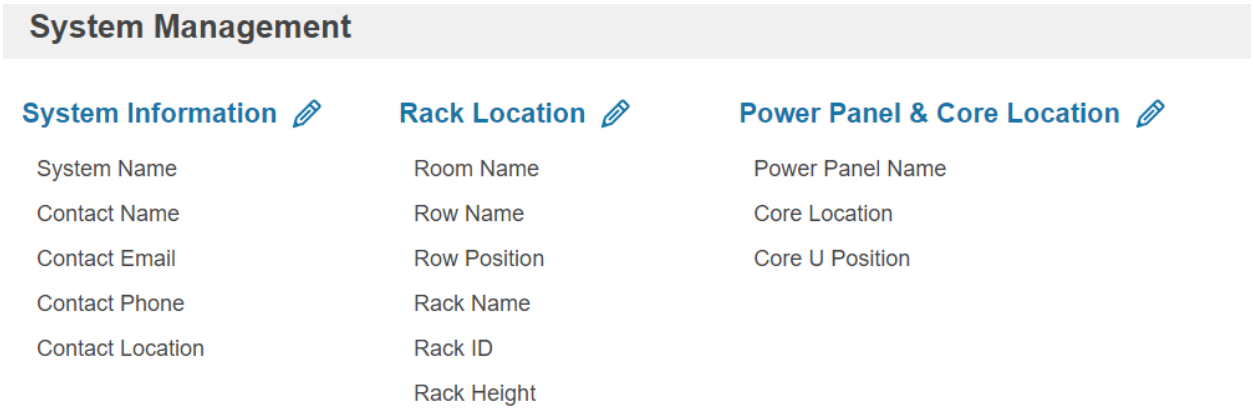


Figure 15: System Management

System Info

The system information includes the name of the UPS 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.**

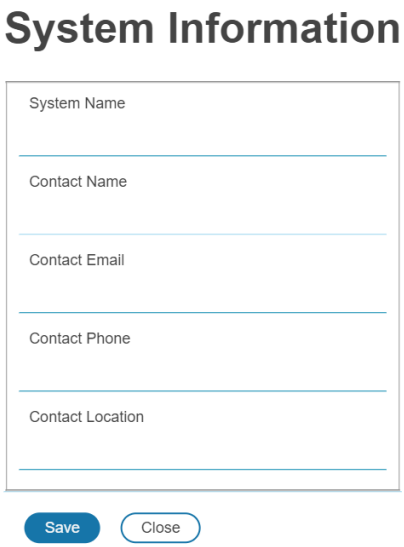


Figure 16: System Information Configuration

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**.

Rack Location

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

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

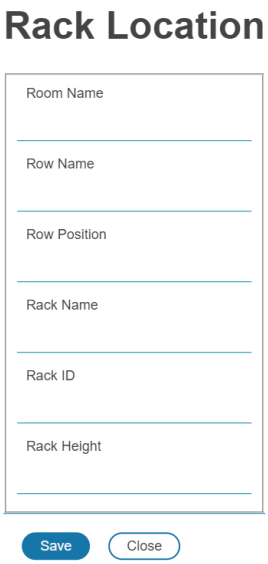


Figure 17: Rack Location Configuration

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

Power Panel & Core Location

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

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

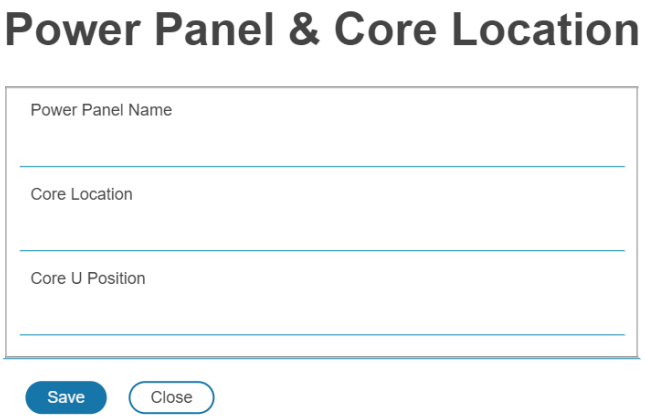


Figure 18: Power Panel & Core Location

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

Network Settings

The Network Settings allow management of IP Configuration, DNS, Web Access, and SSH Configuration.

Ethernet Interface Configuration:

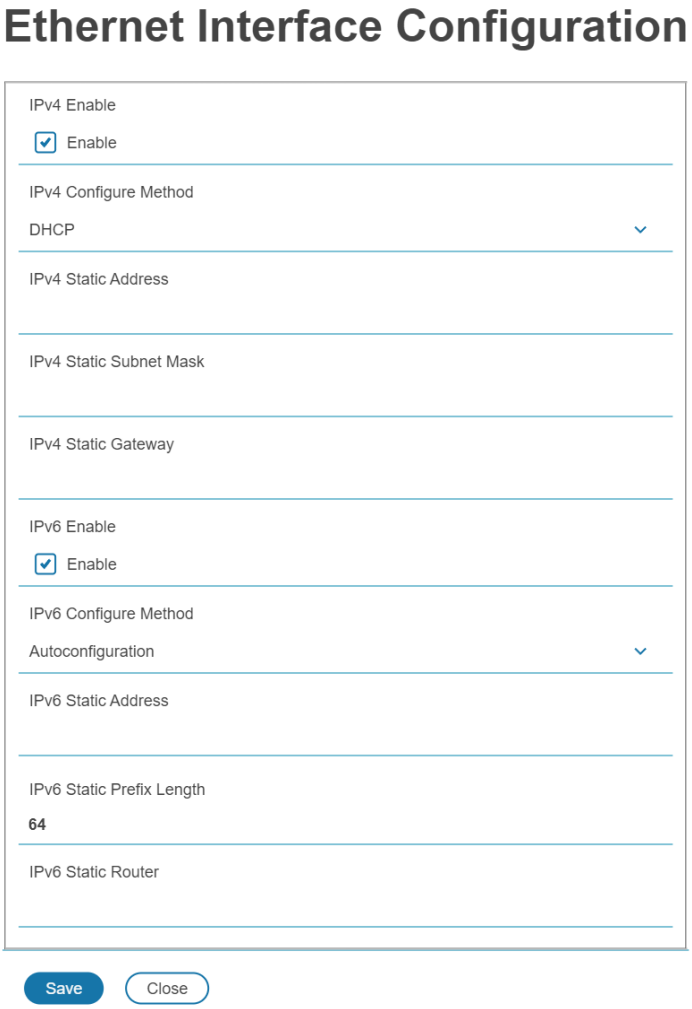


Figure 19: Ethernet Interface Configuration

DNS configuration:

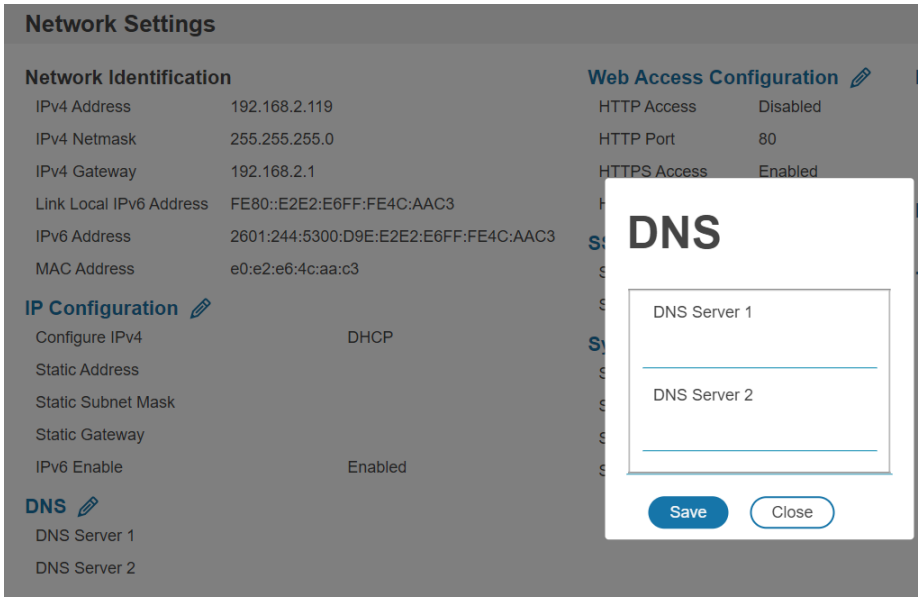


Figure 20: DNS Configuration

mDNS (Multicast DNS)

The NMC uses mDNS (Multicast DNS, RFC 6762) to advertise its presence on the local network. mDNS is enabled by default and operates on UDP port 5353.

The device advertises the following mDNS hostname:
`upsnmc-<macaddress>.local`

For example: `upsnmc-000F9C03000B.local`

This hostname resolves to the device's current IP address (DHCP-assigned or Auto IP) and can be used to access the web interface and SSH without knowing the IP address in advance. It is useful for initial commissioning and for networks where the IP address may change.

What mDNS broadcasts: - The device hostname in the format above - The device's current IP address - Advertised services: `_https._tcp` (web UI, port 443) and `_ssh._tcp` (SSH, port 22)

Web Access Configuration

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

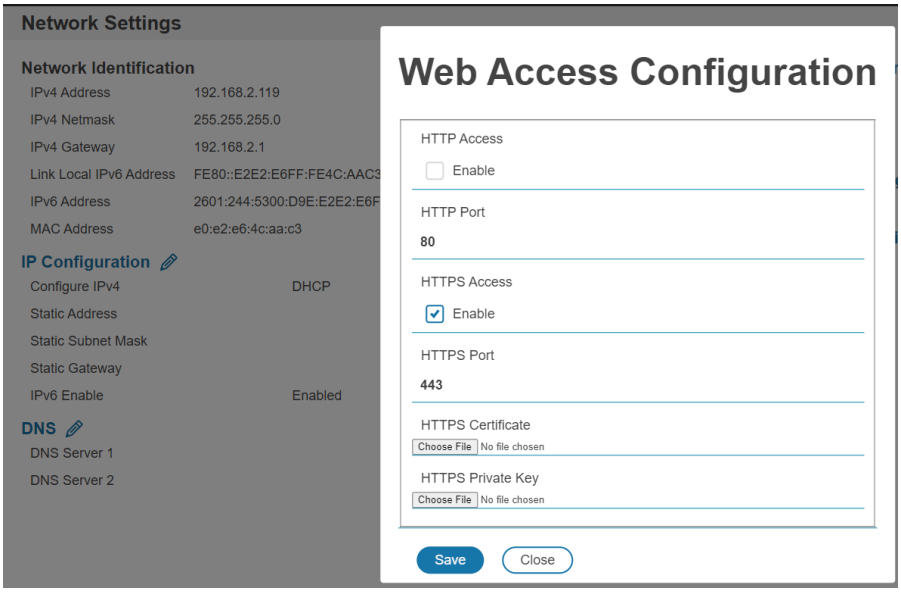


Figure 21: Web Access Configuration

SSH Configuration:

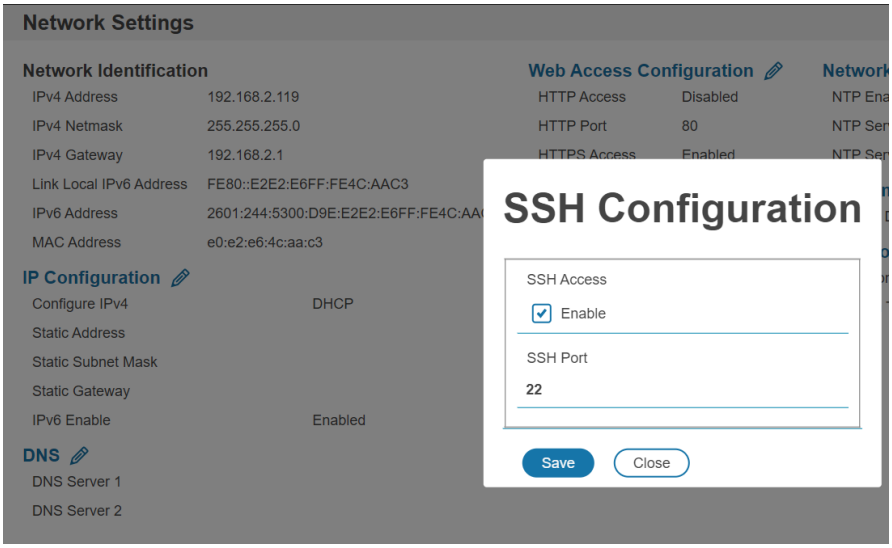


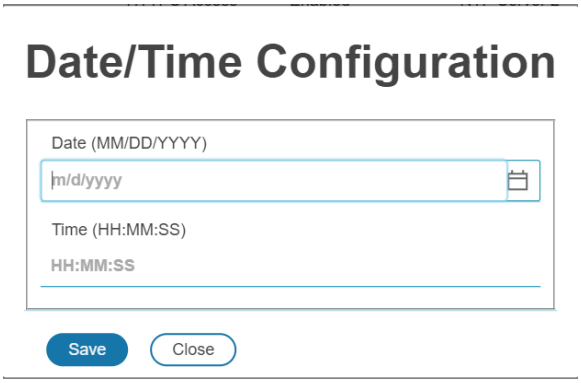
Figure 22: SSH Configuration

Setting Time and Date on the NMC

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

Manually Setting Time and Date

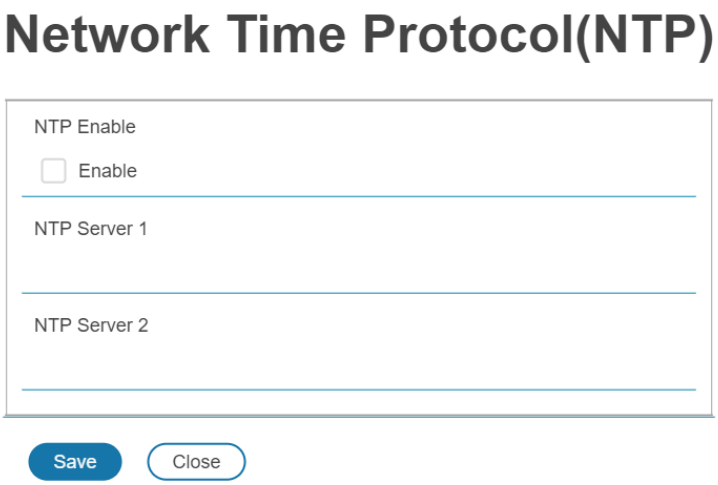
1. Go to **Date & Time** and select **Date/Time Configuration**.



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 displayed in 24-hour format. Enter 2 for 2:00am, 14 for 2:00pm, etc.
4. Press **Save**.

Configure Network Time Protocol (NTP)

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

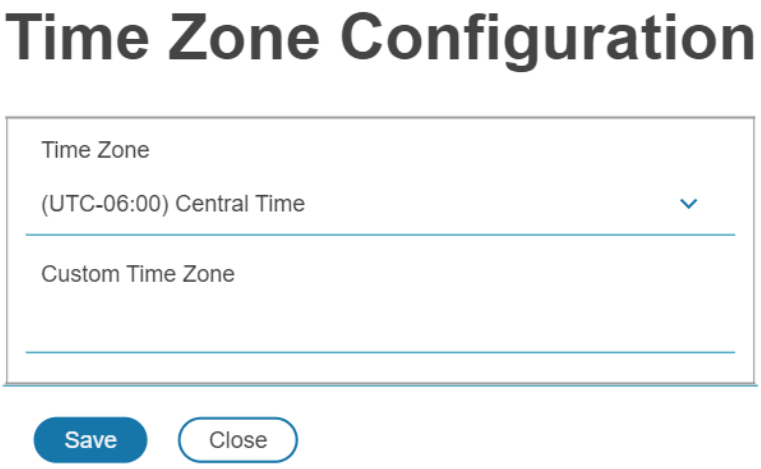


2. Click **Enable** to enable NTP.
3. Enter the hostname or IP address of the primary NTP server in the **Primary NTP Server** field.

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 **Date & Time** and select **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 POSIX time zone in the **Custom Time Zone**:
   - The POSIX format is local_timezone,date/time,date/time.
   - For more information on the POSIX time zone formats see Appendix F: POSIX Time Zone Information.

Control & Manage

The Control and Manage section of the Web GUI will allow a user to control the functionality of the system. These areas include the audible alarm, outlet control and battery test. Control & Manage also include management of Panduit's Smart Load Shedding.

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

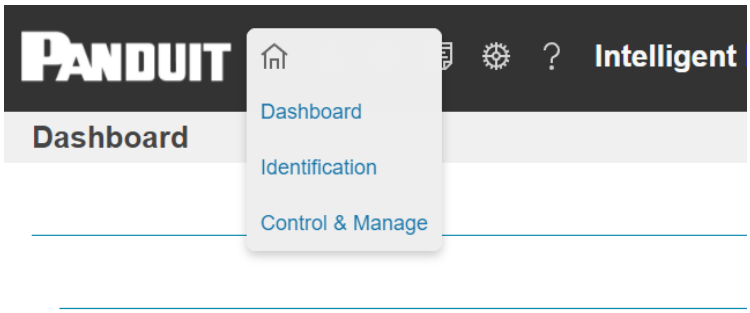


Figure 23: Control & Manage

Audible Alarm

The UPS will emit an audible alarm from certain conditions on the system. To see the list of reasons and the behavior of the audible alarm review the UPS specific user manual. The audible alarm can be enabled of disabled through the Web GUI. Disabling the audible alarm will silence any alarm at the UPS.

1. Select the Home Icon then **Control & Manage** from the drop-down menu in the Web GUI
2. From the UPS tab select pencil next to **Audible Alarm.**

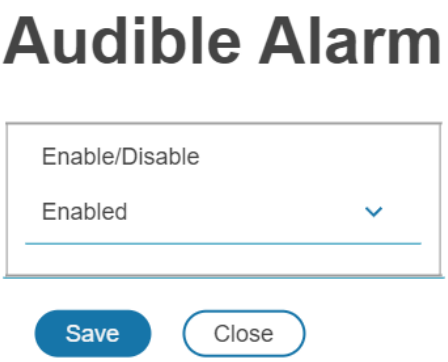


Figure 24: Audible Alarm Configuration

3. Select Enable or Disable.
4. Then select **Save.**

Shutdown

Some UPSes support shutdown functionality to turn off output power.

Enter Shutdown

1. Select the Home Icon then **Control & Manage** from the drop-down menu in the Web GUI
2. Select the **Actions** drop-down menu and choose **Start Shutdown.**

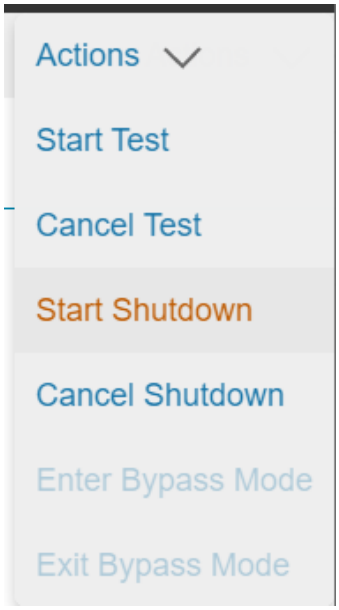


Figure 25: Start Shutdown Example

3. The user will be asked to confirm.
4. Select **YES** to shutdown or select **No** to cancel.

Restore Normal Operation

When the user desired the UPS to transition back to normal operation.

1. Select the Home Icon then **Control & Manage** from the drop-down menu in the Web GUI
2. Select the **Actions** drop-down menu and choose **Cancel Shutdown.**
3. The user will be asked to confirm.
4. Select **YES** to resume normal operation or select **No** to remain in shutdown.

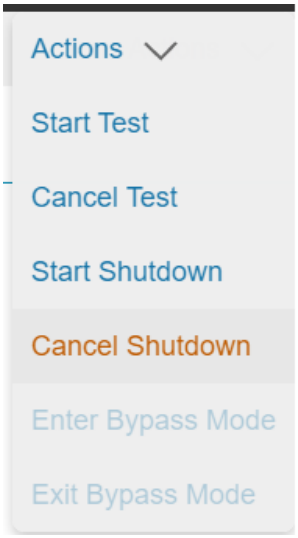


Figure 26: Cancel Shutdown Example

Bypass

Some UPSes support bypass functionality for maintenance purposes.

Manually Enter Bypass

5. Select the Home Icon then **Control & Manage** from the drop-down menu in the Web GUI
6. Select the **Actions** drop-down menu and choose **Enter Bypass Mode.**

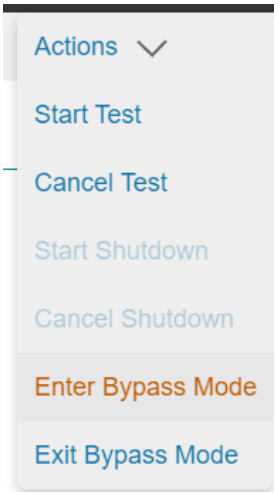


Figure 27: Enter Bypass Example

7. The user will be asked to confirm they want to enter bypass.

8. Select **YES** to enter bypass or select **No** to cancel.

Restore Normal Operation

When the user desired the UPS to transition back to normal operation, the user can exit bypass.

5. Select the Home Icon then **Control & Manage** from the drop-down menu in the Web GUI
6. Select the **Actions** drop-down menu and choose **Exit Bypass Mode.**
7. The user will be asked to confirm they want to exit bypass.
8. Select **YES** to resume normal operation or select **No** to remain in bypass.

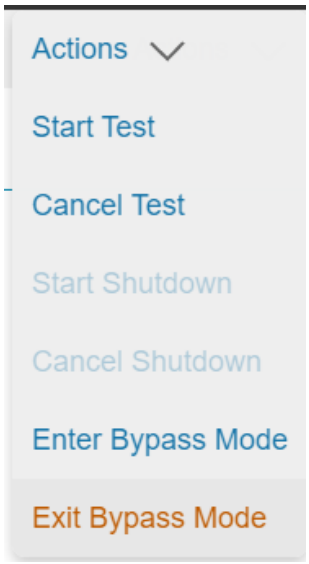


Figure 28: Exit Bypass Example

Battery Test

Manual Battery Test

Running the manual battery test is a two-step process. The user must first configure the type of the test to run and then initiate the test.

Manual Test Configuration

1. Select the Home Icon then **Control & Manage** from the drop-down menu in the Web GUI
2. From the UPS tab select pencil next to **UPS Manual Test.**

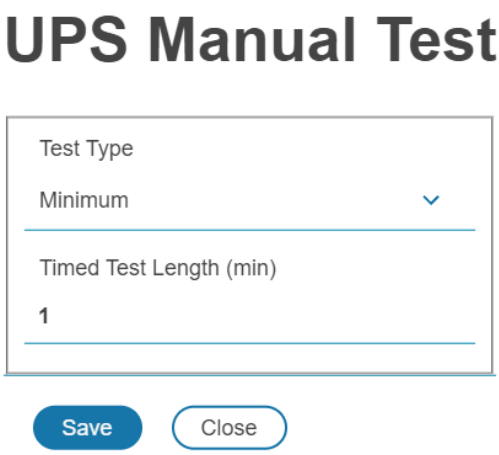


Figure 29: UPS Manual Test Configuration

3. Select the **Test Type** from the pull-down menu. The options are
    a. **Minimum**: This is a quick test of the battery
    b. **Timed**: Test the battery for the configured time.
    c. **Full Discharge**: Places the system on the battery for a full discharge.

    Note: The **Full Discharge** test leaves the battery in the low charge state.
4. If the test selected is **Timed** select the number of minutes to run the test.
5. Then select **Save**

Manual Test Start

1. Select the Home Icon then **Control & Manage** from the drop-down menu in the Web GUI
2. Select the **Actions** drop-down menu and choose **Start Test.**

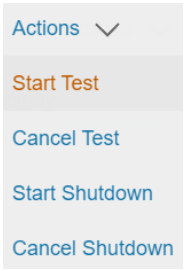


Figure 30: Start Test Example

3. The user will be asked to confirm they want to start the battery test.

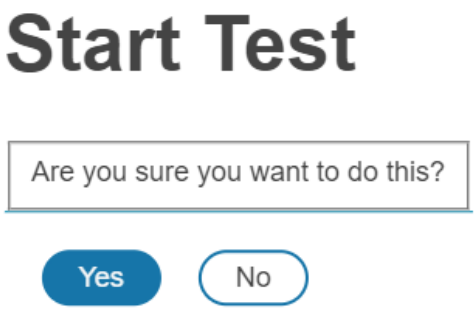


Figure 31: Start Test Confirmation

4. Select **YES** to start the test or select **No** to cancel.

Cancel In progress Manual Test

1. Select the Home Icon then **Control & Manage** from the drop-down menu in the Web GUI
2. Select the **Actions** drop-down menu and choose **Start Test.**

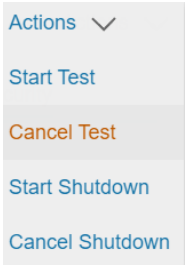


Figure 32: Cancel Test Example

3. The user will be asked to confirm they want to cancel the in progress battery test.

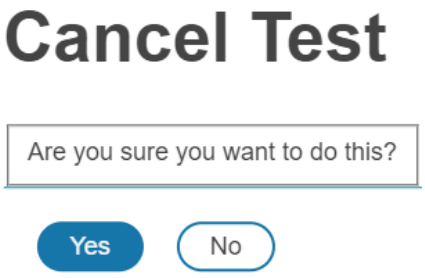


Figure 33: Cancel Test Confirmation

4. Select **YES** to cancel the test or select **No** to continue with the in-progress test.

Running the manual battery test is a two-step process. The user must first configure

the type of the test to run and then initiate the test.

Periodic Battery Test

The system can be enabled to automatically run a periodic battery test. When the test is schedule to execute, the system will run the minimum battery test.

Battery Test Configuration

1. Select the Home Icon then **Control & Manage** from the drop-down menu in the Web GUI
2. From the UPS tab select pencil next to **Battery Test.**
3. To enable the test, click on the box next to enabled. Leaving the box unclicked will leave the test disabled.
4. Enter a **Period** for the test. The period will be the number of days between the test executions.
5. Then select **Save.**

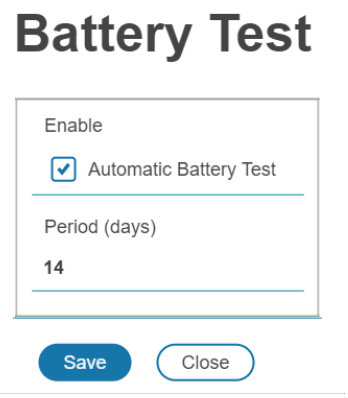


Figure 34: Battery Test Configuration

UPS Main Output Mode

The Output Mode setting controls the mode of operation and sets the output voltage. Output mode is overridden if the UPS is in bypass or running on battery. The UPS must be in bypass mode to change the output voltage. See the specific UPS user manual for details on each mode.

1. Select the Home Icon then Control & Manage from the drop-down menu in the Web GUI.
2. From the UPS tab select pencil next to **UPS Main Output.**
3. Select the desired mode from the drop-down menu.
4. Select the desired output voltage from the drop-down menu.
5. Select the desired output frequency from the drop-down menu.
6. Then select **Save.**

Note. To change the output voltage on single-phase UPS units rated above 5 kVA, turn off the inverter before adjusting the voltage setting; for three-phase units, first change the operating mode to CF, then turn off the inverter to adjust the voltage. The UPS output power will be interrupted during this procedure.

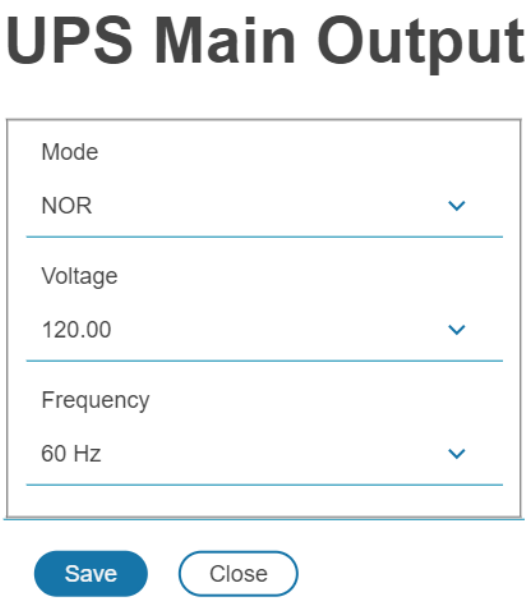


Figure 35: UPS Output Mode

UPS Main Input

The UPS Main Input sensitivity level setting is available on certain UPS models. This can be changed depending on the quality of the input power. If the UPS is experiencing frequent abnormal input warnings, this input sensitivity setting may be adjusted to help resolve the issue. The input sensitivity setting is preserved through the NMC after power cycling of the UPS.

Note: By decreasing the input sensitivity level there is some expected increase to the average transfer time. This is the time expected for the loads to transfer to battery power if the main input is lost.

1. Select the Home Icon then Control & Manage from the drop-down menu in the Web GUI.
2. From the UPS tab select pencil next to **UPS Main Input.**
3. Select the desired **Input Sensitivity** from the drop-down menu.
    a. **P1** – High sensitivity. (Transfer time: 10.5 ms)
    b. **P2** – Medium sensitivity. (Transfer time: 11.9 ms)
    c. **P3** – Low sensitivity. (Transfer time: 13.3 ms)

4. Then select **Save.**

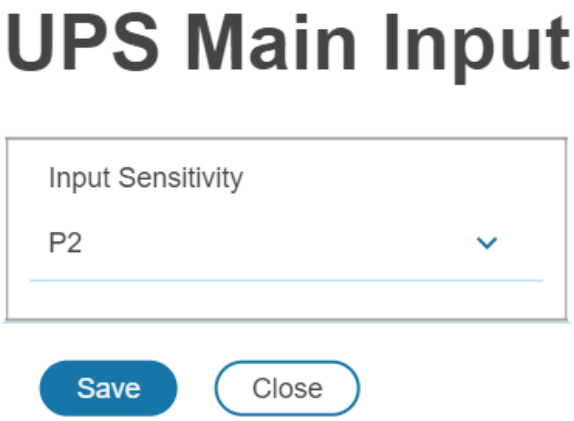


Figure 36: UPS Main Input Setting

UPS Bypass Voltage Limit

The bypass voltage limit sets the upper and lower voltage limit when bypass is not available. Not all values are valid, and it automatically adjusts to a valid input if invalid values are entered. See the specific UPS user manual for details and valid values.

1. Select the Home Icon then Control & Manage from the drop-down menu in the Web GUI.
2. From the UPS tab select pencil next to **UPS Bypass Voltage Limit.**
3. Enter the upper voltage limit and lower voltage limit.
4. Then select **Save.**

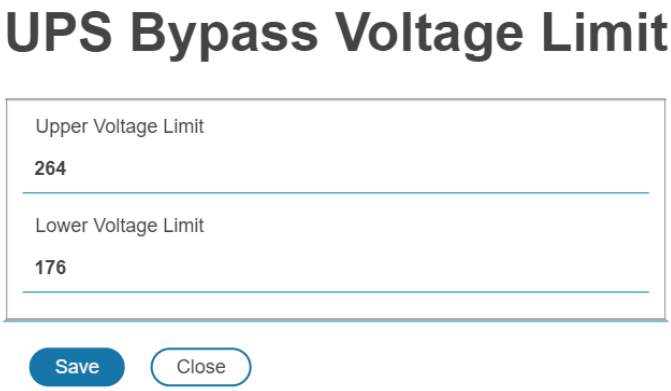


Figure 37: UPS Bypass Voltage Limit configuration

UPS Battery Information

The battery information shows the current battery configuration and the installation date. When the battery configuration changes or new batteries are installed, this information needs to be updated from this page or from the UPS

1. Select the Home Icon then Control & Manage from the drop-down menu in the

Web GUI.

2. From the UPS tab select the pencil next to **Battery Information.**
3. 1-3kVA VRLA models have internal batteries rated for 9Ah (the pre-programmed value). Each external battery pack (EBP), if used, adds 18Ah of additional capacity. Change the **Battery Capacity (Ah)** field according to the number of EBPs connected to each UPS (a maximum of 4). For example:

- UPS internal batteries only: 9
- UPS internal batteries (9) + 1 EBP (18) = 27
- UPS internal batteries (9) + 2 EBP (36) = 45
- UPS internal batteries (9) + 3 EBP (54) = 63
- UPS internal batteries (9) + 4 EBP (72) = 81

Number of Batteries and **Battery Installation Date** may be used for record-keeping, but they do not affect the runtime calculations.

Select **Save.**

4. 5-20kVA models do not have internal batteries; by default, they are shipped with (1) EBP. Thus, these UPS employ the **Number of Batteries** field to quantify additional battery capacity.
5. Change the **Number of Batteries** field to match the number of EBP(s) connected to each UPS. The default will be (1), and the maximum will depend on the battery type:
   - 5-10kVA VRLA UPS will support a maximum of 5 EBPs
   - 5-10kVA Lithium UPS will support a maximum of 8 EBPs
   - 10-20kVA Three Phase VRLA UPS will support a maximum of 8 EBPs
6. Input the correct EBP count for each UPS and select **Save.**

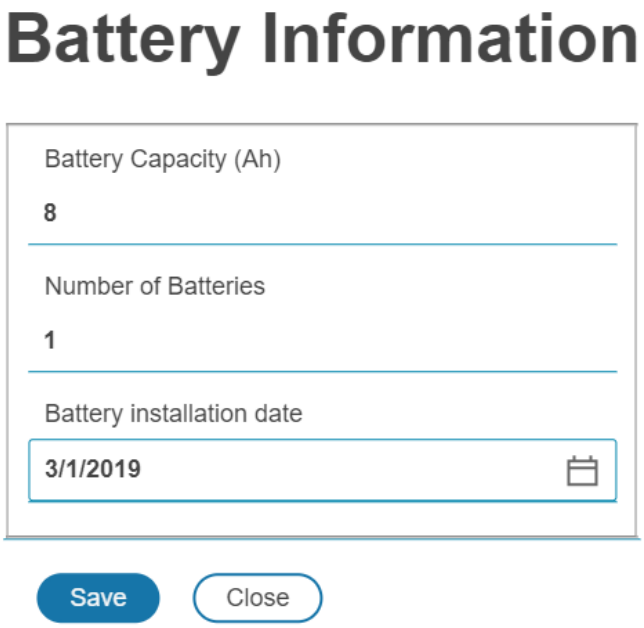


Figure 38: Battery Information configuration

Outlet Group Control

Naming an Outlet Group

For Panduit UPS with outlet group control, you can customize each outlet group through the Web GUI.

1. Select the Home Icon then Control & Manage from the drop-down menu in the Web GUI
2. In the Control & Manage and select, the **Outlet Groups** tab.

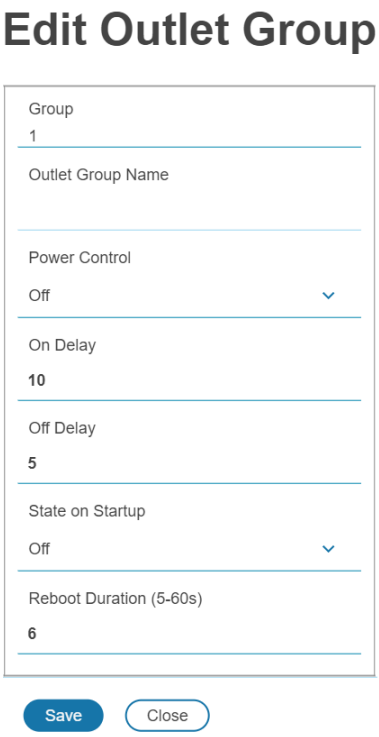


Figure 39: Edit Outlet Group

3. Select the outlet group by clicking on the pencil icon on the right. In the data panel, select the value field for the **Outlet Group Name**.
4. Delete the default name and type the new name.
5. Press **Save**.

Setting the Outlet Group Default State

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

1. Select the Home Icon then Control & Manage from the drop-down menu in the Web GUI
2. In the Control & Manage and select, the **Outlet Groups** tab.
3. Select the outlet group by clicking on the pencil icon on the right.
4. In the settings dialog box, choose a selection from the **State on Startup** dropdown menu:
   - **On**: this will turn an outlet group on upon initial startup
   - **Off**: this will turn an outlet group off upon initial startup
   - **Last**: this will restore outlets to the last known power states before the device was shut down

     Note: If outlet group 1 is off, all other outlet groups will automatically be turned off.

Switching an Outlet Group On or Off

This is only applicable to outlet groups switched UPSs. Outlets Groups on the switched UPS models are easily switched on, switched off, or rebooted. This action requires the user to have Administrator or Controller Privileges.

Enabling Manual Outlet Group Control

1. Select the Home Icon then Control & Manage from the drop-down menu in the Web GUI
2. In the Control & Manage and select, the **Outlet Groups** tab.
3. Select the pencil next to **Outlet Group Control**

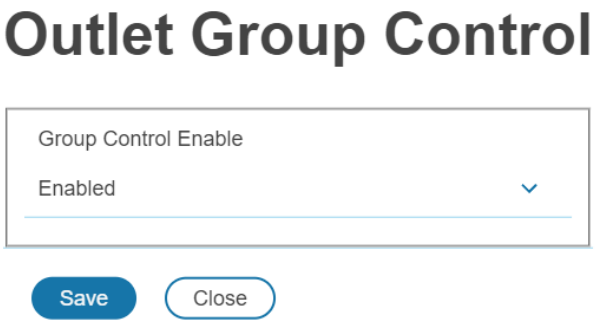


Figure 40: Outlet Group Control

4. Select **Enable** in the pull down to enable manual outlet group control or **Disabled** to disable manual outlet control

Changing the state of the outlet group

1. Select the Home Icon then Control & Manage from the drop-down menu in the Web GUI
2. In the Control & Manage and select, the **Outlet Groups** tab.
3. Select the outlet group by clicking on the pencil icon on the right.
4. Select the desired **Power Control** from the dropdown menu.
5. Select Save.

Available power control options:

Off Orderly: Send shutdown commands to all smart loads on the outlet group, wait “Off Delay”, then remove power from the outlet group.

Off: Immediately remove power from the outlet group.

Off Delayed: Wait “Off Delay” then remove power from the outlet group.

Reboot Orderly: Send shutdown commands to all smart loads on the outlet group, wait the programmed delay, then remove power from the outlet group.

Wait “Reboot Duration” then restore power to the outlet group.

Reboot Delayed: Wait “Off Delay” then remove power from the outlet group. Wait “Reboot Duration” then restore power to the outlet group.

Reboot Immediately: Immediately remove power from the outlet group. Wait “Reboot Duration” then restore power to the outlet group.

On: Immediately restore power to the outlet group.

On Delayed: Wait “On Delay” then restore power to the outlet group.

Setting the Outlet Power On/Off Delay for Panduit NMCs

This is only applicable to outlet group switched UPS.

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

Outlet Power Sequence Setup

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

1. Select the Home Icon then Control & Manage from the drop-down menu in the Web GUI
2. For each Outlet Group select the **Edit** pencil.

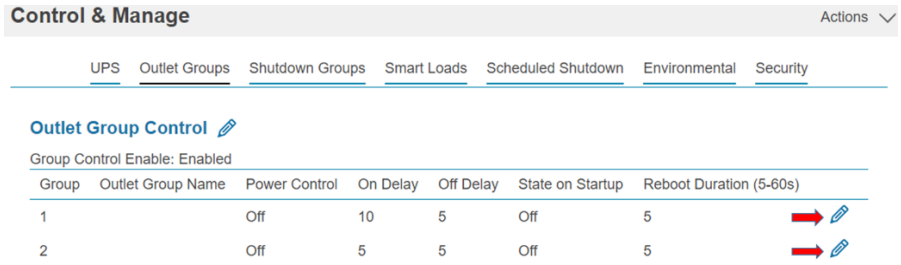


Figure 41: Edit Outlets

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

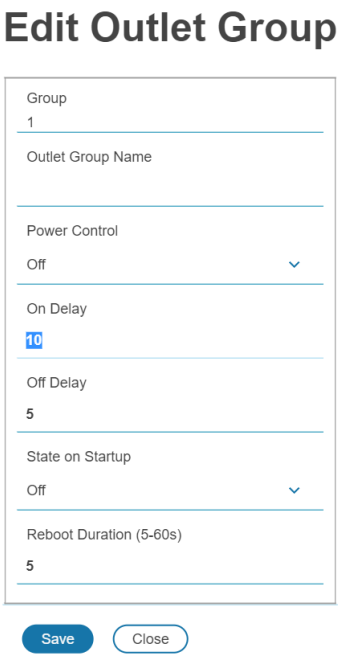


Figure 42: One Delay Time

4. Your Outlet Power Sequence has been set.

Note: If outlet group 1 is off, all other outlet groups will be automatically turned off. Setting a delay of outlet group 1 longer than outlet group 2 will keep outlet group 2 off until outlet group 1 is turned on.

Panduit's Smart Load Shedding

Panduit's Smart Load shedding allows the UPS to be configured to shed different loads depending on the configuration of the Shutdown Groups in order to maintain the battery for higher priority equipment.

Panduit's Smart Load Shedding Configuration Overview

The first step is to decide how the devices will be grouped into Shutdown groups in the system. Each shutdown group will be the group of devices with similar priorities and connected to the same outlet group.

Once the groupings are decided, configure the shutdown groups to maximize the UPS battery to mission critical devices. Groups with lower priorities should be configured to turn off sooner than groups with higher priorities.

Next, configure any Smart Loads connected to the system to be properly shut down. A Smart Load is a device that can be shut down by a CLI command over an SSH

connection or a Windows device running the Panduit Shutdown Agent.

Finally, add the Smart Load to the correct Shutdown Group.

Panduit's Smart Load Shedding Workflow

Once the criteria for the shutdown are met, the Shutdown Group will begin the process of shutting down the Shutdown Group.

First, it will shut down all the Smart Loads associated to the group. The UPS will connect to each of the Smart Loads associated with the Smart Group via SSH and issue the shutdown command.

After all Smart Loads are shutdown, the Shutdown Group will look at the associated outlet group. If the Shutdown Group is the last remaining Shutdown Group turned on associated with the outlet group and any of the Shutdown Groups associated to that outlet have "Request Group Off" enabled, the outlet group will be immediately turned off.

Note: If outlet group 1 is off, all other outlet groups will be automatically turned off. If outlet group 2 is on, outlet group 1 will not be turned off until outlet group 2 is turned off.

Once the system is up and running a normal state, the shutdown groups can be restored. If any of the shutdown groups that were shut down are marked "Restore After Shutdown", the power will be restored to the outlet group after the system returns to a normal state.

Shutdown Groups Configuration

To configure the Shutdown groups, follow these simple steps.

1. Select the Home Icon then Control & Manage from the drop-down menu in the Web GUI
2. Select the **Shutdown Groups** tab.
3. For each Shutdown Group select the **Edit** pencil.

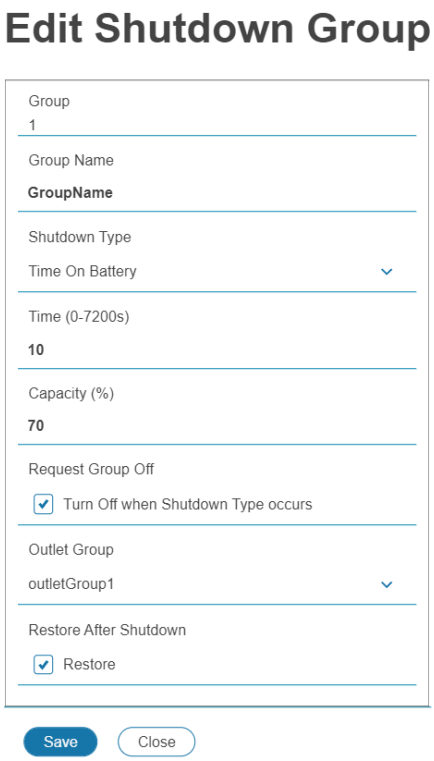


Figure 43: Shutdown Group Configuration

4. Name the group. The **Group Name** is the name of the shutdown group to allow the user to denote the type of devices in the group.

5. Select the **Shutdown Type**. The Shutdown Type is ether **Time on Battery** or **Battery Capacity.**

    a. **Time on Battery –** The Shutdown Group will be shut down after the configured time.

    b. **Battery Capacity –** The Shutdown Group will be shut down when the capacity drops below the configured capacity.

6. Set the **Time.** Time is the number of seconds after the system switches to the battery the Shutdown Group with be shut down, if it is configured to Shutdown Type of Time on battery.

7. Set the **Capacity.** The Shutdown Group will be shut down if the battery capacity falls below the configured thresholf, if it is configured to Shutdown Type of Battery Capacity.

8. If **Request Group Off** is selected, the associated Outlet Group will be shut down when the Shutdown group is shutdown.

9. Select the **Outlet Group** that is associated with the Shutdown Group.
10. If **Restore After Shutdown** is selected, the associated Outlet Group will be toggle when the system transitions off the battery.

Smart Loads Configuration

Smart Loads are connected devices to the UPS that would need to be shutdown gracefully before the system's battery is depleted. To configure the Smart Loads, follow these simple steps.

1. Select the Home Icon then Control & Manage from the drop-down menu in the Web GUI
2. Select the **Smart Loads** tab.
3. For each Smart Load select the **Edit** pencil.

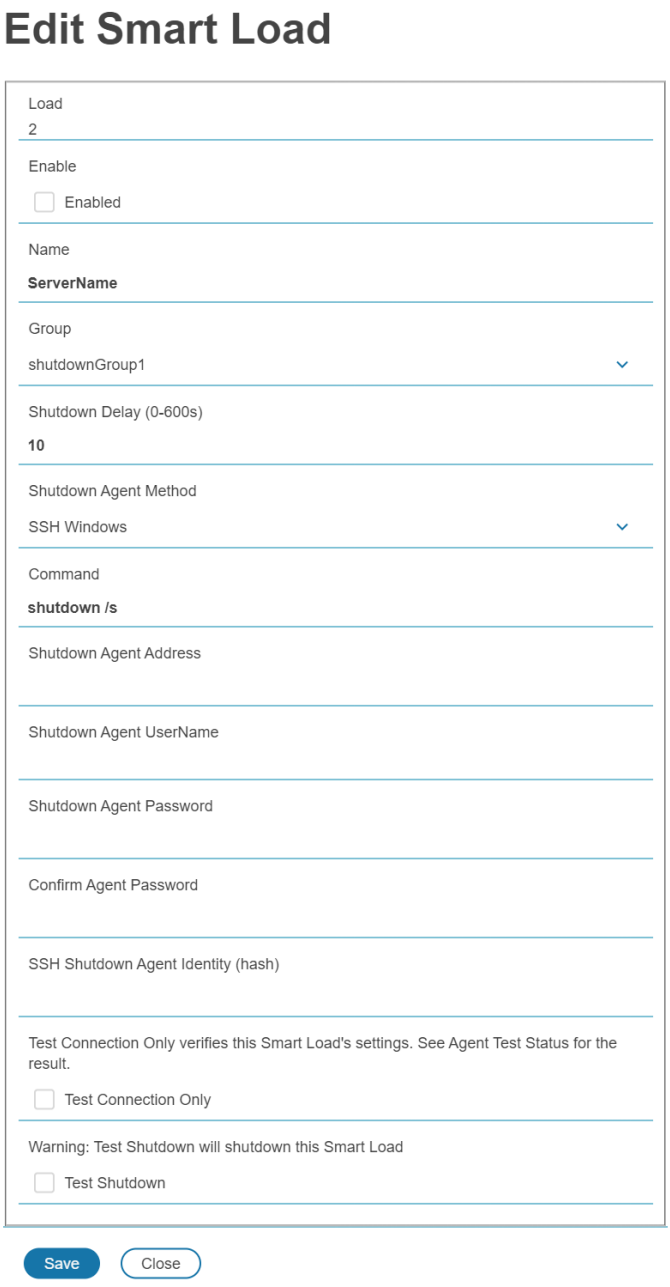


Figure 44: Smart Load Configuration

4. Enable the Smart Load by selecting **Enable.** If the Smart Load is not enabled, it will not be shut down when the associated shutdown group is shut down.
5. The **Name** will allow the user to associate a more meaningful name to the device.
6. Under **Group**, select which Shutdown Group is associated to this Smart Load.
7. The **Shutdown Delay** is the number of seconds the device requires to shutdown

after the NMC sends the shutdown command. This number should include extra margin so there is no risk the device will lose power before shutdown is complete.

8. For ease of operation, you can select one of the common agent shutdown commands. Select one of the following options from the pull down menu.11
    a. SSH Windows – This sends a “shutdown /s” to the remote server.
    b. SSH Linux – This sends “shutdown -P 0” to the remote server.
    c. SSH Linux use sudo - This sends “sudo shutdown -P 0” to the remote server.
    d. SSH Custom Command – This is used to define a custom command. If this is set, the system will send the string defined in **Command.**
9. Next configure the information on how to SSH to the server.
    a. **Shutdown Agent Address –** The address/hostname of the server. The port number can be specified by adding a colon and the port number after the address.
    b. **Shutdown Agent UserName –** The username of the user that will connect to the Smart Load and issue the shutdown command.
    c. **Shutdown Agent Password –** The password of the Shutdown Agent UserName. The password will need to be entered twice.
    d. **SSH Shutdown Agent Identity –** The SSH fingerprint. For the highest level of security, manually enter the SSH fingerprint. It will be automatically updated after the first connection if left blank.
10. Check the test box to verify the configuration after saving.
    a. **Test Connection Only -** This option will verify the configured user can connect to the configured device and can log in but will not issue the shutdown command.
    b. **Test Shutdown -** This option will verify the configured user can connect to the device, log in, and then issue the shutdown command. **NOTE:** The configured device will shutdown.
11. Finally, you can click on the Save button to save the configuration. If no test box is checked, the data will be saved to database without testing the connection.

Scheduled Shutdown

Shutdown groups can be schedule to be shutdown.

1. Select the Home Icon then Control & Manage from the drop-down menu in the Web GUI
2. Select the **Scheduled Shutdown** tab.
3. For each scheduled shutdown, select the **Edit** pencil.

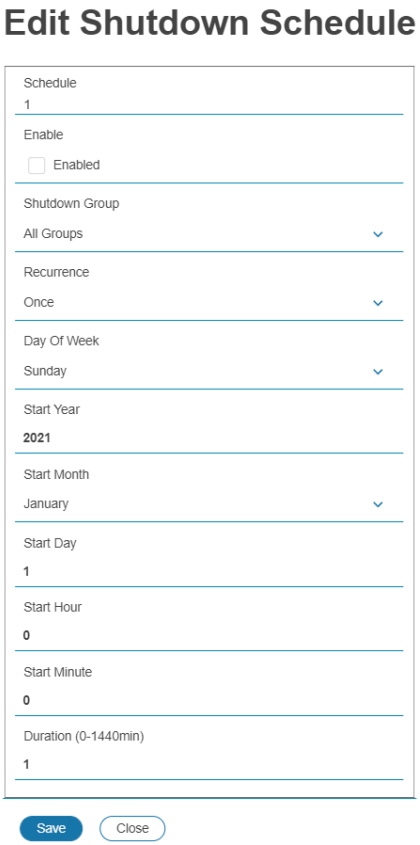


Figure 45: Shutdown Schedule Configuration

4. Enable the schedule shutdown by selecting **Enable.** If the schedule is not enabled, it will not be shut down.
5. Select the associated shutdown groups. The user can select an individual group or **All Groups**
6. Select how often this shutdown will occur.
    a. **Once –** The shutdown will happen once at the configured date and time.
    b. **Daily –** The shutdown will happen every day at the configured time.
    c. **Weekly** – The shutdown will happen once a week at the configured time and day of week.
    d. **First Week, Second Week, Third Week, Fourth Week,** and **Last Week –** The shutdown will occur once a month at the selected week at the configured time and day of week.
7. Configure the date, time, and day of week that the event should first occur.
    a. **Day of Week** – If the recurrence is Weekly, First Week, Second Week, Third Week, Fourth Week, or Last Week the **Day of Week** will determine

which day of the week the shutdown will occur

b. **Start Year, Start Month,** and **Start Day –** The configured day of the first occurrence of the scheduled shutdown.
c. **Start Hour** and **Start Minute –** The configured start time of the first occurrence of the scheduled shutdown.

8. Finally, the **Duration.** The duration is how long the shutdown group will remain shutdown.

Email Setup

The Panduit UPS 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.

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

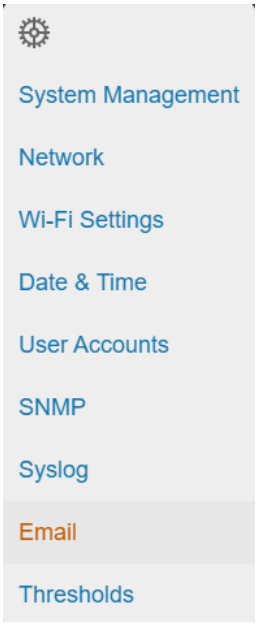


Figure 46: Email Setup

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

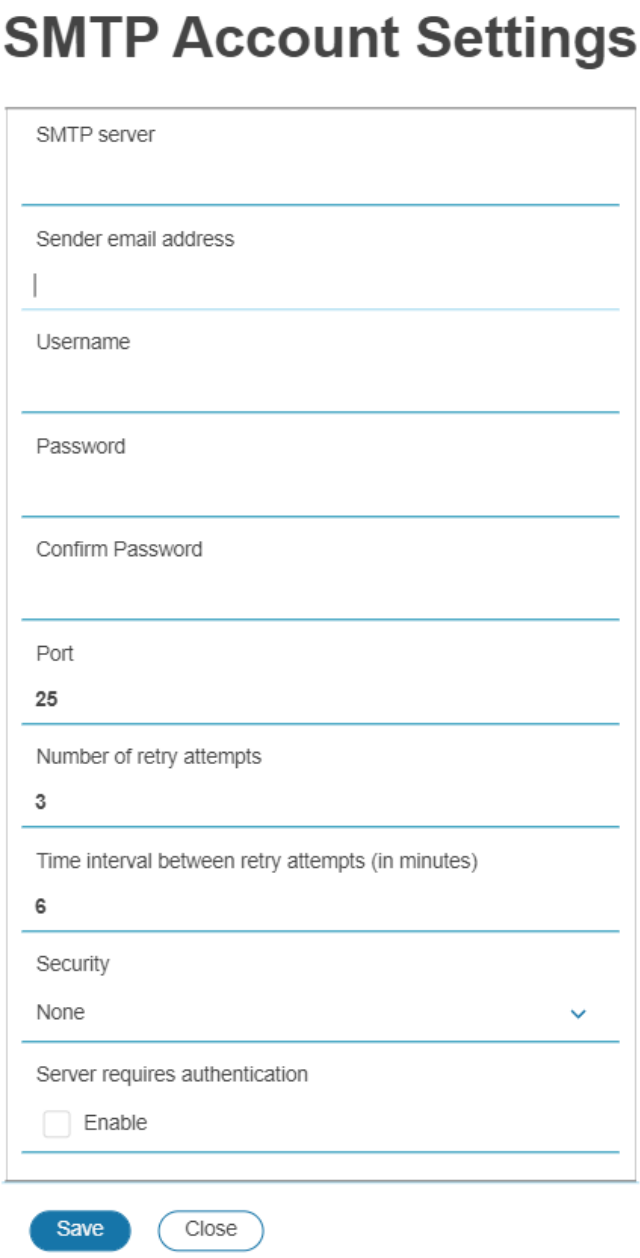


Figure 47: SMTP Account Settings

- 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 that the email is sent from. You could use a unique email address on each UPS or the same email address across all UPSs.

- Configure the **Port** number. The port number is the communication endpoint on the server. The default is 25. Other common SMTP ports are 587 and 465
- If the SMTP server requires authentication, enter the **username** and **password.** These will be determined by the configuration on the SMTP server.
- Set **Number of Sending Retries.** This will be the number of times the UPS will attempt to resend a message if the message fails. The default setting is 3.
- Set **Time Interval Between Sending Retires (In Minutes).** This is the time, in minutes, the NMC will wait before retrying to send a failed message. The default setting is 6 minutes.
- 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.

3. Press **Save** when done.

Next, fill out the Email Recipients list.

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

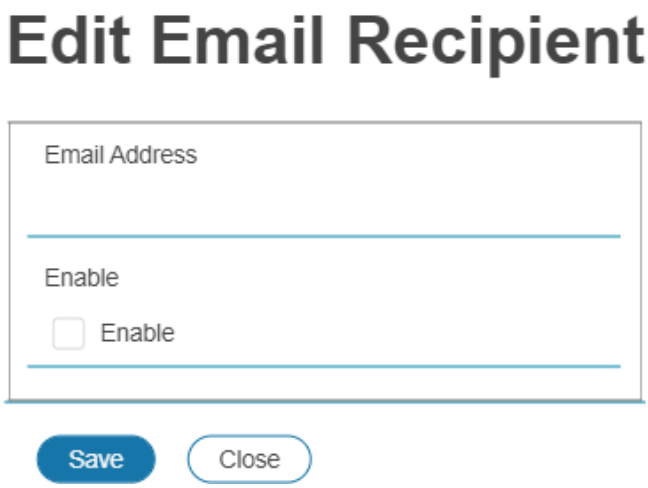


Figure 48: Email Recipient

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

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

Event Log

UPS events and NMC events or alarms are recorded in the event log. Syslog can also be configured to report this to remotely.

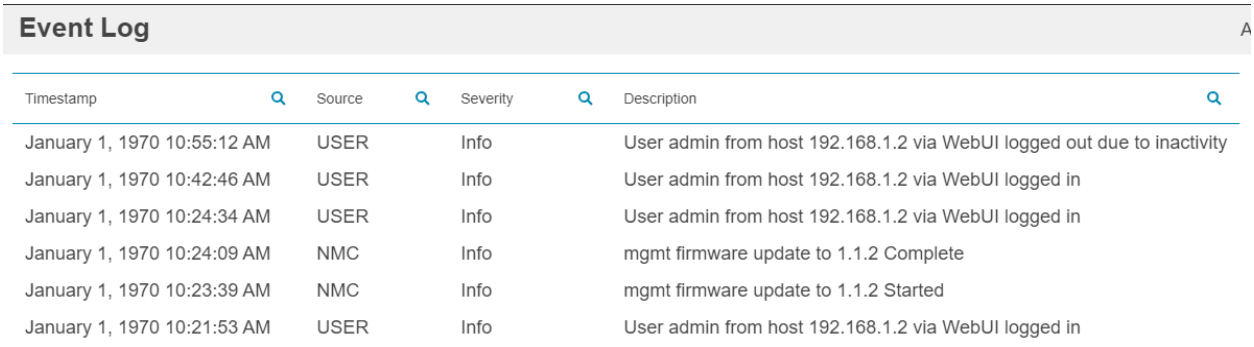


Figure 49: Event log

Event log can be downloaded or cleared from Actions menu.

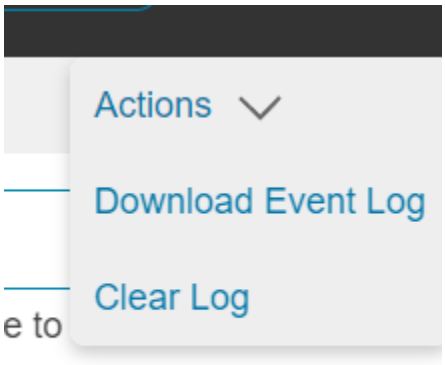


Figure 50: Event log Actions menu

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**.

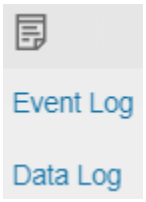


Figure 51: Data Log

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

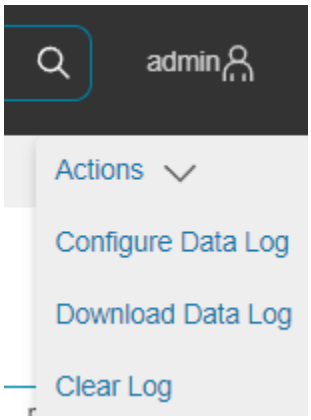


Figure 52: Data Log Configuration

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.)

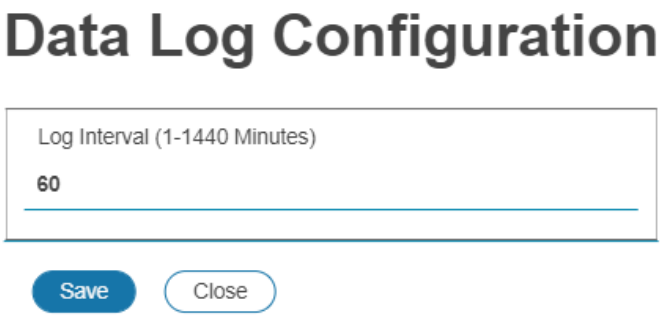


Figure 53: Data Log Configuration Panel

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 UPS 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 UPS functionality, like outlet control and battery test, 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 UPS 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.

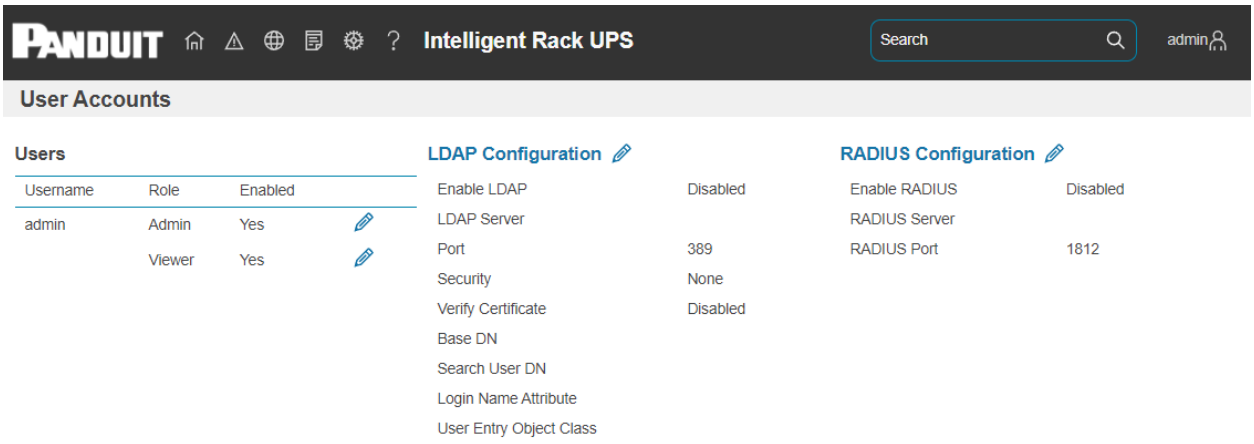


Figure 54: User Accounts

2. Go to **RADIUS Configuration 1 or 2** and click the edit pencil.

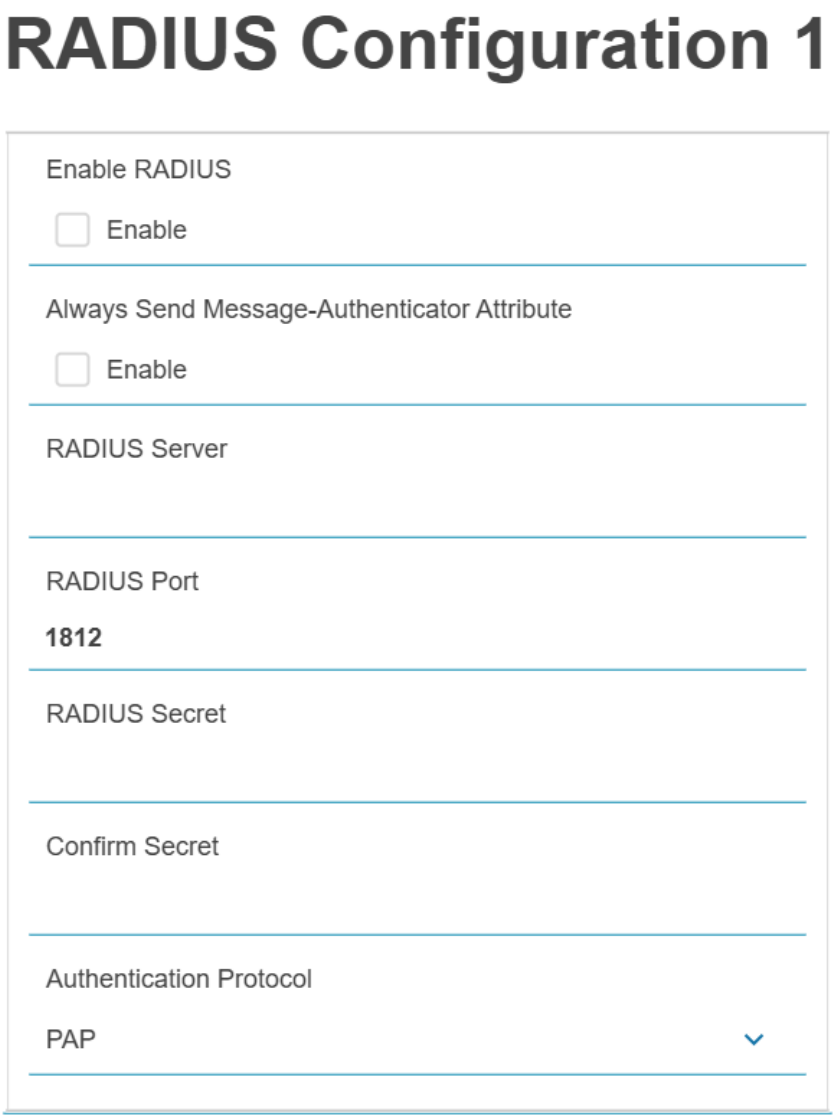


Figure 55: RADIUS Configuration

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

Note: By default, a RADIUS user will have the “viewer” Role if one is not specified. The administrator of the RADIUS server may configure a Panduit vendor (19536) dictionary, with a “User-Role” integer attribute set to User (1) or Admin (2) or Control(3). For complete details, see Appendix E: RADIUS Server Configuration

Configuring the system with LDAP Server Settings

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

1. Go to User Accounts (under the Settings) > LDAP Configuration.
2. Select the LDAP Enable checkbox.
3. Use the drop-down menu to choose the Type of LDAP Server. Choose Microsoft Active Directory.
4. Enter an IP Address of the domain controller/Active Directory (AD) Server.
   e.g. *192.168.1.101*
5. Enter a Port.
   Note: For Microsoft, this is typically 389.
6. Enter the Security. None for unencrypted transmission. StartTLS to upgrade the connection after connect to a TLS connection. TLS to start with TLS connection
7. In the Base DN field, enter in the account to be used to access AD.
   e.g. *CN=myuser,CN=Users,DC=EMEA,DC=mydomain,DC=com*
8. Enter the password in the Bind Password and Confirm Password fields.
9. In the Search User DN field:
   e.g. *DC=subdomain,DC=mydomain,DC=com*
10. In the Login Name Attribute field, enter **sAMAccountName** (typically).
11. In the User Entry Object Class field, enter **person**.

With these LDAP settings configured, the Bind is complete.

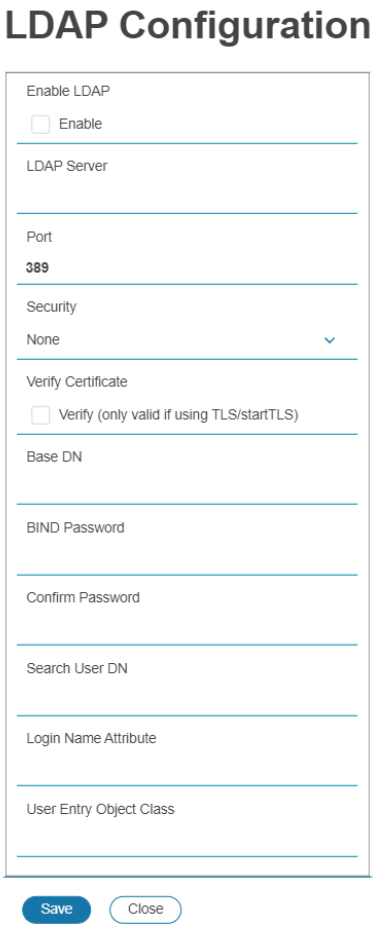


Figure 56: LDAP Configuration

Once LDAP is configured, the UPS must understand for which group authentication occurs. A role must be created on the UPS 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 UPS imposes. However, there may be limits by the LDAP server.

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

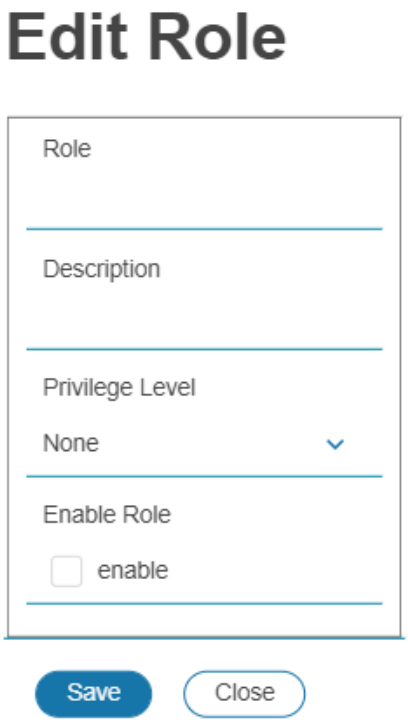


Figure 57: Enable Role Privileges

4. LDAP authentication is ready to use.

Wi-Fi Settings

The UPS NMC can connect wirelessly to a Wi-Fi Network. It can also act as a Wi-Fi access point so the user can connect a computer, mobile phone, or tablet directly to the NMC and 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.

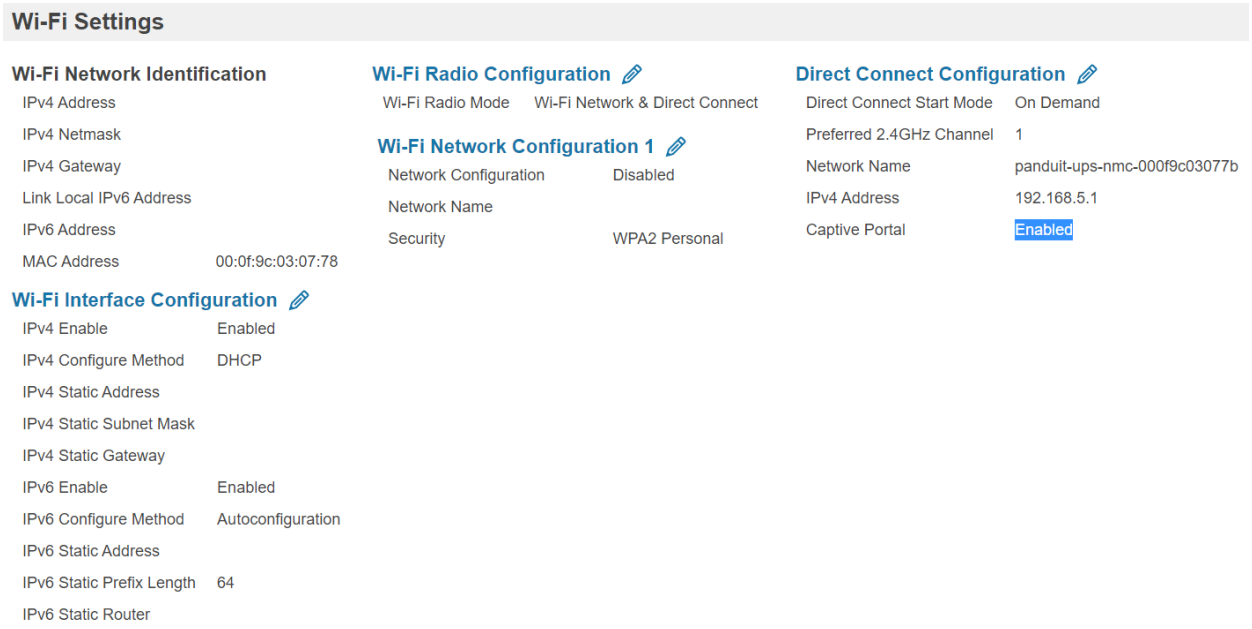


Figure 58: Wi-Fi Settings screen

Configuring Wi-Fi Radio mode

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

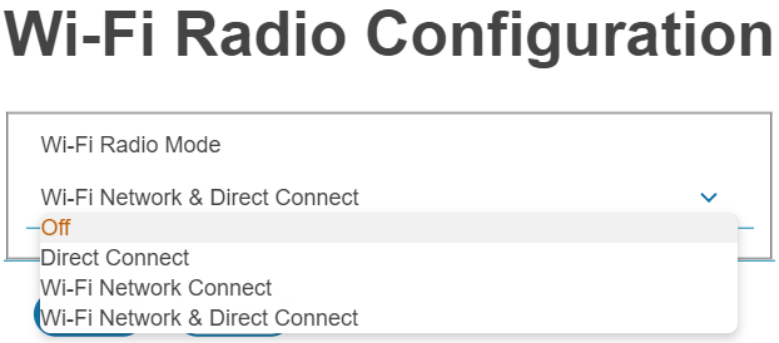


Figure 59: Wi-Fi Radio Configuration

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.

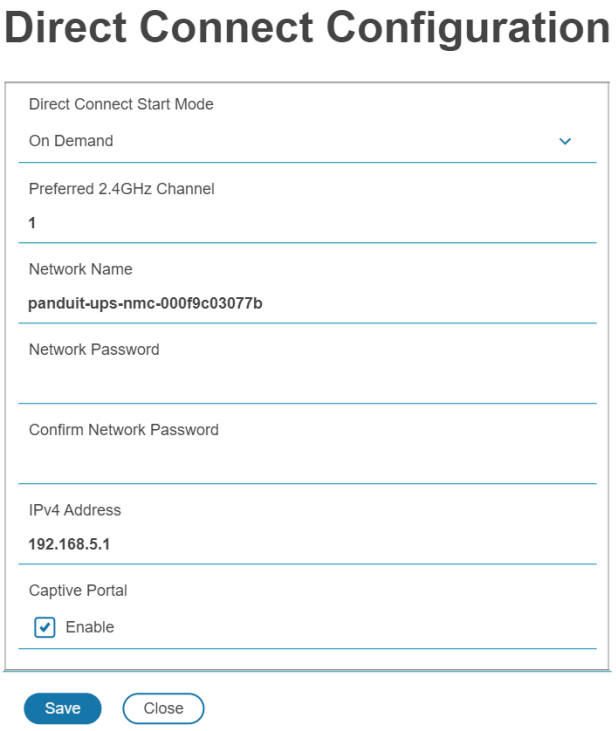


Figure 60: Wi-Fi Direct Connect Configuration

1. Select Start mode option
   - On Demand: Push the reset button to start the Direct Connect mode and it is 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, WPA3 Enterprise. To connect to a Wi-Fi network, the Wi-Fi Network Configuration must match the configuration of the desired Wi-Fi

network.

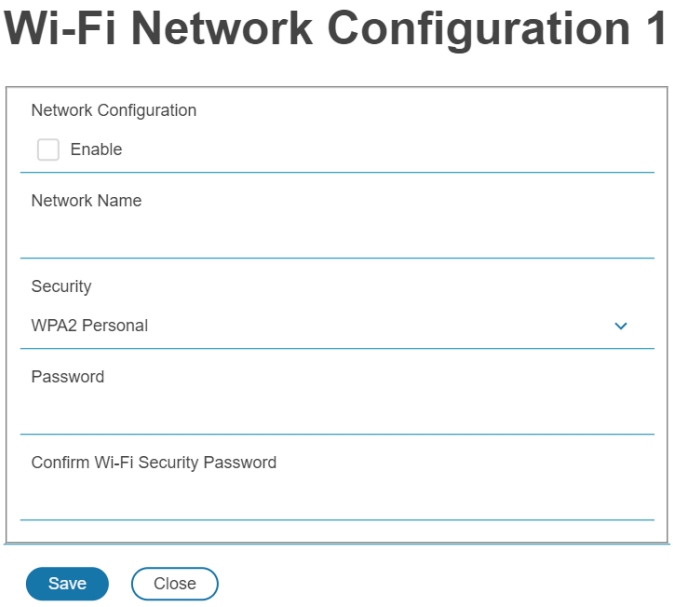


Figure 61: Wi-Fi Personal security Network configuration

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.

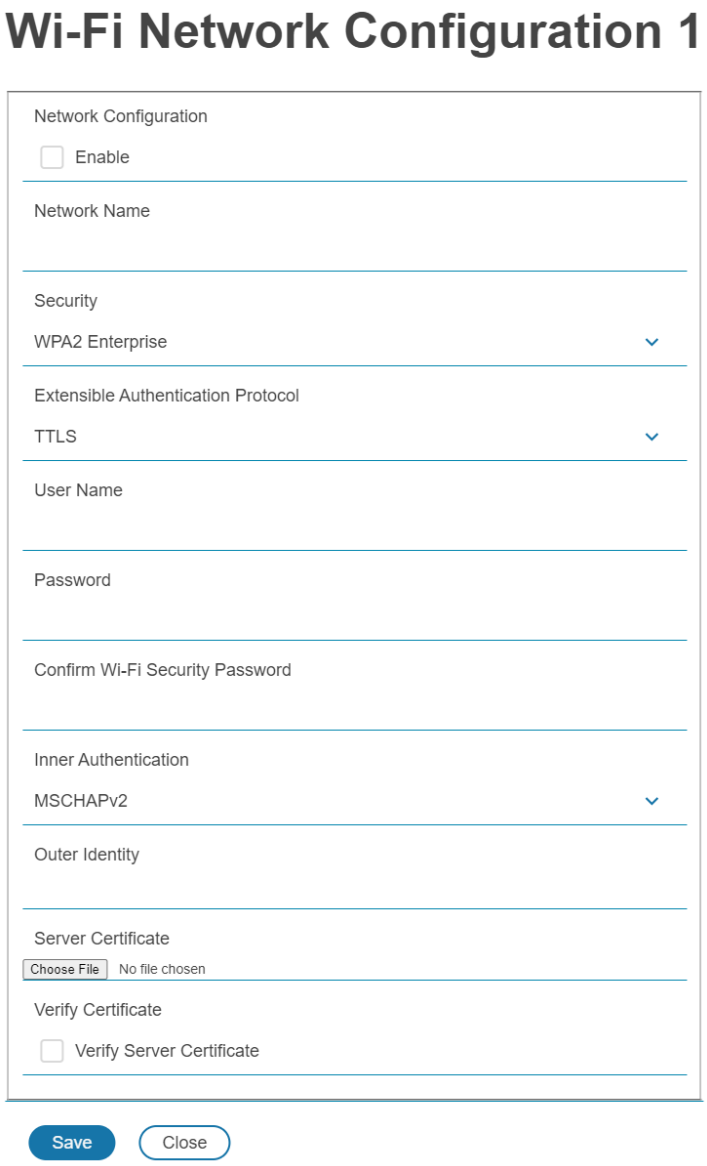


Figure 62: Wi-Fi Enterprise security Network configuration

Wi-Fi Enterprise security supports PEAP, TLS, TTLS protocol. MSCHAPv2, MSCHAP, PAP, and CHAP inner authentication protocol are available with 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.

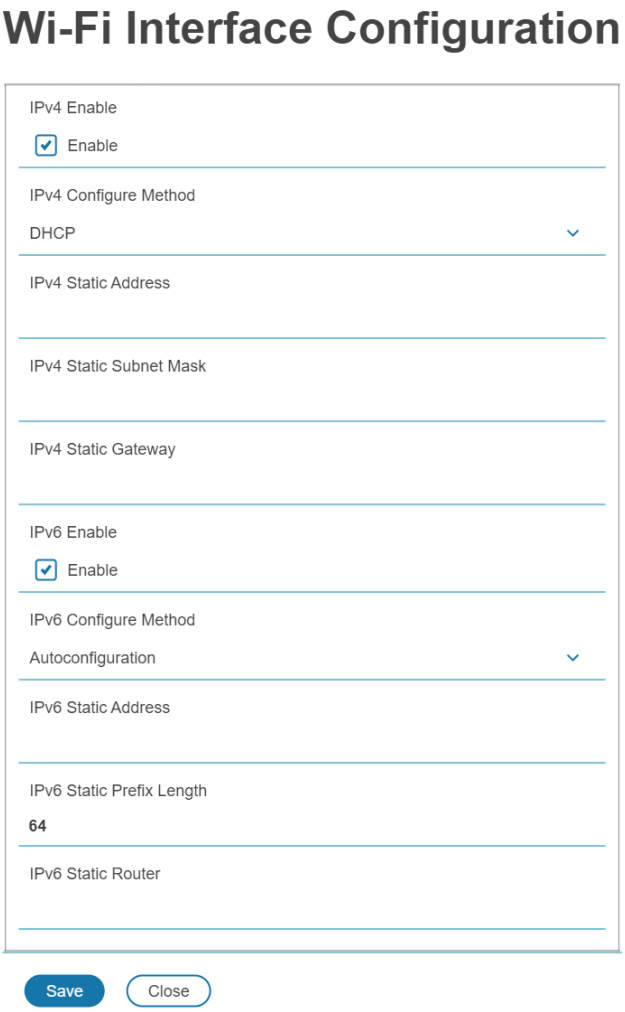


Figure 63: Wi-Fi Interface Configuration

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.

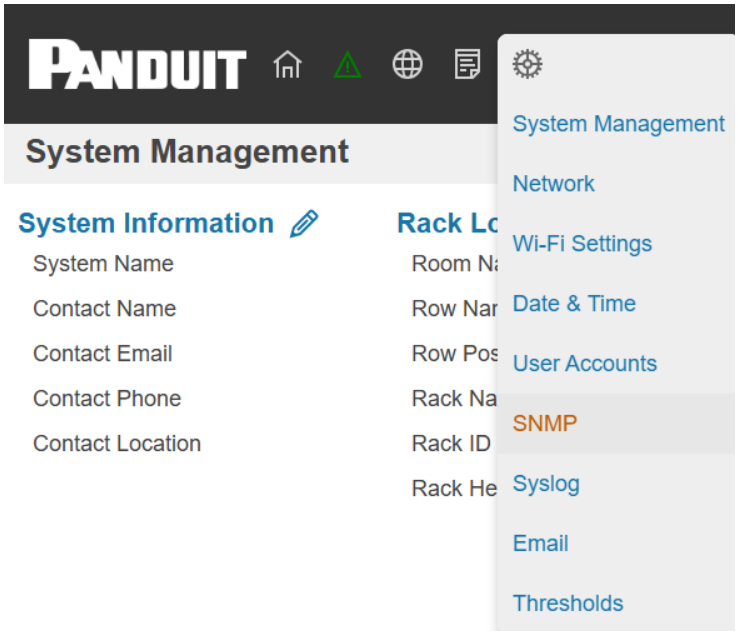


Figure 64: SNMP Management

3. The SNMP General includes SNMP Access and Version.



Figure 65: SNMP General

Setup SNMP Port

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

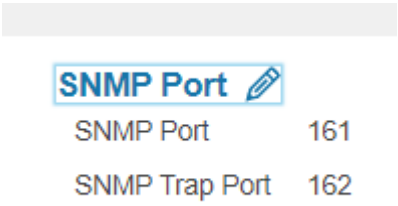


Figure 66: SNMP Port

3. Set up SNMP Port and SNMP Trap Port.

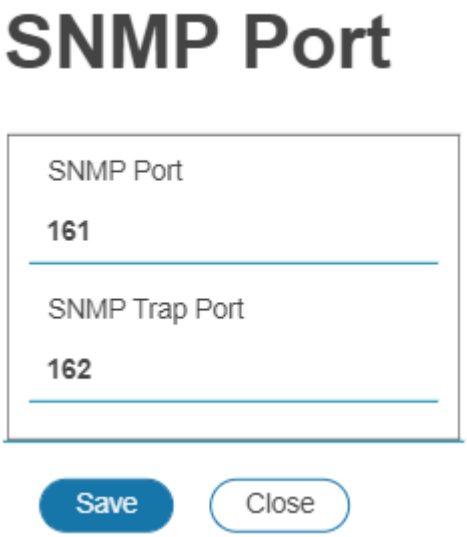


Figure 67: Setup SNMP Port and Trap Port

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.

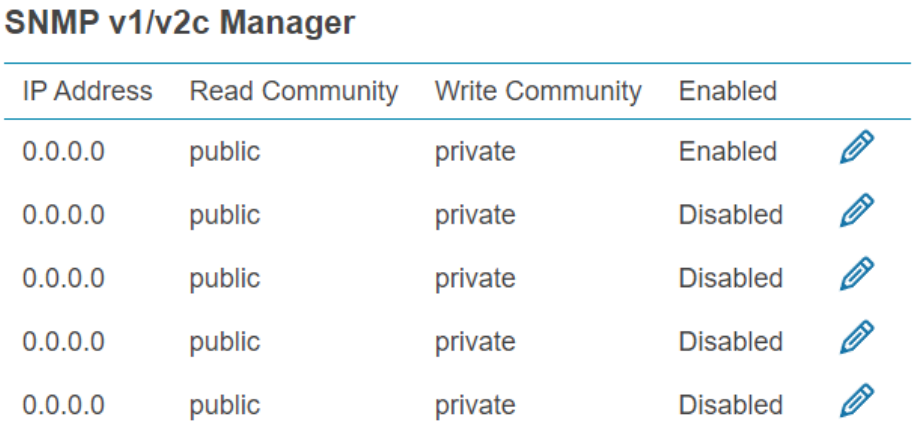


Figure 68: Define SNMP V1/V2c User

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

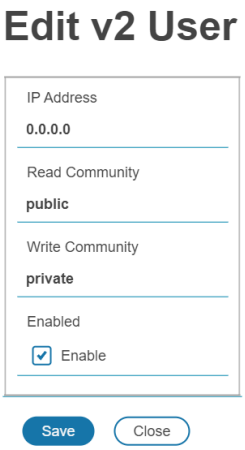


Figure 69: Edit V1/2c Manager

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

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

Configuring Users for SNMP v3

1. Access the Web interface and log in.
2. Under Settings, select **SNMP**.
3. In the **SNMP v3 Manager** panel, select the SNMP v3 manager to configure. Select the **pencil** icon in the last column.

SNMP v3 Manager

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

Figure 70: SNMP v3 Manager

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

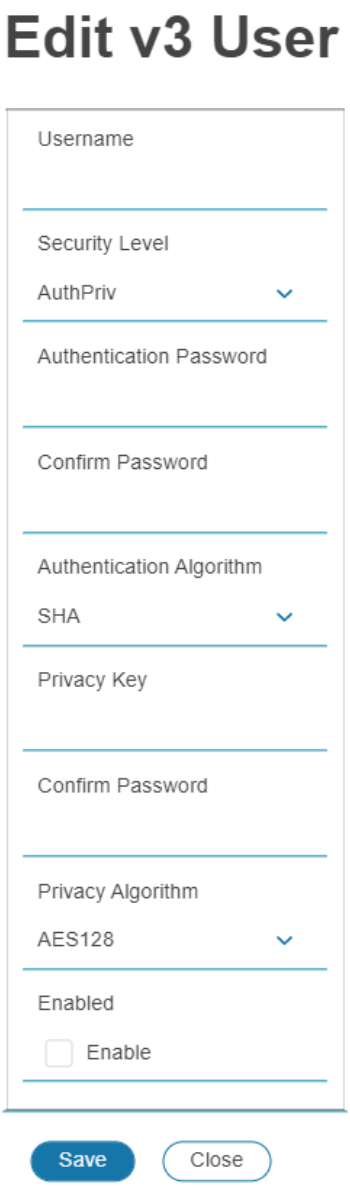


Figure 71: SNMP V3 Edit

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.

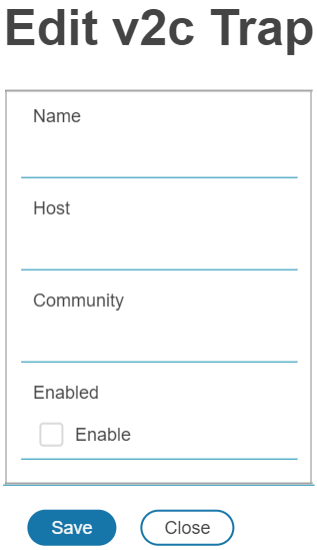


Figure 72: SNMPv2c Trap Receiver Configuration Information

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.

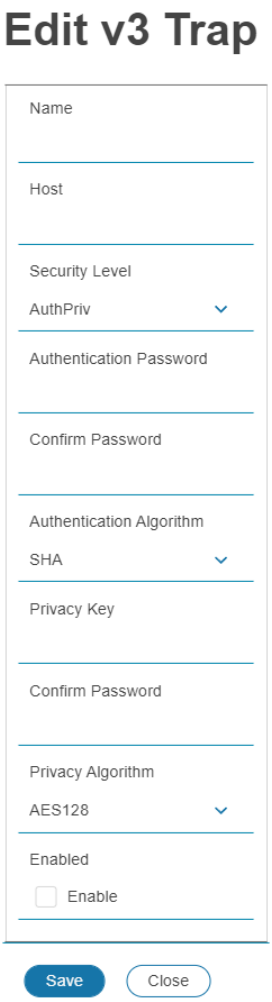


Figure 73: SNMPv3 Trap Server configuration Information.

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 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 – Network Management Controller

Status LED

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

LED State	Description
Green LED On / Red LED off	Normal operation
Red LED on	NMC Initialization or NMC internal error condition

Network LED

The LED will change colors depending on the Ethernet link status and the speed. Hardware version can be checked under Identification page.

Hardware

LED State	Description
Green blink	Link Status / Network activity
Yellow On	100 Mbps link
Yellow Off	10 Mbps link

Legacy Hardware (v01.00.00)

LED State	Description
Green blink	Network activity
Yellow On	Link Status

Section 5 – G5 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 G5 PDU accessories are specially designed to interoperate The UPS NMC controller. Connecting unapproved sensors to the NMC controller or connecting G5 PDU Sensors to 3rd party controllers may result in damage.

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

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

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

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



Figure 74: Sensor Port

Configuring Temperature Scale

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

1. Go to **User Accounts.**

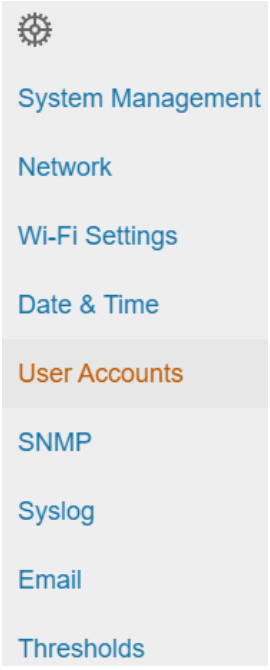


Figure 75: User Accounts

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

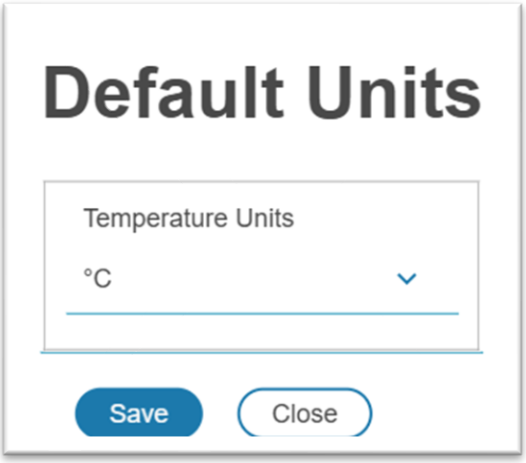


Figure 76: Temperature Units Setting

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.

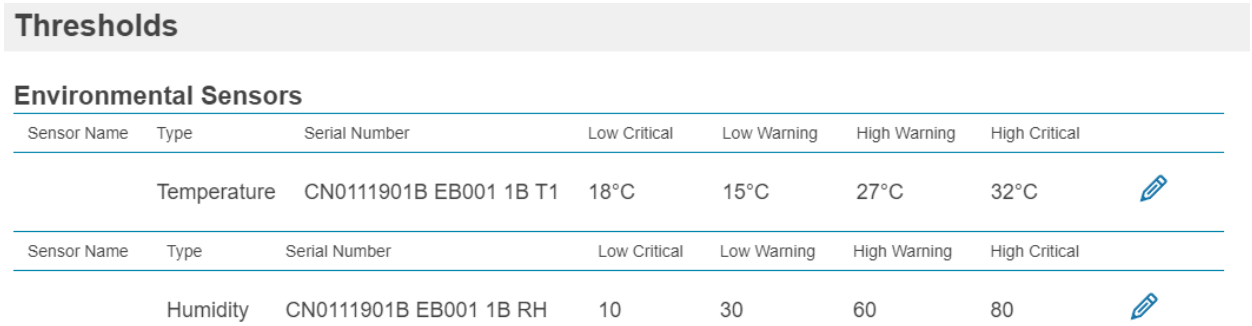


Figure 77: Environmental Sensor Threshold Configuration View

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

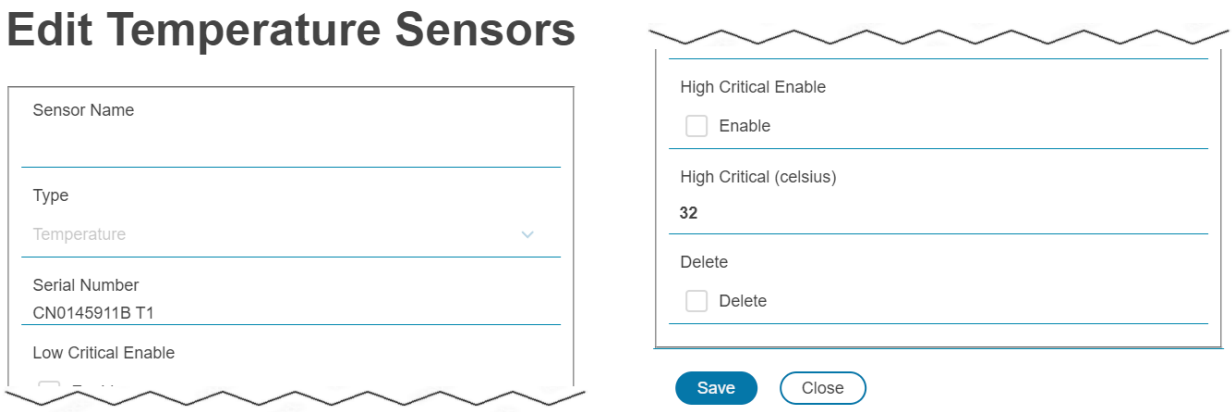


Figure 78: Temperature Sensor Edit dialog

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.

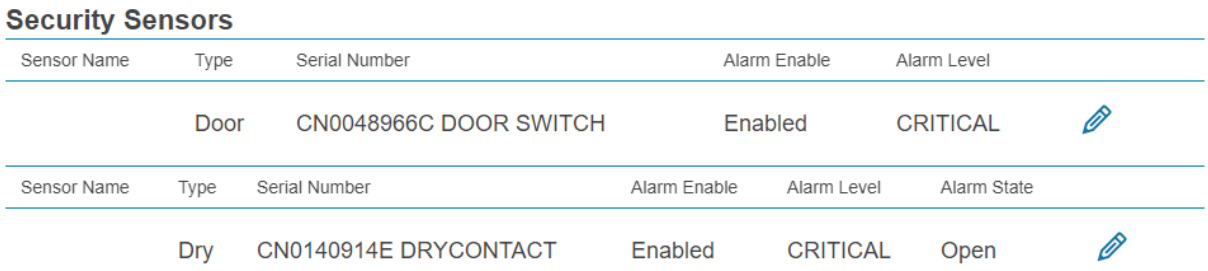


Figure 79: Security Sensor Alarm Configuration view

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

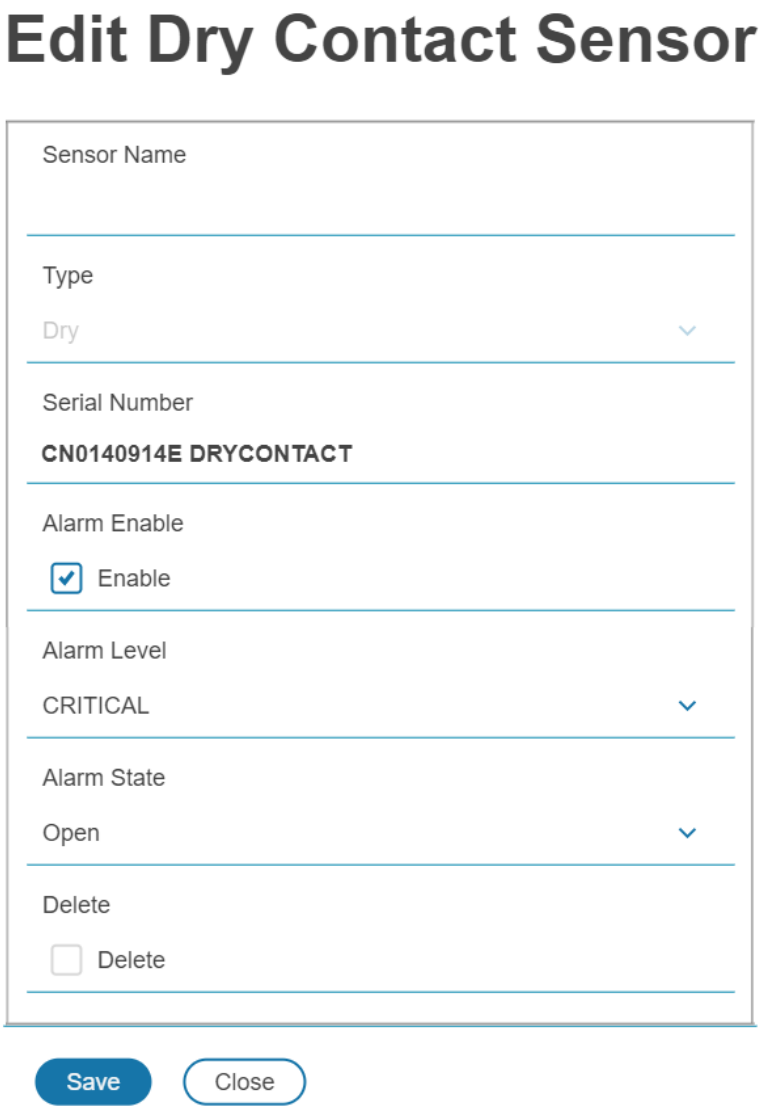


Figure 80: Dry Contact Sensor Edit dialog

Deleting Sensors

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

Section 6 – Security Handle

The Panduit UPS NMC allows users to electronically secure and control access to cabinets.

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

Note. The security handle is supported by the NMC hardware version 1.00.03 or later. When the NMC is inserted into 10-20k 3 phase UPS, the serial number of the UPS must be CN236WXXXX or later.



Figure 81: 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 Home icon > Rack Access Control.

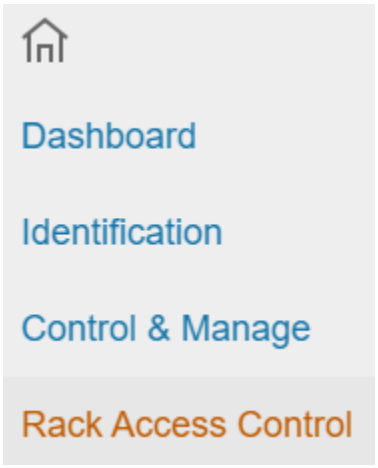


Figure 82: Rack Access Control

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.

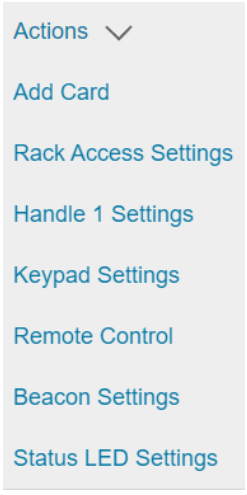


Figure 83: Rack Access Control Actions

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. Go to the event logs on the NMC.
3. Look for the most recent message about an unauthorized card swipe.

   Example:

   Smart Cabinet Cold Aisle lock is swiped by non-authorized card 16573691

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

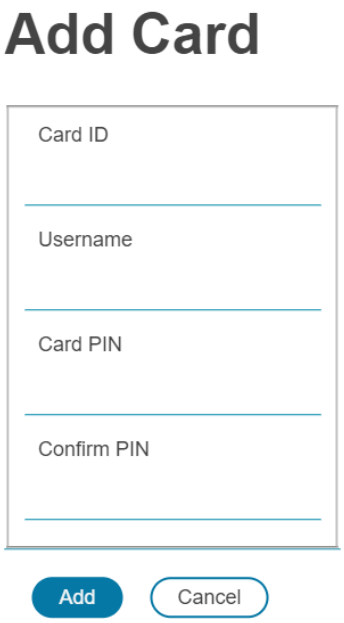


Figure 84: Add Card

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. Click Add.

Editing an access user

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

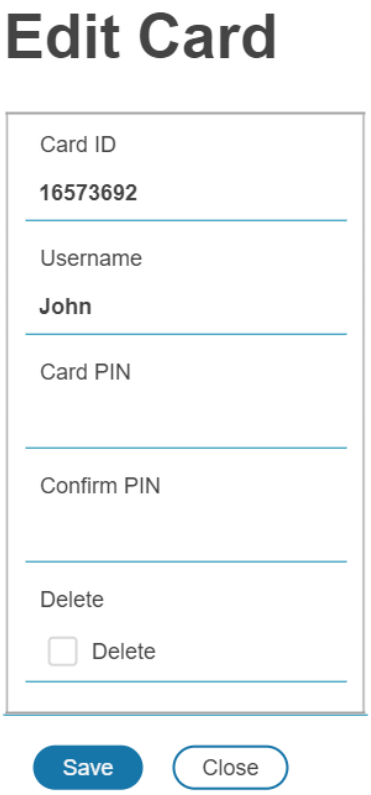


Figure 85: Edit Card

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. 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.

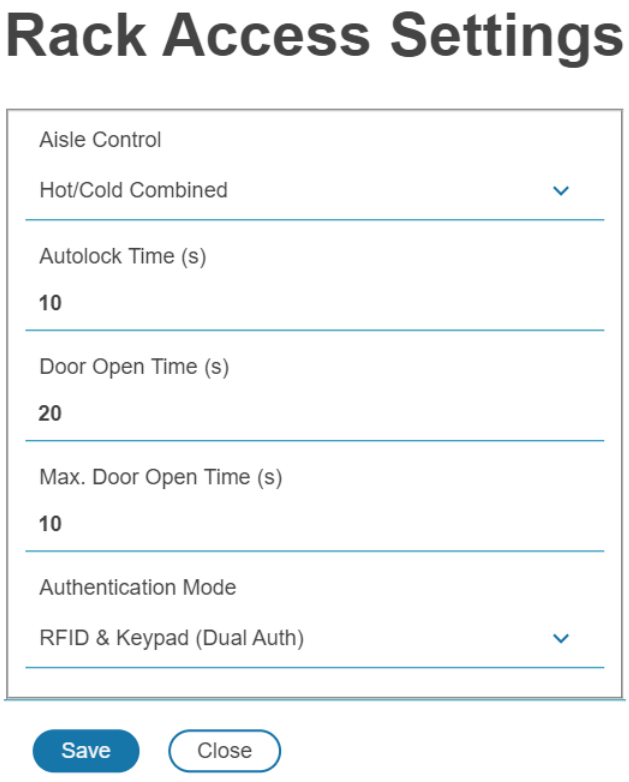


Figure 86: Rack Access Settings

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.

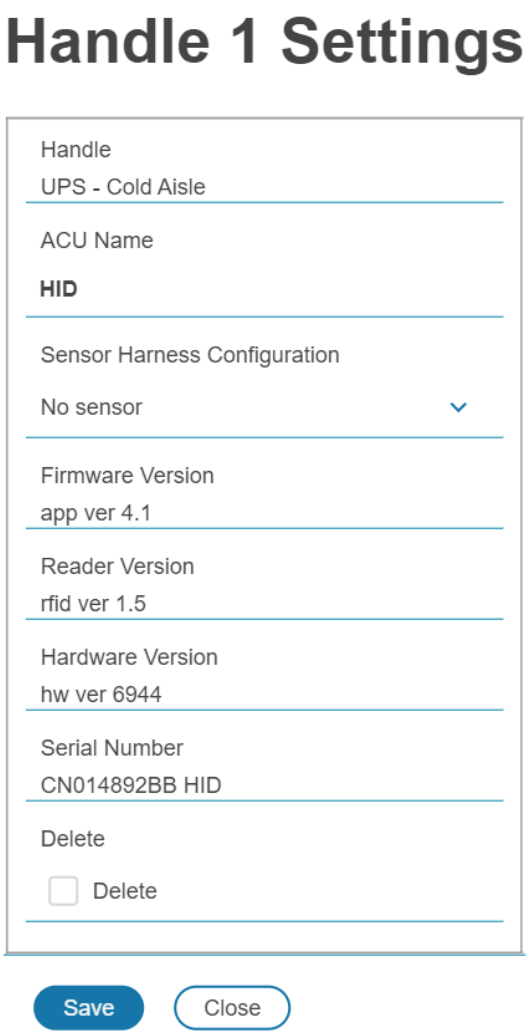


Figure 87: Handle Settings

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** 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.

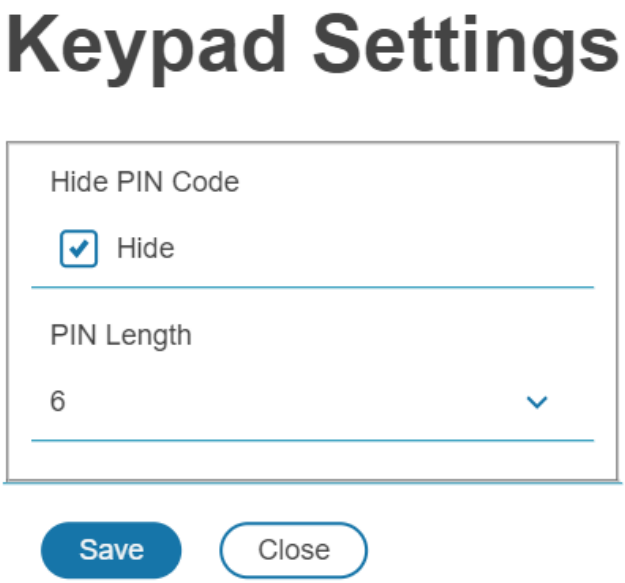


Figure 88: Keypad Settings

2. To Hide PIN code from event log, 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.

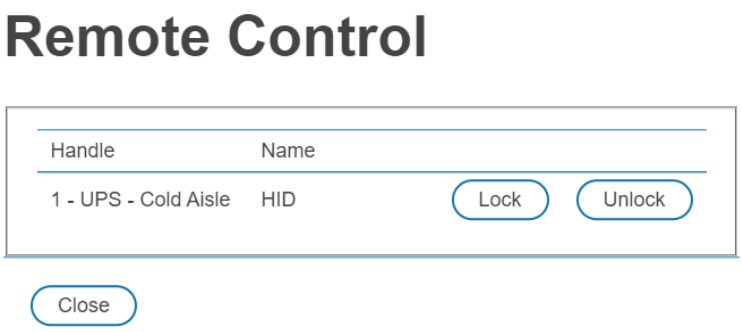


Figure 89: Remote Control

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 cabinet is in a minor alarm or flash red when the cabinet has a critical alarm. You can also use the beacon's locate function to flash the beacon a certain color to easily locate the cabinet. The default state of the beacon LED is on solid blue.



Figure 90: 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.

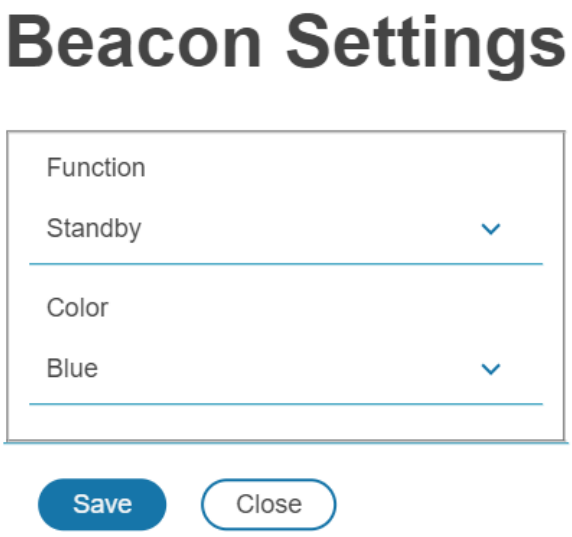


Figure 91: Beacon Settings

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 on solid blue.

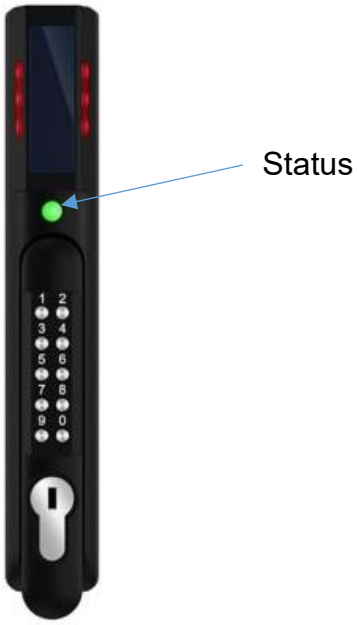


Figure 92: Status LED

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 past Door Open Time (not customizable)
Red - Solid	Lock open for longer than Autolock Time. (look for obstruction) (not customizable)
Red - Solid	Door open for longer than Door Open Time (door sensor) (not customizable)

Setting Status LED State

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

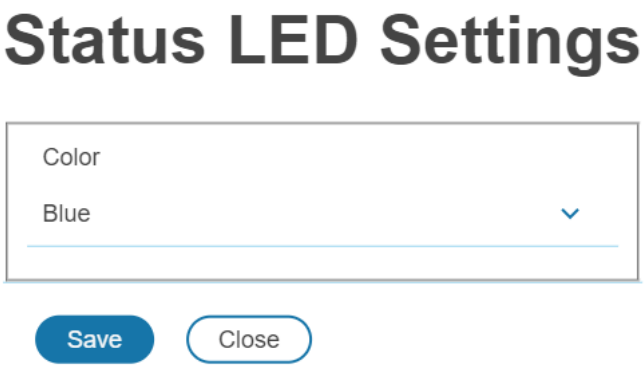


Figure 93: Status LED Settings

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	UID	UID	UID	-	CSN	CSN	Wlegand

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

Section 7 – Security

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

API Access to Primary Features

- The product provides APIs to configure and control the system. For access to this documentation, please contact “Technical Support” as described in the Support chapter.
- The web server provides a backend REST API that is used by the web GUI frontend to manage the system.

Primary Features

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

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

Security Implications of Configuration Changes

The NMC generates a notification event whenever a security-relevant configuration item is changed. This section describes the security and privacy implications of each such configuration change to assist administrators in understanding the impact of changes before and after they are made.

Enabling HTTP

- Credentials (username and password), session tokens, and configuration data exchanged with the device via the web interface will be transmitted in plaintext and will be readable by any observer with access to the network path between the browser and the device.
- Enabling HTTP in addition to HTTPS creates the additional risk that a client may inadvertently connect over the unencrypted channel.

Enabling SSH

- SSH may be disabled during provisioning if remote CLI access is not required. Re-enabling SSH when unneeded adds an attack vector.

SNMP Version Configuration

- Enabling SNMPv2c or SNMPv1 or downgrading from SNMPv3 Auth+Priv removes security encryption and authentication.
- Community strings and any transferred data are visible to any network observer.
- SNMP messages may be injected or modified by an attacker.

Syslog — Remote Forwarding

- Disabling remote syslog forwarding means audit events are stored only in the local on-device event log, which has limited storage capacity and is permanently erased by a factory reset.
- An attacker who performs a factory reset after unauthorized access can destroy local audit evidence if remote forwarding has been disabled.
- If Syslog TCP+TLS network protocol is not used, all logged data will be visible to any network observer.

LDAP

- If LDAP (non-TLS) is used for external authentication, credentials (username and password) and authentication decisions are transmitted between the NMC and the LDAP server without encryption.
- Any observer with access to the network path between the device and the LDAP server can read user credentials.

HTTPS Certificate Upload / Replacement

- The factory-provisioned self-signed certificate allows HTTPS to function from first boot but cannot be verified by a browser against a trusted certificate authority.
- Replacing with a CA-issued certificate allows users and administrators to verify device identity before entering credentials.
- Uploading an expired, revoked, or otherwise invalid certificate will cause browser certificate warnings, which may cause users to accept invalid connections or be unable to connect.
- Uploading a certificate with an incorrect (unsupported or non-matching) private key will cause the device to regenerate the default certificate.

User Account Changes

- Creating, modifying, or deleting user accounts directly affects which individuals can authenticate to the device.
- Deleting the last administrator account, or changing a password without notifying the affected user, may result in loss of access to the device. All account changes are logged and generate event notifications to configured channels.

SMTP (RFC 5321) Configuration Changes

- Changing the SMTP server address, port, credentials, or TLS settings immediately affects where email notifications are delivered.
- An incorrect SMTP configuration may silently suppress all email alerts (including security event notifications) without any visible indication in the web interface until the failure is observed in the event log.
- Disabling TLS will make all logged data visible to any network observer.

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 USB serial interface.
- The default settings feature erases the encryption keys for the non-volatile storage used for configuration data and reinitializes the non-volatile storage area to default settings.
- The default settings feature erases the flash memory that stores the Event Log and Data Log.
- The default settings feature erases the flash memory that is used to temporarily store firmware update uploads.
- The default settings feature causes the SSH RSA 3072-bit private host key to be regenerated.
- The default settings feature causes the SSH ED25519 256-bit private host key to be regenerated.
- If the 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.

Non-volatile Storage

- The product uses encrypted non-volatile storage to store all configuration information.
- The product uses industry standard encryption algorithms to protect non-volatile data. It uses an AES-XTS algorithm similar to the disk encryption storage standard IEEE P1619. A 32-byte encryption key and a 32-byte tweak key protect the data. The keys are stored in an encrypted non-volatile storage.
- The product uses industry standard encryption algorithms to protect the executable code stored on the device. The bootloader, partition table, and firmware update images are stored on encrypted flash. The flash encryption algorithm is AES-256, where the key is 'tweaked' with the offset address of each 32-byte block of flash. This means that every 32-byte block (two consecutive 16-

byte AES blocks) is encrypted with a unique key derived from the flash encryption key.
- The product disables the JTAG debugger.
- The Event Log and Data Log are stored on NMC's on-device flash storage. Unlike configuration data, log data is not encrypted at rest. An attacker with physical possession of the NMC and the capability to desolder or directly access the flash chip could read or corrupt log contents. The security context for this product assumes the device is installed in a physically secured location (see Intended Use Security Context). Users operating in environments that cannot guarantee physical security of the NMC should forward log data to a remote syslog server in real time; remote syslog ensures audit records are preserved off-device even if the device is later compromised or reset.

Authentication Data

- Usernames are stored in non-volatile memory and are available to 'administrator' role users, for the purpose of managing access to the system.
- Passwords used for managing the software are stored as a one-way bcrypt hash.
- Passwords that the user enters are not returned to the customer. (They are 'write only' from a user perspective.)
- External service authentication credentials (RADIUS, LDAP) that must be provided in plain-text, are stored on encrypted non-volatile storage.
- SNMP v1/v2c (RFC 3584) community strings are stored on encrypted non-volatile storage.
- SNMP v3 (RFC 3584) usernames and passwords are stored on encrypted non-volatile storage.
- The product only communicates with user configured remote servers/devices.

Authentication Priority

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

- User Accounts
- RADIUS
- LDAP

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 (RFC 3702) and SMTPS servers (RFC 2487).
- 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 (RFC 4253) 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

- The product connects to user configured SSH servers using these algorithms:
  - Key exchange algorithms:
    - ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521, diffie-hellman-group-exchange-sha256, diffie-hellman-group16-sha512, diffie-hellman-group18-sha512, diffie-hellman-group14-sha256, diffie-hellman-group14-sha1, diffie-hellman-group-exchange-sha1
  - Host key algorithms:
    - ecdsa-sha2-nistp256
  - Encryption algorithms:
    - chacha20-poly1305@openssh.com, aes128-ctr, aes192-ctr, aes256-ctr, aes256-cbc, rijndael-cbc@lysator.liu.se, aes192-cbc, aes128-cbc
  - MAC algorithms:
    - hmac-sha2-256, hmac-sha2-512, hmac-sha1, hmac-sha1-96

Wireless Communication

- 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 the following Wi-Fi Extensible Authentication Protocols: TLS, PEAP, TTLS.
- The product supports the 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, Syslog Remote (RFC 3164, RFC 5424), Email (RFC 5321) and SNMP trap (RFC 3416, RFC 3413) may contain 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 Authentication Mechanisms

- The product collects and verifies a fingerprint (hash) of the public key of the remote SSH shutdown agent to establish authenticity of the shutdown agent.
- 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 (RFC 4511) is not encrypted over the network.
- LDAPS (RFC 4513) and LDAP with StartTLS (RFC 4511) 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.
- RADIUS (RFC 2865) does not transmit the password as cleartext in the User-Password attribute, but its native protections are not equivalent to modern TLS-based transport security. Use Message-Authenticator protections and deploy RADIUS only on trusted/segmented networks.

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.
- 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, by applying the same algorithm as used by the ROM bootloader to load the bootloader.

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.

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) to enable MacOS and Windows to easily connect to the device via “panduit-ups-nmc-<macaddress>.local”.

Intended Use Security Context

This product is designed for deployment in physically secure environments such as corporate data centers or IT rooms. The assumed physical security baseline includes:

- Building entry controls: security lobby and access badges.

- Server room / cabinet level controls: in-zone, in-row, or cabinet-level restricted physical access, such as key locks or electronic access control.

Security features of the device are designed to complement these physical controls, not replace them. Users operating the device in environments that do not meet this baseline should apply additional compensating controls (for example, network segmentation, enhanced logging, and heightened monitoring).

Do not route serial, sensor, or USB cables through unsecured areas as these interfaces do not provide confidentiality (encryption).

Secure deployment

Configure the NMC regarding the following settings:

User Roles

The “Web Interface Access” section describes Roles of system users. Choose the least-privileged role that provides the access required for the user’s responsibilities.

To verify whether a user has the access they need, the logged-in user may run the “list *” command in the CLI. This command enumerates the objects and properties available to that user, identifies readable and writable items, shows permitted input values or ranges, and indicates whether each item is read-only.

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 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**

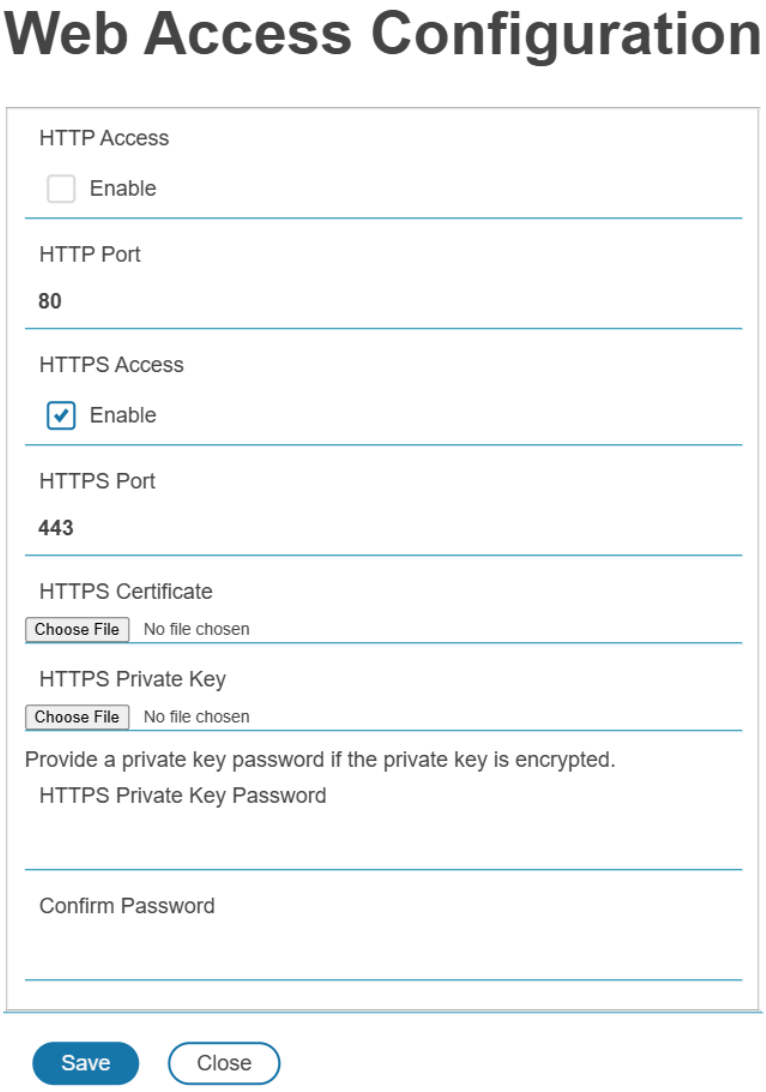


Figure 94: SSL Certificate Load Screen

Use SNMPv3

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 and a privacy algorithm of AES128.

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

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

Disabling unused interfaces

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

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

Review Session management

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

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.

SSH Algorithm Strength

The SSH protocol provides algorithms for negotiating a secure connection. Over time, these may become weak or obsolete. To mitigate this, please refer to your SSH client's documentation on how to disable weak algorithms, which will prevent the client's connection from using them.

The REST /api/login provides info about password policy

The api/login REST API endpoint provides the password policy when given an empty request, to aid a user in choosing a new password that meets the security policy. We consider the length & complexity properties to be non-sensitive information for an unauthorized actor. As a best practice, users of the system should be informed to always use passwords that meet their organization’s password policy.

Secure Operation Summary

Secure operation depends on customer administration of the product’s security-relevant configuration and on using the product within the documented intended security context.

Administrators are responsible for configuring accounts, roles, authentication domains, secure communication options, time sources, logging/notification destinations, firmware update sources, and enabled interfaces according to site security policy. Periodic maintenance should be performed by ensuring the firmware is upgraded when a new release is available. Firmware upgrade automation can be achieved by using a DCIM or the Auto Upgrade feature on products that provide the feature. Administrators should also periodically review local accounts and assigned roles, external authentication server configuration, certificate validity and expiration dates, enabled services and interfaces, and security-relevant configuration changes. If remote Event Notification is not used, the Data Log and Event Log may be reviewed periodically, as the logs roll over based on log usage.

As a best practice, include the following periodic checks in the maintenance plan: verify that user accounts and role assignments remain appropriate; confirm that RADIUS, LDAP, TACACS+, SNMP, syslog, SMTP, NTP, DNS, DHCP, and other external service settings still point to approved servers; review certificate expiration dates and replace certificates before expiration; trigger an event and verify event notification delivery; validate configuration backup and restore procedures where needed; and confirm that unused services, protocols, APIs, and physical or logical interfaces remain disabled or protected.

Users are expected to operate only within assigned privileges and report suspected unauthorized access or unexpected security-relevant behavior to the administrator.

These responsibilities rely on the assumption that the product is installed in the Intended Use Security Context and that customer-managed services provided by the product are maintained in a trusted state. Some examples of customer-managed services: DHCP, DNS, NTP, remote authentication protocols, SMTP, syslog, SNMP managers, certificate authorities, firmware repositories.

Defense-in-Depth Strategy Summary

The product's defense-in-depth strategy links defense-in-depth layers, security chapter sections, threats, and mitigations together. It is intended as a mapping aid and does not replace the detailed specifications in this chapter.

Note: this table mentions general functions, features, interfaces and protocols that may or may not be available on this product. If the interface has a security feature or concern, the details for applicable items are listed above.

Defense-in-depth	Applicable Security	Threats or risks	User mitigation strategy

layer (Applicability)	chapter sections	addressed	
Security context and physical deployment (Platform-specific)	Intended Use Security Context; Secure deployment	Physical access to exposed ports, removable media, local interfaces, logs, configuration data, and storage devices.	Deploy the product in the intended physically secured environment, local peripheral interfaces (e.g. serial, accessories, USB), and use compensating controls such as network segmentation, enhanced logging, and external monitoring when the baseline environment is not met.
Interface and API access control (Feature-dependent)	API Access to Primary Features; Primary Features; Secure deployment	Unauthorized control of configuration, firmware update, outlet power, power flow, or other product functions exposed through APIs or local interfaces.	Limit API and interface use to authorized users and roles, review API documentation, disable unused APIs or interfaces where supported, and protect physical ports when not required.
Identity, authentication, and authorization (Platform-specific)	Authentication Data; Authentication Priority; User Account Changes; External Authorization Mechanisms	Credential misuse, unexpected privilege assignment, weak account management, duplicate usernames across authentication domains, and unauthorized access.	Manage user accounts and roles carefully, avoid defining the same username in multiple authentication domains with different permissions, protect administrator access, and use the configured authentication domains according to local security policy.
Credential and secret protection at rest (Platform-specific)	Non-volatile Storage; Authentication Data; External Authorization Mechanisms; Wireless Communication	Disclosure of stored configuration data, passwords, SNMP community strings, remote authentication secrets, Wi-Fi configuration, firmware images, or other sensitive data.	Be aware of product features and configuration options that protect sensitive data at rest where available, maintain physical protection for the device, and follow secure disposal or destruction guidance when stored data must not be recoverable.
Network confidentiality, integrity, and endpoint authenticity (Platform- and version-specific)	Network Transport Security; HTTPS Certificate Upload / Replacement; TLS Server Certificate Verification; TLS Client Certificate and Client Private Key; External Authorization Mechanisms	Eavesdropping, credential exposure, server impersonation, weak certificate trust, downgrade to unencrypted protocols, and use of obsolete or compatibility algorithms.	Prefer HTTPS, SSH, LDAPS, StartTLS, SMTPS, and other encrypted protocol options; upload trusted certificates; enable server certificate verification where supported; provide client certificates where required; and configure clients to avoid weak SSH algorithms.
Legacy and compatibility protocol risk	Network Transport Security; Security Implications of	Plaintext management access, weak or legacy authentication and	Disable legacy or unused protocols where possible, prefer SNMPv3 AuthPriv, encrypted LDAP variants, HTTPS, SSH,

management (Feature-dependent)	Configuration Changes; External Authorization Mechanisms; Protocols; Secure deployment	integrity mechanisms, exposure from SNMPv1/v2c, Telnet, LDAP without TLS, RADIUS compatibility behavior, TACACS+ native protection limits, legacy SSH algorithms, discovery protocols, and other compatibility features.	and TLS-protected services, enable RADIUS Message-Authenticator protection where applicable, and restrict legacy protocol use to trusted and segmented networks when it cannot be disabled.
Secure configuration and hardening (Common with platform-specific details)	Security Implications of Configuration Changes; Secure deployment; Review Session management; Disabling unused interfaces	Insecure defaults, unnecessary exposed services, misconfiguration, loss of alerts, insecure session settings, and accidental use of less secure communication paths.	Review security-relevant configuration changes before use, disable unused services and physical interfaces where supported, configure session settings to match local policy, use secure notification paths, and periodically review the deployment configuration.
Logging, monitoring, and time accuracy (Platform-specific)	Logging; Network Configuration Data; Security Implications of Configuration Changes; NTP; Syslog Remote Forwarding; Security Response	Loss of audit evidence, inaccurate timestamps, inability to investigate unauthorized access, local log destruction after reset, and missed security notifications.	Configure a trusted NTP source, enable remote syslog or other remote notification channels where supported, protect log destinations, review event notifications, and report suspected security incidents and vulnerabilities through Technical Support.
Firmware authenticity, integrity, and update control (Platform- and version-specific)	Secure Boot Protection; Firmware Update Protection; Automatic Firmware Upgrade; Auto Update Config URI	Execution of unauthorized firmware, tampered update packages, corrupted boot or application images, unauthorized update repositories, and exposure of secrets in update configuration files.	Use the authenticated firmware update process, keep firmware current, restrict access to configured firmware and configuration update repositories, use HTTPS for update resources, and protect update configuration files that may contain sensitive information.
Wireless exposure control (Feature-dependent)	Wireless Communication; Direct Connect; Secure deployment	Unauthorized wireless access, unintended access point exposure, weak wireless configuration, and exposure of wireless credentials or configuration.	On products that have Wi-Fi, keep Wi-Fi disabled unless required, understand Direct Connect activation behavior, use supported WPA security options appropriate for the deployment, and protect any physical action required to activate wireless access.
Discovery and network visibility	Protocols; Network Configuration Data	Unwanted local network discoverability, disclosure of hostnames or	Account for mDNS, LLMNR, DHCP, DNS, and exposed network identification behavior in network design and

(Platform-specific)		addressing information, and increased visibility on shared networks.	segmentation, and enable discovery behavior only where it supports the intended deployment.
Secure disposal and data sanitization (Platform- and feature-dependent)	Secure Disposal Features; Secure Erase — NIST SP 800-88 Media Sanitization; Non-volatile Storage	Residual data exposure after decommissioning, inability to erase local storage, recovery of logs or configuration data, and reuse of device identity keys after reset.	Use reset-to-defaults or secure erase features where available, verify the disposal procedure appropriate to the storage type, and physically destroy PCBAs or media when software-based disposal cannot be completed or residual data must not be recoverable.

Security Response

To report a security vulnerability or incident, please contact “Technical Support” as described in the Support chapter.

Warranty and Regulatory Information

Warranty Information

(https://www.panduit.com)

Regulatory Information

Safety and regulatory compliance

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

Panduit Support and Other Resources

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

Accessing Panduit Support

North America

Customer Service

- Price & Availability
- Expedites

800-777-3300 or cs@panduit.com

UPS Technical Support:

- UPS 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

UPS Technical Support:

- UPS Selection
- Competitor Cross references
- Product Documentation
- Technical Issues

Email: TechSupportEMEA@panduit.com

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

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

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

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. Also, the firmware can be updated with Panduit *m*Power tool, and the firmware can be bulk updated with the *m*Power tool. For the latest firmware please visit: panduit.com → Support → Download Center → UPS

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 > System Management > Actions > Update Firmware**.
6. In the Firmware Update dialog box, click on 'Choose File', then browse to the firmware file named ups-nmc-vx.x.x-release.bin.

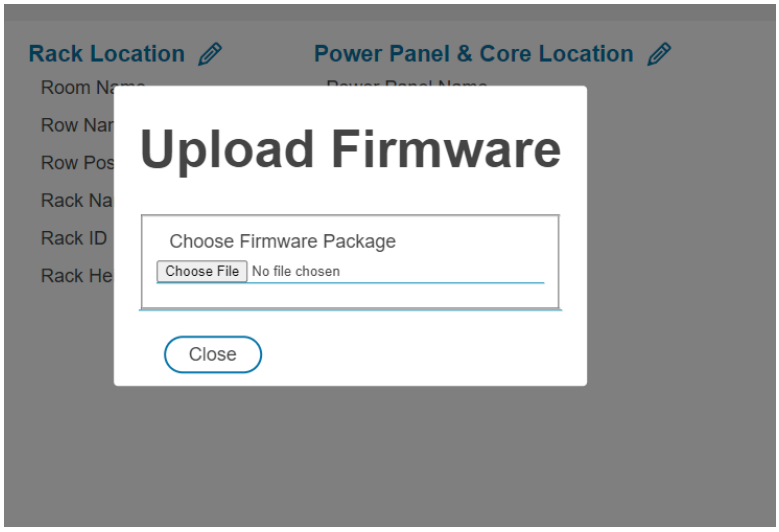


Figure 95: Upload Firmware

7. The system will update after selecting the file.
8. When the upload is finished, the system will reboot automatically.

Appendix B: System Reset or Password Recovery

Press and hold the Reset Button for 8 seconds to recover from a NMC controller communication failure. The green LED will flash slowly indicating the controller will reset. This will cause a reset of the NMC controller, all configuration(s) will be retained.

To Default the controller to factory settings, press and hold the Reset Button for at least 20 seconds. The green LED will flash fast indicating the controller will reset to the factory default. This will cause a reset of the NMC controller erasing all existing configurations, including username(s) and password(s).

Appendix C: Direct connect to the UPS 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**.

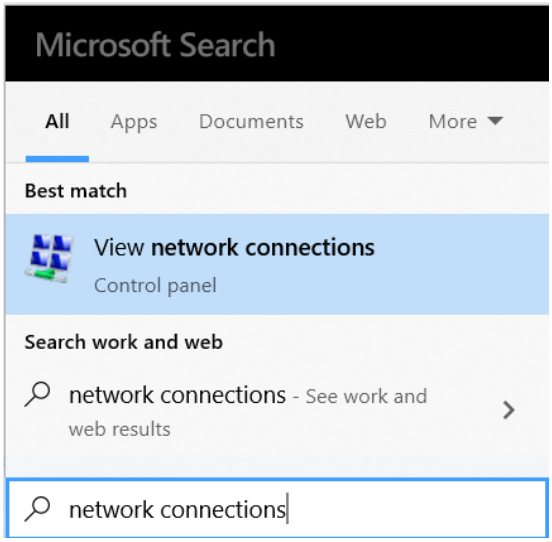


Figure 96: View network Connections

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

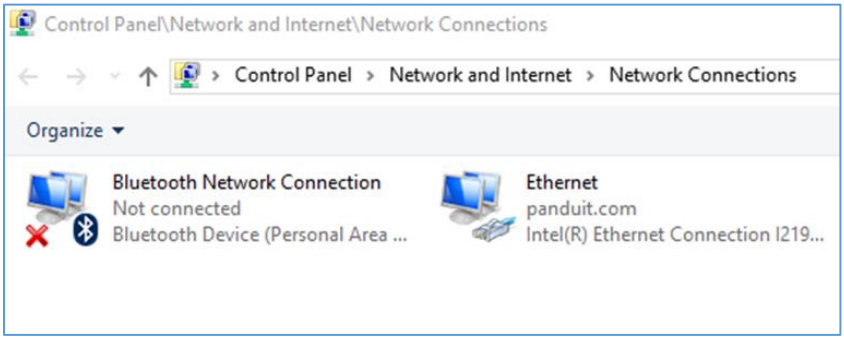


Figure 97: Properties

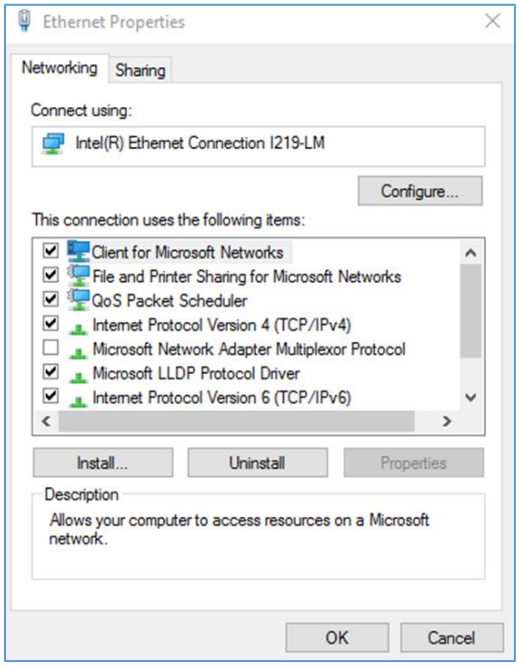


Figure 98: Ethernet Properties

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



Figure 99: 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 10 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.

Note: If the browser does not connect, the device may have older firmware. Try again with the following additional steps:

1. The MAC address of the NMC is printed on a label on the face plate of the card. Get the last two bytes of the MAC address.

    Example: if the label shows 00:0F:9C:03:07:83, use 0783

2. From the Start menu, Run cmd.exe
    a. Type the following commands but replace the number with the last two bytes of the MAC address from the following step.

```
set m=0783
set /a h="0x%m% % 256 + 1" && set /a l=0x%m% / 256 % 256
echo 169.254.%h%.%l%
```

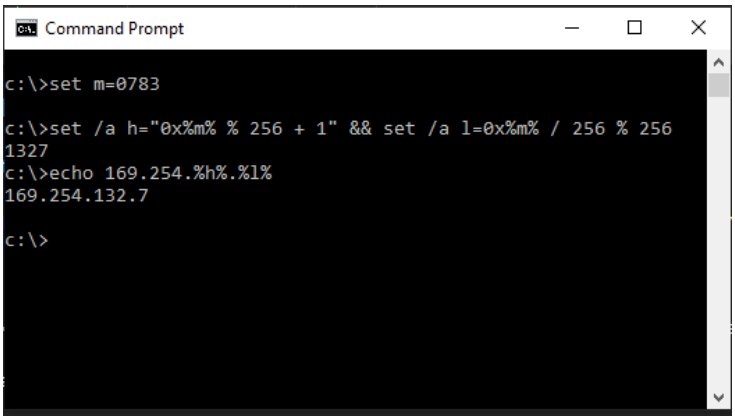


Figure 100: IP Address Calculation

3. Open a web browser on the PC.
4. In web browser address bar, type https://<ip address>, replacing <ip address> with the address previously calculated.

   example: **https://169.254.132.7/**
5. Use the Enter key to navigate to the web site.
6. A Privacy Error or an error explaining that the certificate (cert) authority is invalid. 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 command line interface through USB port and SSH network protocol. The command line interface allows the user to read or write to NMC data model.

Logging in using USB port

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

Logging in using SSH protocol

- Identify IP address of the NMC
- Open a SSH program such as PuTTY
- Open connection to the NMC
- Use the same credential 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

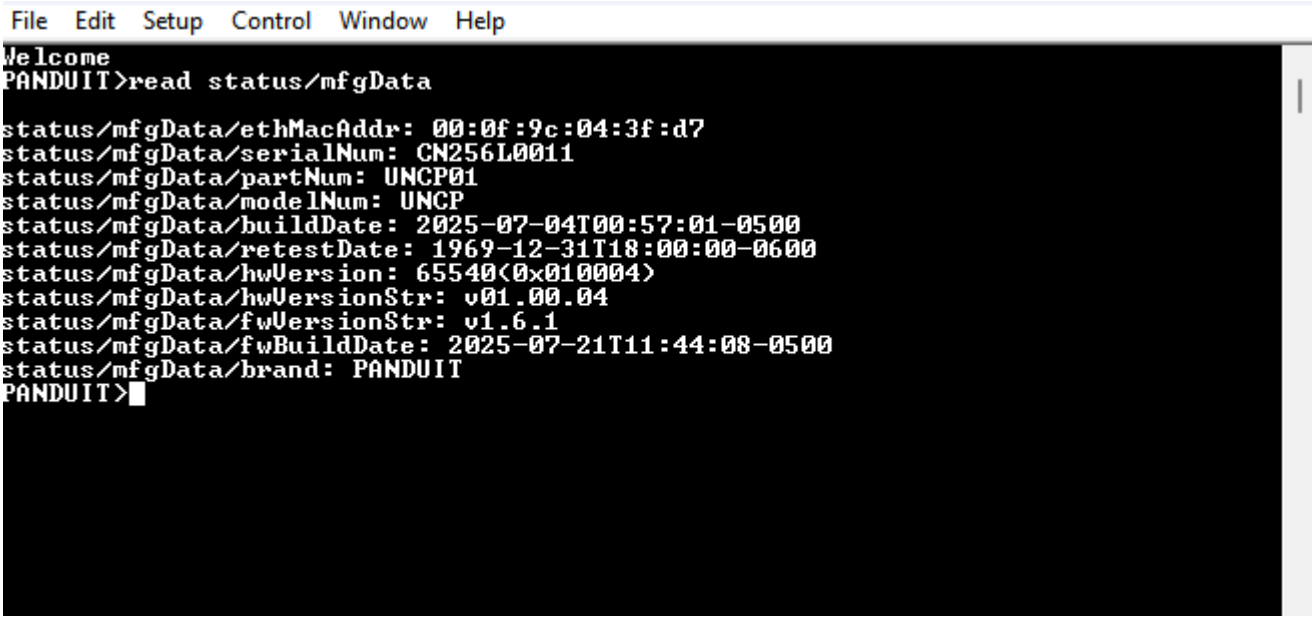


Figure 101: Reading from CLI

- **write**

  Set a value to an individual item in the data model

  Example: write config/systemInfo/systemName DC1-UPSA1

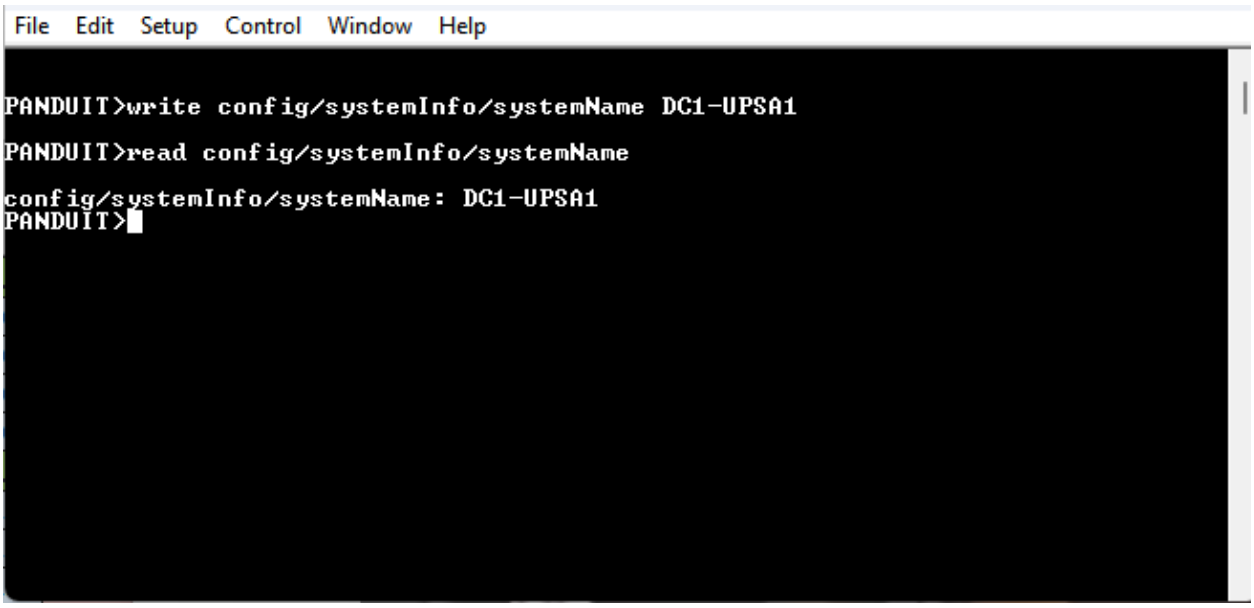


Figure 102: Writing from CLI

- **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: Consolidated Network Interface and Protocol Inventory

Physical Interfaces

Interface	Default State	Notes
Ethernet	Enabled	Primary management interface; DHCP by default
Wi-Fi AP	Disabled	2.4 GHz 802.11b/g/n; Direct Connect; Local button enable
Wi-Fi Station	Disabled	2.4 GHz 802.11b/g/n; Connected to Wi-Fi Intrastructure
USB Serial	Enabled	CLI access; 115200 baud (User login required/unencrypted)
Sensor bus	Enabled	Local Bus(RS-485/ unencrypted)
UPS Core	Enabled	Device internal(RS-232/ unencrypted)
Reset button	Enabled	Local Only/ Triggers factory reset / Direct Connect activation

Network Host Protocols

Protocol	Default Port	Default State	Notes
HTTPS	443/TCP*	Enabled	Remote Management (secure)
HTTP	80/TCP*	Disabled	Remote Management (insecure)
SSH	22/TCP*	Enabled	Remote Management CLI (secure)
SNMP (v1/v2c)	161/UDP*	Disabled	Remote Management (insecure)
SNMP (v3)	161/UDP*	Disabled	Remote Management Secure only with Auth+Priv
mDNS	5353/UDP	Enabled	Device discovery; link-local only

Note: * indicates the port is configurable

Network Client Protocols

Protocol	Port	Default State	Notes
NTP	123/UDP	Enabled	Time sync
DHCP	68/UDP	Enabled	IP acquisition on Ethernet/Wi-Fi
DNS	53/UDP	Enabled	Name resolution
mDNS	5353/UDP	Enabled	Device discovery; link-local only
LDAP	389/TCP*	Disabled	External Authentication (insecure)
LDAP(StartTLS)	389/TCP*	Disabled	External Authentication (secure)

LDAPS	636/TCP*	Disabled	External Authentication (secure)
SNMP Traps	162/UDP*	Disabled	Event Forwarding
SMTP	25/TCP*	Disabled	Event Forwarding (insecure)
SMTPS	587/TCP*	Disabled	Event Forwarding (secure)
SSH	22/TCP*	Disabled	Client for Smart Load Shedding
Syslog UDP	514/UDP*	Disabled	Event Forwarding (unreliable/insecure)
Syslog TCP	601/TCP*	Disabled	Event Forwarding (reliable/insecure)
Syslog(TLS)	6514/TCP*	Disabled	Event Forwarding (reliable/secure)
RADIUS	1812/UDP*	Disabled	External Authentication (insecure)

Note: * indicates the port is configurable