

# smartzone™ UPS

## **User Manual**

UPS Network Management Card

Version 1.2.2

## 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
Network Settings.....	19
System Management Information .....	23
Setting Time and Date on the NMC .....	26
Control & Manage.....	28
Panduit’s Smart Load Shedding.....	40
Email Setup .....	46
Event Log .....	49
Data Log .....	50
Web Interface Access.....	51
Setting Up the System for RADIUS Authentication.....	53
Configuring the system with LDAP Server Settings .....	54
Wi-Fi Settings .....	57
Section 3 – Simple Network Management Protocol (SNMP).....	63
SNMP Management Configuration .....	63
Configuring Users for SNMP V1/V2c.....	65
Configuring Users for SNMP v3.....	66

Configuring SNMP Traps..... 69

Section 4 – Network Management Controller ..... 73

    Status LED ..... 73

    Network LED ..... 73

Section 5 – SmartZone G5 Accessories..... 74

    Hardware Overview ..... 74

    Configuring Temperature Scale..... 75

    Configuring Environmental Sensors ..... 76

    Configuring Security Sensors ..... 77

    Deleting Sensors ..... 79

Section 6 – Security ..... 80

    Secure Disposal Features ..... 80

    Non-volatile Storage ..... 80

    Authentication Data ..... 81

    Network Transport Security ..... 81

    Wireless Communication ..... 84

    Network Configuration Data..... 85

    External Authorization Mechanisms..... 85

    Secure Boot Protection..... 86

    Firmware Update Protection ..... 86

    Other Features ..... 86

    Secure deployment..... 87

Warranty and Regulatory Information..... 89

    Warranty Information ..... 89

    Regulatory Information ..... 89

Panduit Support and Other Resources..... 90

    Accessing Panduit Support..... 90

Acronyms and Abbreviations..... 91

Appendix A: Firmware Update Procedure ..... 98

---

Appendix B: System Reset or Password Recovery..... 99

Appendix C: Direct connect to the UPS via Ethernet without Bonjour ..... 100

Appendix D: Command Line Interface..... 104

Appendix E: RADIUS Server Configuration..... 107

Appendix F: POSIX Time Zone Information ..... 109

## 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 CLI..... 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: Ethernet Interface Configuration ..... 19

Figure 16: DNS Configuration ..... 20

Figure 17: Web Access Configuration ..... 20

Figure 18: SSH Configuration ..... 21

Figure 19: Syslog Configuration ..... 21

Figure 20: Network Time Protocol..... 22

Figure 21: Date/Time Configuration ..... 22

Figure 22: Time Zone Configuration..... 23

Figure 23: System Management ..... 23

Figure 24: System Information Configuration ..... 24

Figure 25: Rack Location Configuration ..... 25

Figure 26: Power Panel & Core Location ..... 26

Figure 27: Setting the Date and Time..... 26

Figure 28: NTP Configuration..... 27

Figure 29: Daylight Saving Time Zone Configuration ..... 28

Figure 30: Control & Manage ..... 29

Figure 31: Audible Alarm Configuration..... 29

Figure 32: Start Shutdown Example..... 30

Figure 33: Cancel Shutdown Example ..... 31

Figure 34: Enter Bypass Example ..... 31

Figure 35: Exit Bypass Example ..... 32

Figure 36: UPS Manual Test Configuration..... 33

Figure 37: Start Test Example..... 33

Figure 38: Start Test Confirmation ..... 34

Figure 39: Cancel Test Example ..... 34

Figure 40: Cancel Test Confirmation..... 34

Figure 41: Battery Test Configuration..... 35

Figure 42: UPS Mode Example ..... 36

Figure 43: Edit Outlet Group ..... 36

Figure 44: Outlet Group Control ..... 37

Figure 45: Edit Outlets..... 39

Figure 46: One Delay Time ..... 39

Figure 47: Shutdown Group Configuration ..... 41

Figure 48: Smart Load Configuration ..... 43

Figure 49: Shutdown Schedule Configuration ..... 45

Figure 50: Email Setup..... 46

Figure 51: SMTP Account Settings ..... 47

Figure 52: Email Recipient ..... 49

Figure 53: Event log ..... 49

Figure 54: Event log Actions menu ..... 50

Figure 55: Data Log..... 50

Figure 56: Data Log Configuration ..... 51

Figure 57: Data Log Configuration Panel ..... 51

Figure 58: User Accounts..... 54

Figure 59: RADIUS Configuration ..... 54

Figure 60: LDAP Configuration ..... 56

Figure 61: Enable Role Privileges ..... 57

Figure 62: Wi-Fi Settings screen ..... 58

Figure 63: Wi-Fi Radio Configuration ..... 58

Figure 64: Wi-Fi Direct Connect Configuration..... 59

Figure 65: Wi-Fi Personal security Network configuration..... 60

Figure 66: Wi-Fi Enterprise security Network configuration..... 61

Figure 67: Wi-Fi Interface Configuration..... 62

Figure 68: SNMP Management..... 63

Figure 69: SNMP General ..... 64

Figure 70: SNMP Port ..... 64

Figure 71: Setup SNMP Port and Trap Port ..... 65

Figure 72: Define SNMP V1/V2c User ..... 65

Figure 73: Edit V1/2c Manager..... 66

Figure 74: SNMP v3 Manager..... 67

Figure 75: SNMP V3 Edit ..... 68

Figure 76: SNMPv2c Trap Receiver Configuration Information..... 70

Figure 77: SNMPv3 Trap Server configuration Information..... 71

Figure 78: Sensor Port ..... 75

Figure 79: User Accounts..... 76

Figure 80: Temperature Units Setting ..... 76

Figure 81: Environmental Sensor Threshold Configuration View ..... 77

Figure 82: Temperature Sensor Edit dialog..... 77

Figure 83: Security Sensor Alarm Configuration view ..... 78

Figure 84: Dry Contact Sensor Edit dialog ..... 79

Figure 85: SSL Certificate Load Screen ..... 87

Figure 86: Upload Firmware..... 98

Figure 87: View network Connections ..... 100

Figure 88: Properties..... 100

Figure 89: Ethernet Properties ..... 101

Figure 90: Internet Protocol Version 4..... 101

Figure 91: IP Address Calculation ..... 103

Figure 92: Reading from CLI ..... 105

Figure 93: Writing from CLI ..... 106

## 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 HTTPS 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

```

COM12 - Tera Term VT
File Edit Setup Control Window KanjiCode Help

login: admin
password: *****

PANDUIT>read status.netStatus.*
status.netStatus.activeIPv4Address: 169.254.184.63
status.netStatus.activeIPv4Netmask: 255.255.0.0
status.netStatus.activeIPv4Gateway: 0.0.0.0
status.netStatus.linkLocalIPv6Address: FE80::20F:9CFF:FE03:3FB7
status.netStatus.autoConfigIPv6Address: ::
status.netStatus.ethMacAddr: 00:0f:9c:03:3f:b7
PANDUIT>
    
```

Figure 4: Network information from CLI

## 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).

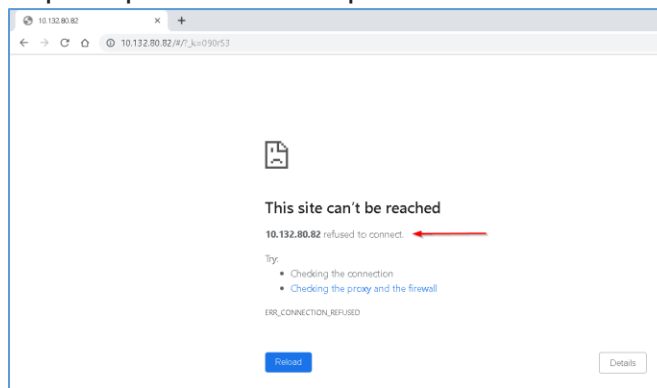
### Web Connection

#### Supported Web Browsers

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

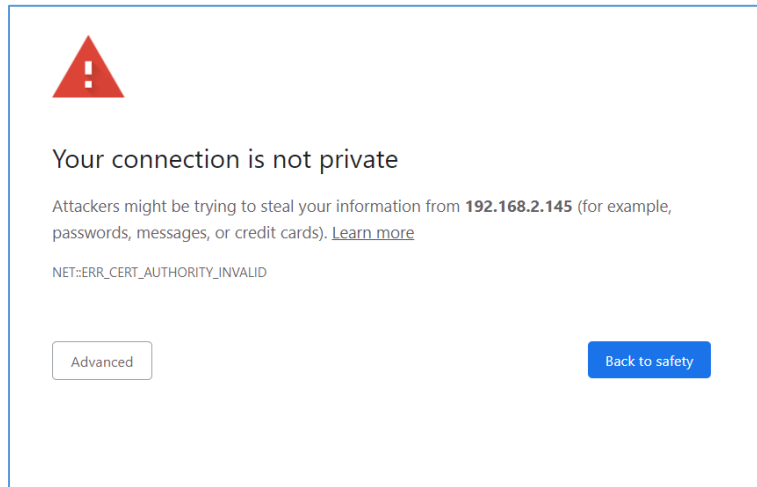
#### Logging in to the Web Interface

- 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://”



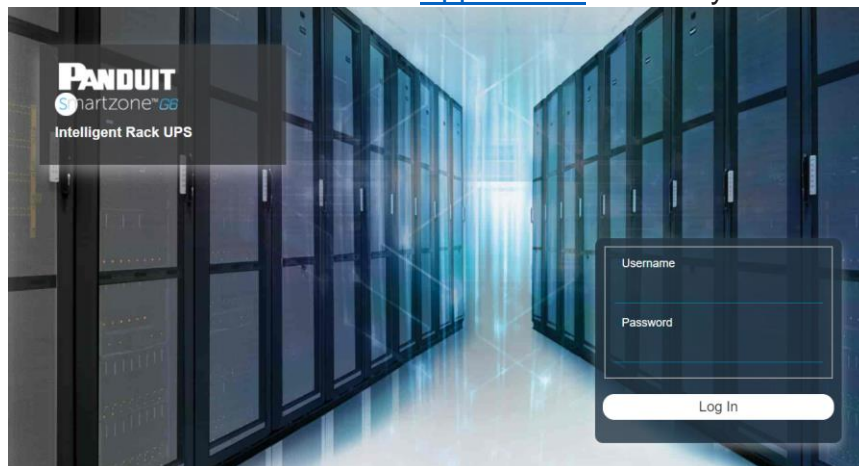
**Figure 5: Refused Connection Example**

- 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.

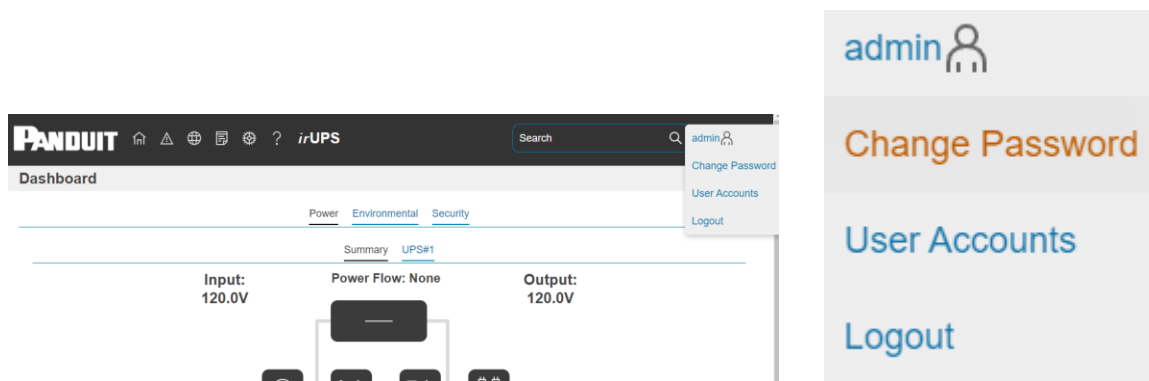


**Figure 8: Changing Your Password**

- 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**

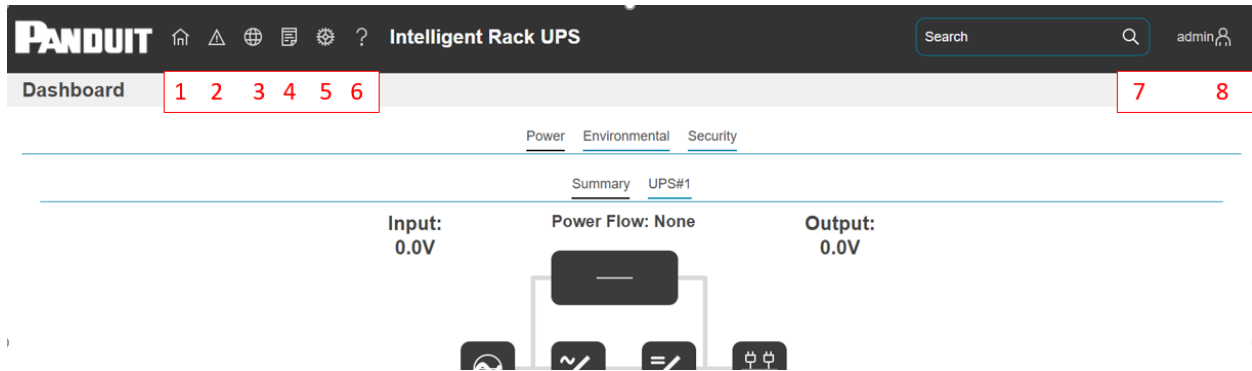
- 2. The **Change Password** window opens.
- 3. Follow the previous instructions in **Changing Your Password** and Figure 8:

## 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.
7		The search icon allows you to input key words and search for the related results.


Number	Icon	Description
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**

-  Dashboard
- Identification
- Control & Manage


**Alarms**

-  Active Alarms


**Language**

-  English
- Français
- Deutsch
- Español


**Logs**

-  Event Log
- Data Log


**Setting**

-  Network Settings
- System Management
- SNMP Manager
- Email Setup
- Trap Receiver
- User Accounts
- Thresholds
- Wi-Fi Settings

**Help**

-  Support

**User**

- admin 
- Change Password
- User Accounts
- Logout

## Introduction to the Dashboard

### Power Summary Page

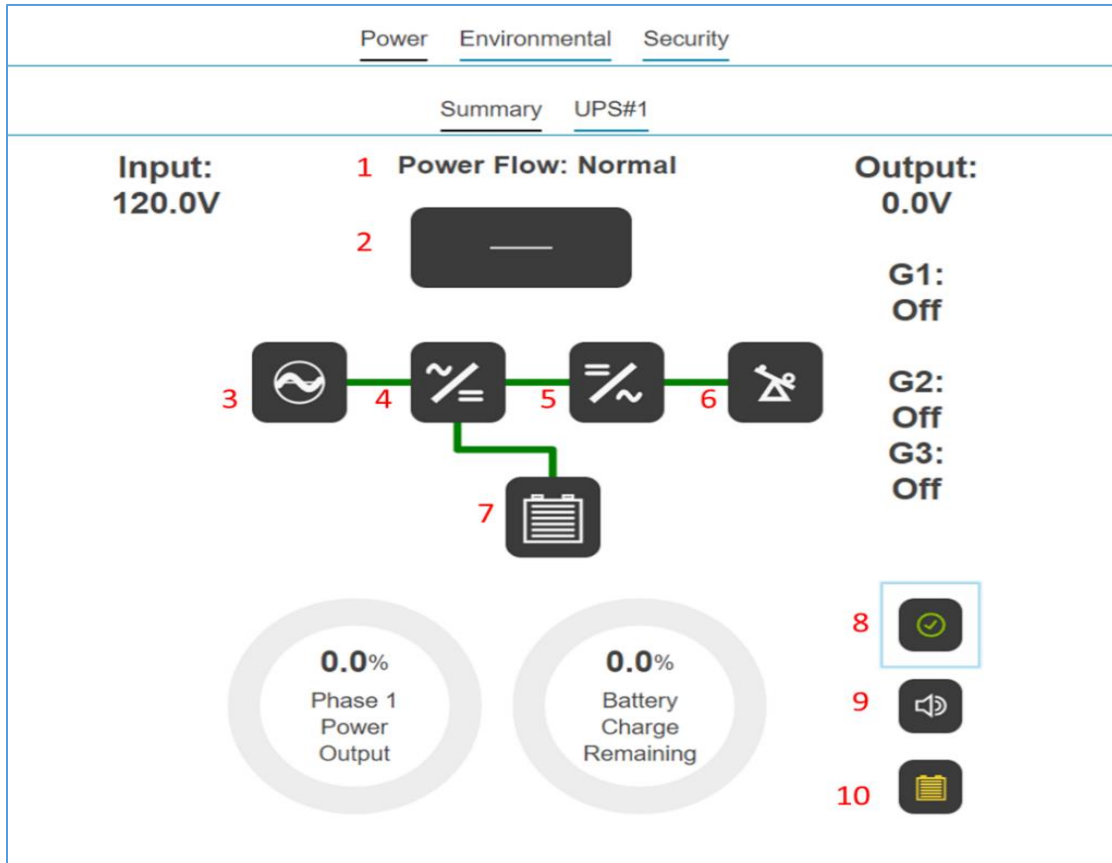


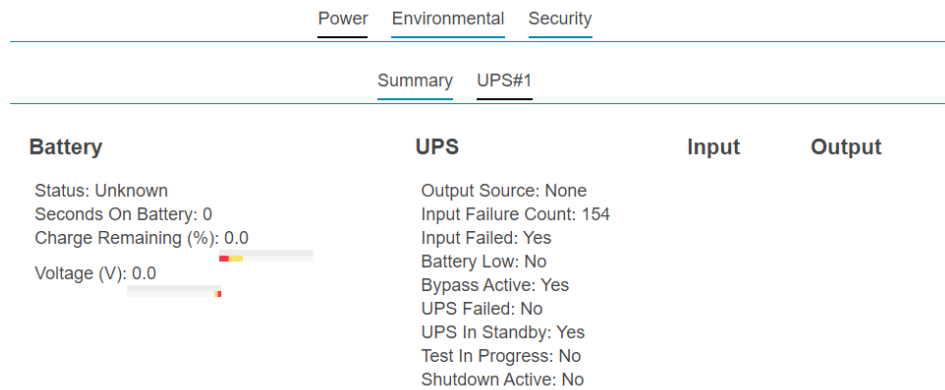
Figure 11: Power Summary Page

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

[Power](#)   [Environmental](#)   [Security](#)

---

**Internal Sensors**

---

Temperature (°C)

---

30

**External Sensors**

Type	Sensor Name	Serial Number	Value	Status
Temperature		CN0145911B T1	23.0°C	✓OK
Temperature		CN0145911B T2	29.0°C	✓OK
Temperature		CN0145911B T3	24.0°C	✓OK
Humidity		CN0145911B RH	29.0%RH	✓OK

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

[Power](#)   [Environmental](#)   [Security](#)

---

**Security Sensors**

Type	Sensor Name	Serial Number	Value	Status
Door		CN0048966C DOOR SWITCH	CLOSED	✓OK

Figure 14: Security Monitoring Page

## Network Settings

The Network Settings allow management of IP Configuration, DNS, Web Access, SSH Configuration, Syslog Configuration, Network Time Protocol (NTP), Date/Time Configuration and Time Zone Configuration.

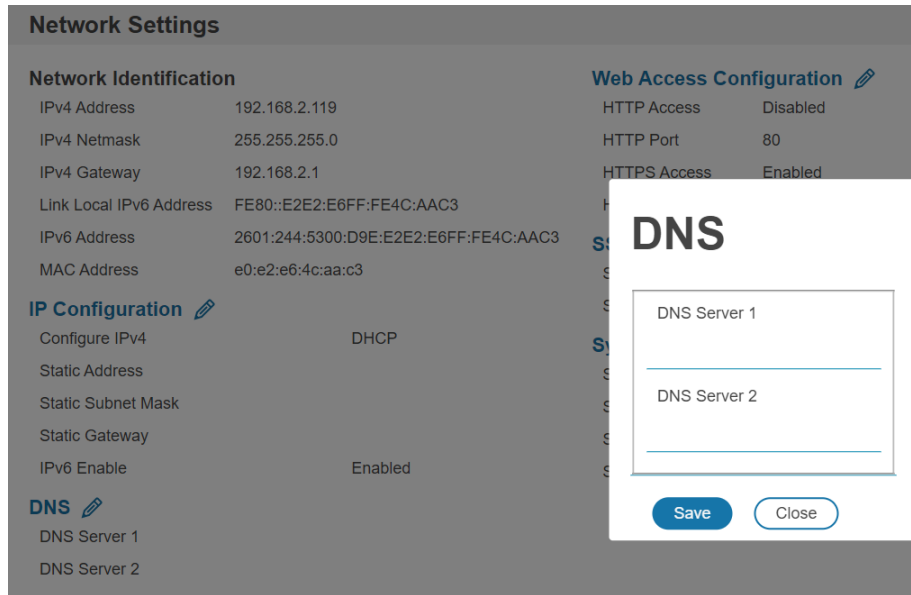
*Ethernet Interface Configuration:*

### Ethernet Interface Configuration

IPv4 Enable	<input checked="" type="checkbox"/> Enable
IPv4 Configure Method	DHCP <span>▼</span>
IPv4 Static Address	
IPv4 Static Subnet Mask	
IPv4 Static Gateway	
IPv6 Enable	<input checked="" type="checkbox"/> Enable
IPv6 Configure Method	Autoconfiguration <span>▼</span>
IPv6 Static Address	
IPv6 Static Prefix Length	64
IPv6 Static Router	

**Figure 15: Ethernet Interface Configuration**

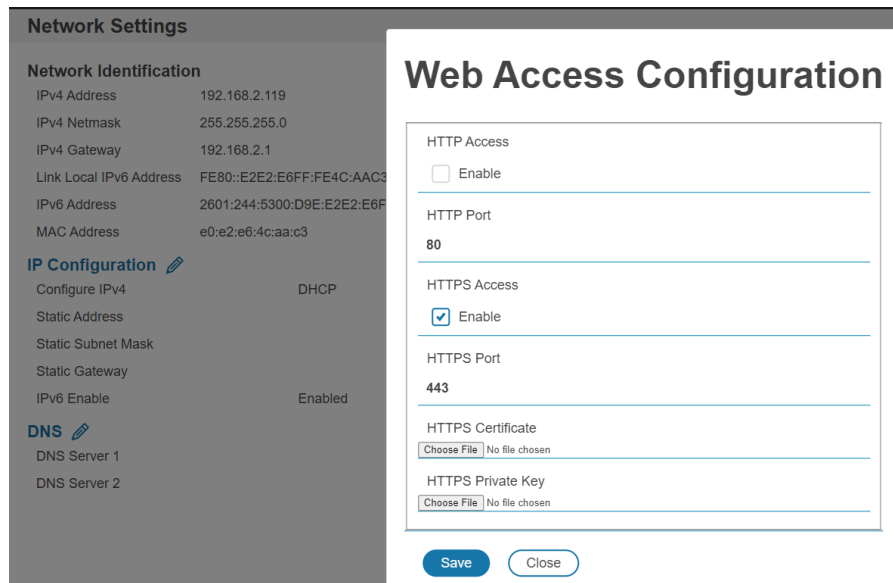
*DNS configuration:*



**Figure 16: DNS Configuration**

*Web Access Configuration*

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



**Figure 17: Web Access Configuration**

SSH Configuration:

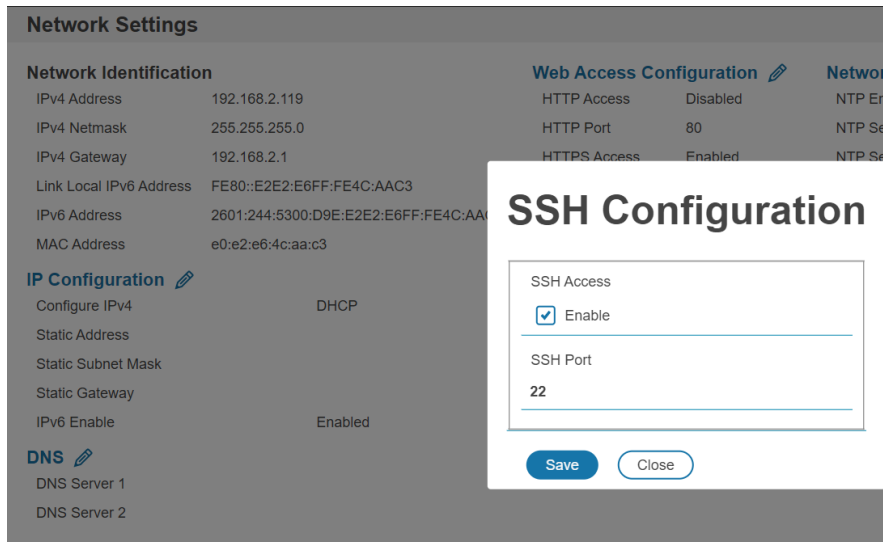


Figure 18: SSH Configuration

Syslog Configuration:

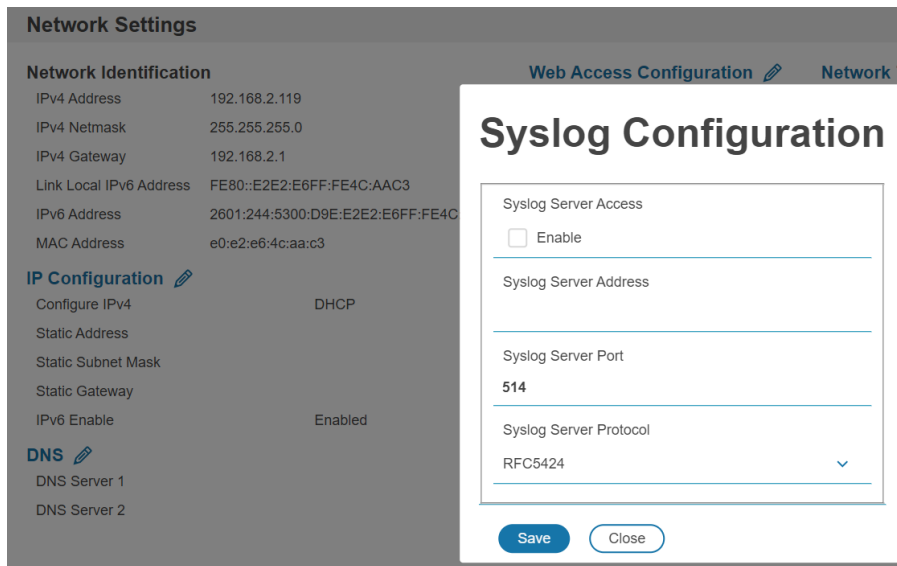


Figure 19: Syslog Configuration

Network Time Protocol (NTP)

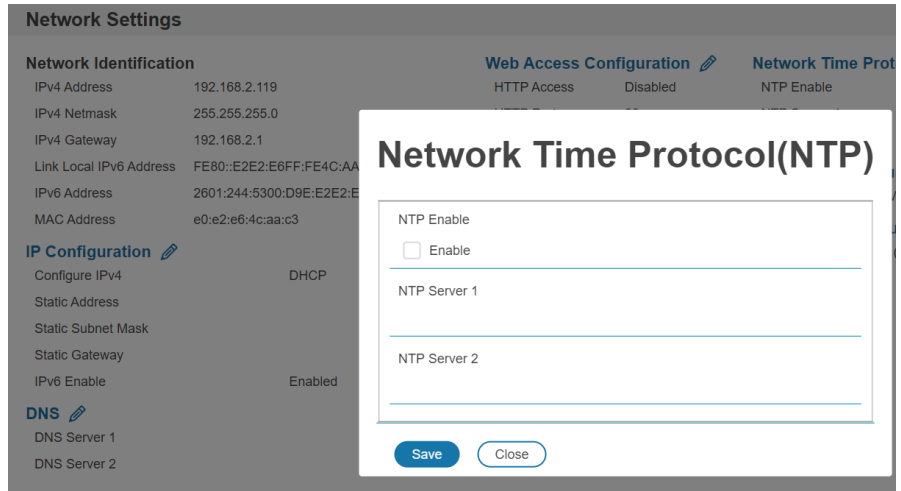


Figure 20: Network Time Protocol

*Date/Time Configuration:*

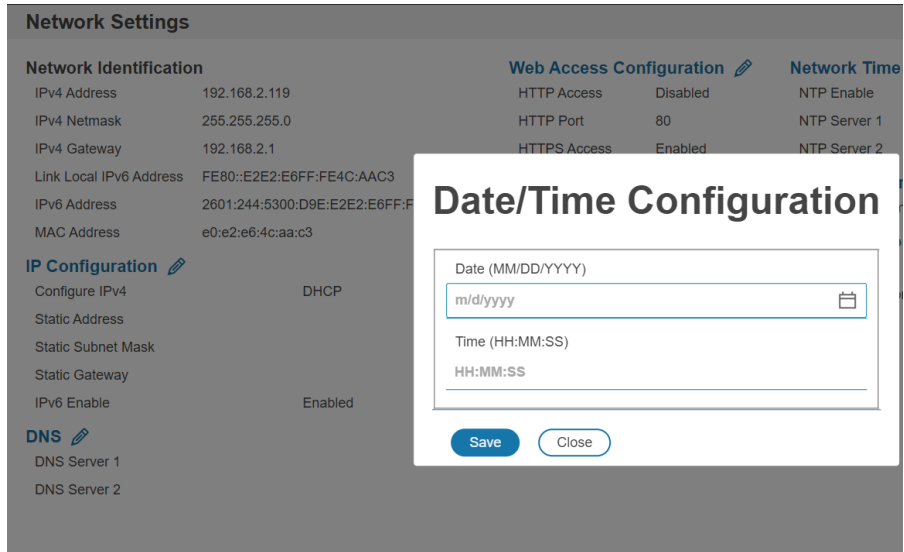
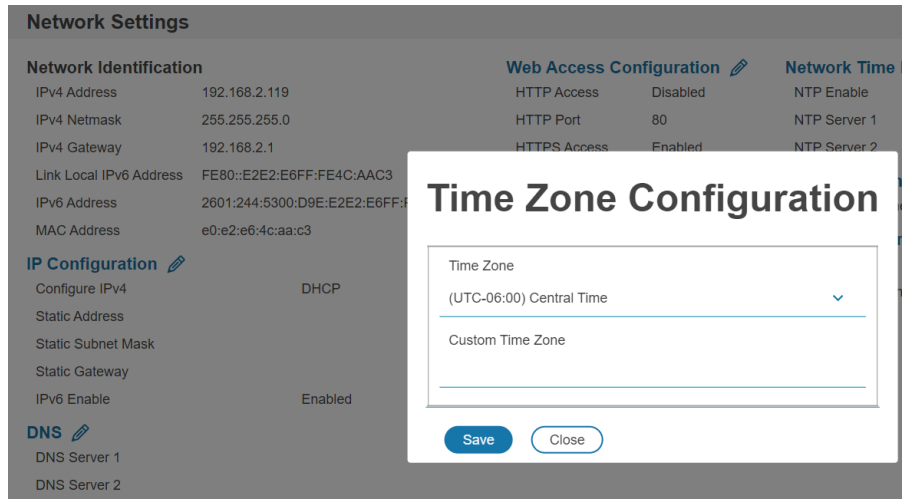


Figure 21: Date/Time Configuration

*Time Zone Configuration:*

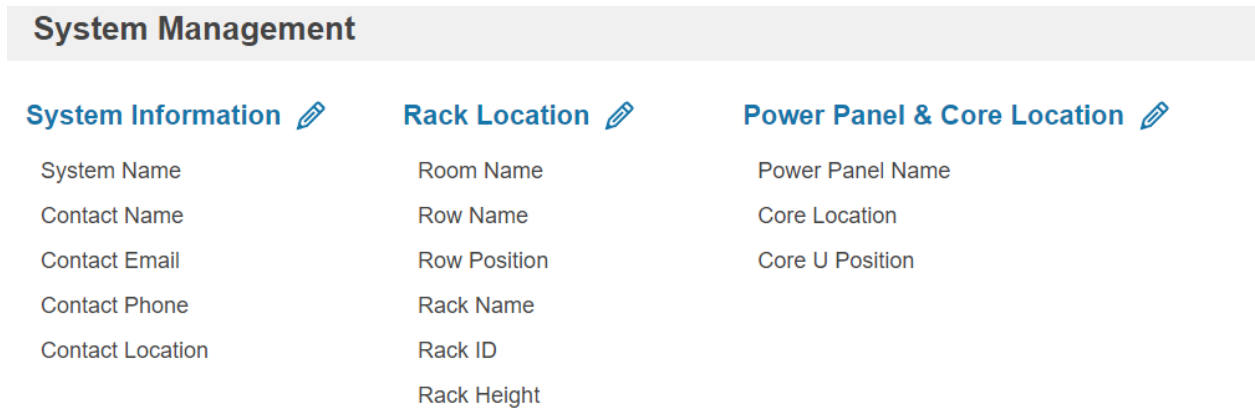


**Figure 22: Time Zone Configuration**

## 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 23: System Management**

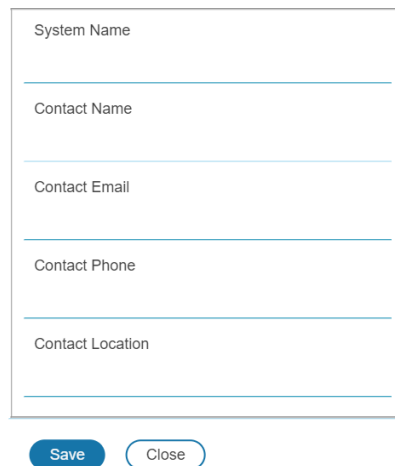
### System Info

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**.

## System Information



The screenshot shows a web form titled "System Information". It contains five text input fields, each with a label above it: "System Name", "Contact Name", "Contact Email", "Contact Phone", and "Contact Location". Below the form are two buttons: a blue "Save" button and a white "Close" button with a blue border.

**Figure 24: 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**.



## Rack Location

Room Name

---

Row Name

---

Row Position

---

Rack Name

---

Rack ID

---

Rack Height

---

Save Close

**Figure 25: 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**.

## Power Panel & Core Location

Power Panel Name

Core Location

Core U Position

Save Close

**Figure 26: 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**.

## Setting Time and Date on the NMC

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

### *Manually Setting Time and Date*

1. Go to **Network Settings** and select **Date/Time Configuration**.

Date/Time Configuration

Date (MM/DD/YYYY)

m/d/yyyy

Time (HH:MM:SS)

HH:MM:SS

Save Close

**Figure 27: Setting the Date and Time**

2. Enter the date using the MM/DD/YYYY format or use the calendar icon to select a date.
3. Enter the time in the three fields provided: the hour in the first field, minutes in the next field, and seconds in the third field. Time is measured in 24-hour format. Enter 13 for 1:00pm, 14 for 2:00pm, etc.
4. Press **Save**.

*Configure Network Time Protocol (NTP)*

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

## Network Time Protocol(NTP)

The screenshot shows a configuration window titled "Network Time Protocol(NTP)". At the top, it says "NTP Enable" with an unchecked checkbox labeled "Enable". Below this is a horizontal line, followed by the label "NTP Server 1" and an empty text input field. Another horizontal line follows, with the label "NTP Server 2" and another empty text input field. At the bottom of the window, there are two buttons: a blue "Save" button and a white "Close" button with a blue border.

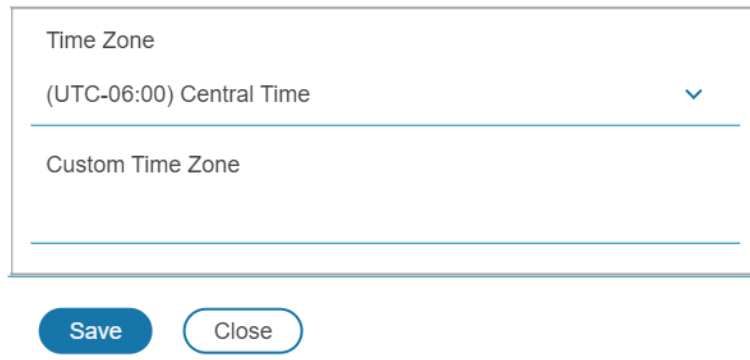
**Figure 28: NTP Configuration**

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

*Time Zone Configuration*

1. Go to **Network Settings** and select **Time Zone Configuration**.

## Time Zone Configuration



Time Zone  
(UTC-06:00) Central Time

Custom Time Zone

Save Close

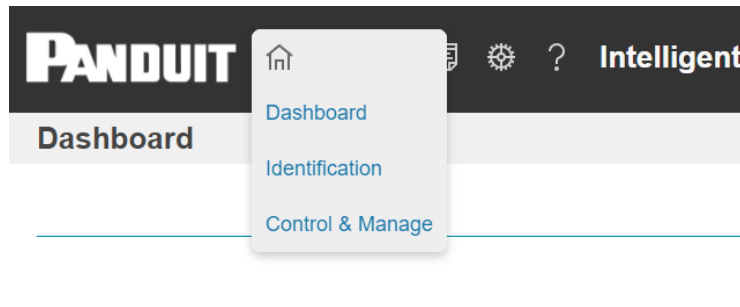
**Figure 29: Daylight Saving Time Zone Configuration**

2. Select a predefined time zone from the pull-down menu.
3. If the desired time zone is not in pull down menu, enter the 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.



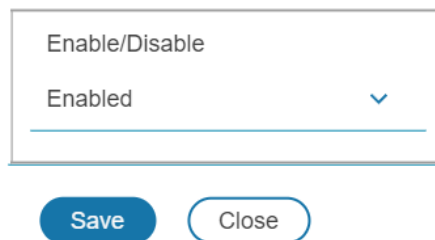
**Figure 30: Control & Manage**

*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 or 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**.

## Audible Alarm



**Figure 31: Audible Alarm Configuration**

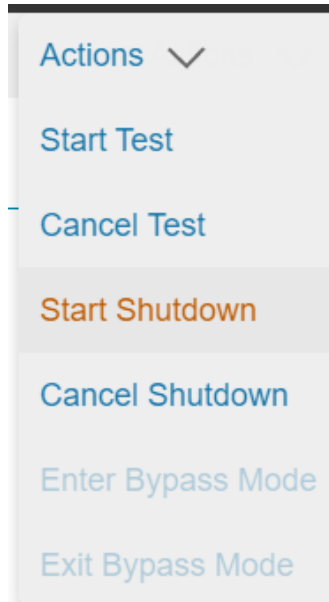
3. Select Enable or Disable.
4. Then select **Save**

*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**.



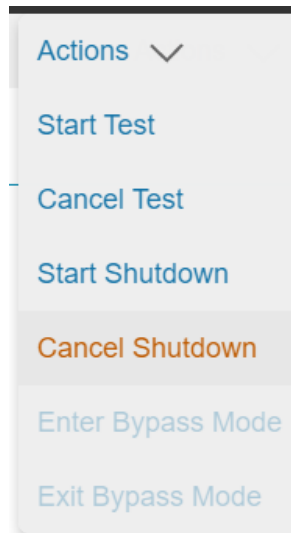
**Figure 32: Start Shutdown Example**

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.



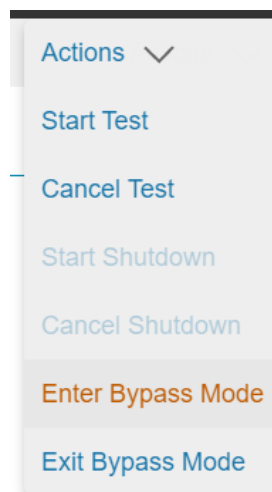
**Figure 33: Cancel Shutdown Example**

### *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 34: 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.

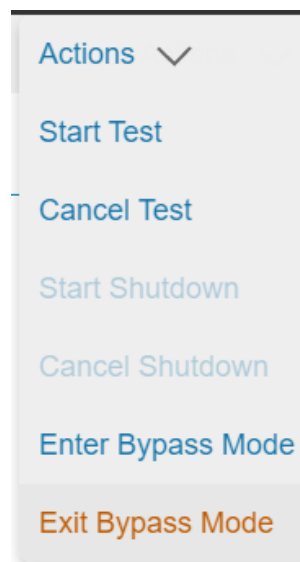


Figure 35: Exit Bypass Example

### Battery Test

#### Manual Battery Test

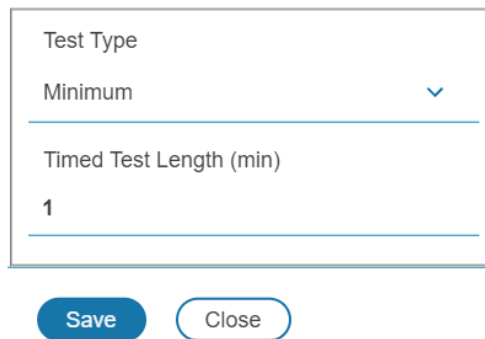
Running the manual battery test is a two-step process. The user must first configure the type of the test to run and then initiate the test.

#### 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**.



## UPS Manual Test



Test Type  
Minimum

Timed Test Length (min)  
1

Save Close

**Figure 36: UPS Manual Test Configuration**

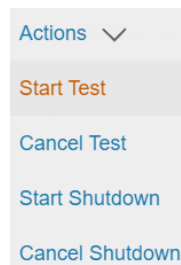
3. Select the **Test Type** from the pull-down menu. The options are
  - a. **Minimum**: This is a quick test of the battery
  - b. **Timed**: Test the battery for the configured time.
  - c. **Full Discharge**: Places the system on the battery for a full discharge.

**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 37: Start Test Example**

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

# Start Test

Are you sure you want to do this?

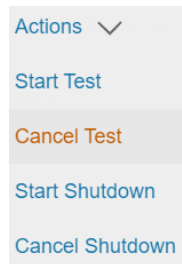


**Figure 38: Start Test Confirmation**

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 39: Cancel Test Example**

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

# Cancel Test

Are you sure you want to do this?



**Figure 40: 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**.

## Battery Test

The screenshot shows a configuration window titled "Battery Test". It contains the following elements:

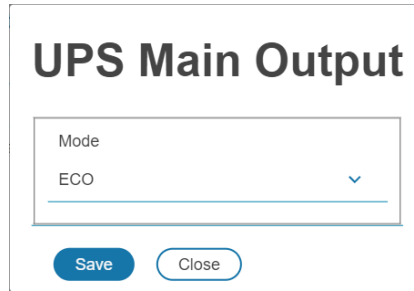
- An "Enable" section with a checked checkbox labeled "Automatic Battery Test".
- A "Period (days)" input field containing the number "14".
- Two buttons at the bottom: "Save" (a blue button) and "Close" (a white button with a blue border).

**Figure 41: Battery Test Configuration**

### UPS Main Output Mode

The Output Mode setting controls mode of operation during normal operation. Output mode is overridden if the UPS is in bypass or running on battery. 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. Then select **Save**.



**Figure 42: UPS Mode Example**

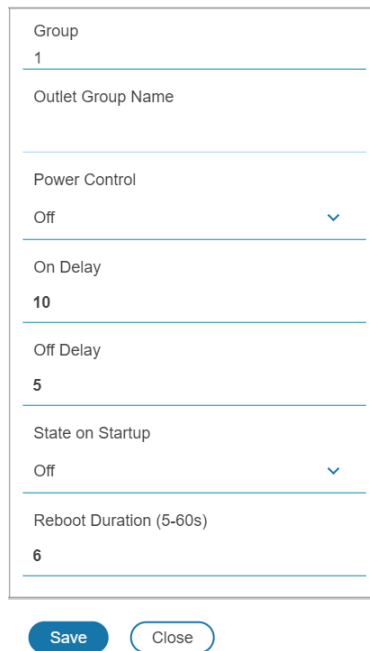
*Outlet Group Control*

*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.

**Edit Outlet Group**



**Figure 43: 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.

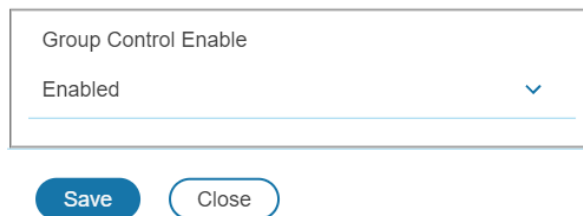
Switching an Outlet Group On or Off

This is only applicable to outlet group 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**

## Outlet Group Control



**Figure 44: 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.

**Note:** If outlet group 1 is off, all other outlet groups will automatically be turned off. For example, if you reboot outlet group 1, outlet group 2 will be rebooted.

### 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.

Group	Outlet Group Name	Power Control	On Delay	Off Delay	State on Startup	Reboot Duration (5-60s)	
1		Off	10	5	Off	5	
2		Off	5	5	Off	5	

**Figure 45: Edit Outlets**

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

### Edit Outlet Group

Group  
1

Outlet Group Name

Power Control  
Off

On Delay  
10

Off Delay  
5

State on Startup  
Off

Reboot Duration (5-60s)  
5

**Save** **Close**

**Figure 46: 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.

### Edit Shutdown Group

The screenshot shows a configuration form for an 'Edit Shutdown Group'. The form is titled 'Edit Shutdown Group' and contains the following fields and options:

- Group:** 1
- Group Name:** GroupName
- Shutdown Type:** Time On Battery (with a dropdown arrow)
- Time (0-7200s):** 10
- Capacity (%):** 70
- Request Group Off:**  Turn Off when Shutdown Type occurs
- Outlet Group:** outletGroup1 (with a dropdown arrow)
- Restore After Shutdown:**  Restore

At the bottom of the form, there are two buttons: a blue 'Save' button and a white 'Close' button with a grey border.

**Figure 47: 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 will 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 threshold, 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.

## Edit Smart Load

Load	1
Enable	<input checked="" type="checkbox"/> Enabled
Name	ServerName
Group	shutdownGroup1
Shutdown Delay (0-600s)	10
Shutdown Agent Method	SSH Custom Command
Shutdown Agent Address	
Shutdown Agent UserName	
Shutdown Agent Password	
Confirm Agent Password	
SSH Shutdown Agent Identity (hash)	
Command	shutdown /s
<input type="button" value="Save &amp; Test Connection Only"/>	
<input type="button" value="Save &amp; Test Shutdown"/>	

**Figure 48: 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.
  - 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.
  - 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. Finally, you can test the configuration.
  - a. **Save & Test Connection Only** - This option will save modified settings and verify the configured user can connect to the configured device and can log in but will not issue the shutdown command.
  - b. **Save & Test Shutdown** - This option will save modified settings and verify the configured user can connect to the device, log in, and then issue the shutdown command. **NOTE:** The configured device will shutdown.
  - c. **Save** – The data will be saved to the 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.

### Edit Shutdown Schedule

Schedule	1
Enable	<input type="checkbox"/> Enabled
Shutdown Group	All Groups <span>▼</span>
Recurrence	Once <span>▼</span>
Day Of Week	Sunday <span>▼</span>
Start Year	2021
Start Month	January <span>▼</span>
Start Day	1
Start Hour	0
Start Minute	0
Duration (0-1440min)	1

**Figure 49: Shutdown Schedule Configuration**

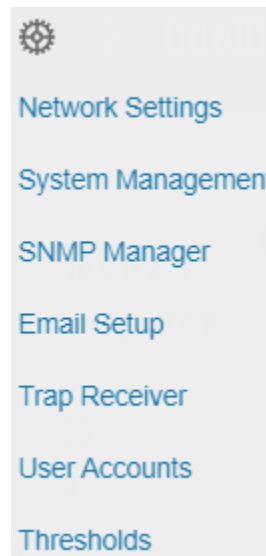
4. Enable the schedule shutdown by selecting **Enable**. If the schedule is not enabled, it will not be shut down.
5. Select the associated shutdown groups. The user can select an individual group or **All Groups**
6. Select how often this shutdown will occur.
  - a. **Once** – The shutdown will happen 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 50: Email Setup**

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

## SMTP Account Settings

SMTP server
Sender email address
Username
Password
Confirm Password
Port
25
Number of retry attempts
3
Time interval between retry attempts (in minutes)
6
Security
None <span>▼</span>
Server requires authentication
<input type="checkbox"/> Enable

[Save](#) [Close](#)

**Figure 51: 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.



## Edit Email Recipient

Email Address

---

Enable

Enable

---

Save
Close

**Figure 52: 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.

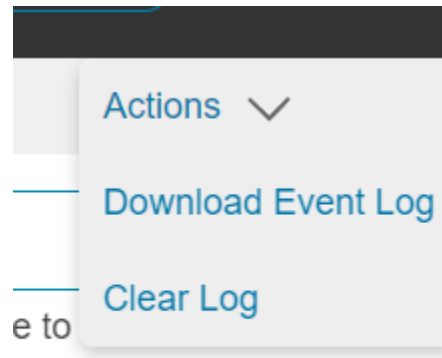
## Event Log

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

Event Log				
Timestamp	Source	Severity	Description	
January 1, 1970 10:55:12 AM	USER	Info	User admin from host 192.168.1.2 via WebUI logged out due to inactivity	
January 1, 1970 10:42:46 AM	USER	Info	User admin from host 192.168.1.2 via WebUI logged in	
January 1, 1970 10:24:34 AM	USER	Info	User admin from host 192.168.1.2 via WebUI logged in	
January 1, 1970 10:24:09 AM	NMC	Info	mgmt firmware update to 1.1.2 Complete	
January 1, 1970 10:23:39 AM	NMC	Info	mgmt firmware update to 1.1.2 Started	
January 1, 1970 10:21:53 AM	USER	Info	User admin from host 192.168.1.2 via WebUI logged in	

**Figure 53: Event log**

Event log can be downloaded or cleared from Actions menu.

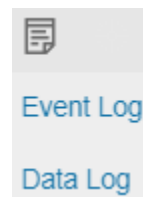


**Figure 54: Event log Actions menu**

## 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 55: Data Log**

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

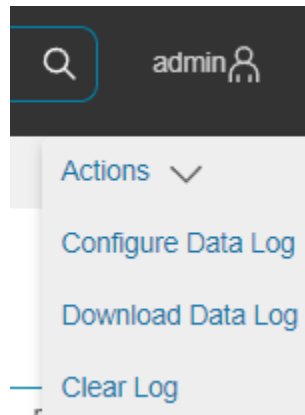


Figure 56: Data Log Configuration

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.)

## Data Log Configuration

A screenshot of the 'Data Log Configuration' panel. It features a text input field with the label 'Log Interval (1-1440 Minutes)' and the value '60'. Below the input field are two buttons: a blue 'Save' button and a white 'Close' button with a blue border.

Figure 57: 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.

The screenshot shows the 'User Accounts' settings page in the Panduit Intelligent Rack UPS interface. At the top, there is a navigation bar with the Panduit logo, home, back, forward, search, and help icons, and the text 'Intelligent Rack UPS'. A search box and a user profile icon labeled 'admin' are also present.

The main content area is titled 'User Accounts' and contains three sections:

- Users:** A table with columns for Username, Role, and Enabled. The 'admin' user is listed with roles 'Admin' and 'Viewer', both of which are enabled.
- LDAP Configuration:** A list of settings including 'Enable LDAP' (Disabled), 'LDAP Server', 'Port' (389), 'Security' (None), 'Verify Certificate' (Disabled), 'Base DN', 'Search User DN', 'Login Name Attribute', and 'User Entry Object Class'.
- RADIUS Configuration:** A list of settings including 'Enable RADIUS' (Disabled), 'RADIUS Server', and 'RADIUS Port' (1812).

**Figure 58: User Accounts**

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

## RADIUS Configuration

Enable RADIUS

Enable

---

RADIUS Server

---

RADIUS Port

**1812**

---

RADIUS Secret

---

Confirm Password

---

**Save** **Close**

**Figure 59: 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.

### LDAP Configuration

The screenshot shows a configuration form with the following fields and values:

- Enable LDAP:  Enable
- LDAP Server: \_\_\_\_\_
- Port: 389
- Security: None
- Verify Certificate:  Verify (only valid if using TLS/startTLS)
- Base DN: \_\_\_\_\_
- BIND Password: \_\_\_\_\_
- Confirm Password: \_\_\_\_\_
- Search User DN: \_\_\_\_\_
- Login Name Attribute: \_\_\_\_\_
- User Entry Object Class: \_\_\_\_\_

Buttons: Save, Close

**Figure 60: 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).



## Edit Role

Role

---

Description

---

Privilege Level

None ▼

---

Enable Role

enable

---

**Save** **Close**

**Figure 61: 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.

**Wi-Fi Settings**

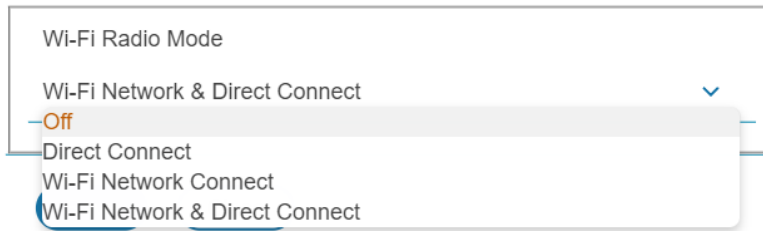
<p><b>Wi-Fi Network Identification</b></p> <p>IPv4 Address</p> <p>IPv4 Netmask</p> <p>IPv4 Gateway</p> <p>Link Local IPv6 Address</p> <p>IPv6 Address</p> <p>MAC Address      00:0f:9c:03:07:78</p>	<p><b>Wi-Fi Radio Configuration</b> </p> <p>Wi-Fi Radio Mode    Wi-Fi Network &amp; Direct Connect</p> <p><b>Wi-Fi Network Configuration 1</b> </p> <p>Network Configuration    Disabled</p> <p>Network Name</p> <p>Security                    WPA2 Personal</p>	<p><b>Direct Connect Configuration</b> </p> <p>Direct Connect Start Mode    On Demand</p> <p>Preferred 2.4GHz Channel    1</p> <p>Network Name                  panduit-ups-nmc-000f9c03077b</p> <p>IPv4 Address                    192.168.5.1</p> <p>Captive Portal                  <b>Enabled</b></p>
<p><b>Wi-Fi Interface Configuration</b> </p> <p>IPv4 Enable                    Enabled</p> <p>IPv4 Configure Method        DHCP</p> <p>IPv4 Static Address</p> <p>IPv4 Static Subnet Mask</p> <p>IPv4 Static Gateway</p> <p>IPv6 Enable                    Enabled</p> <p>IPv6 Configure Method        Autoconfiguration</p> <p>IPv6 Static Address</p> <p>IPv6 Static Prefix Length    64</p> <p>IPv6 Static Router</p>		

**Figure 62: 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.

# Wi-Fi Radio Configuration



**Figure 63: 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.

## Direct Connect Configuration

Direct Connect Start Mode  
On Demand

---

Preferred 2.4GHz Channel  
1

---

Network Name  
panduit-ups-nmc-000f9c03077b

---

Network Password

---

Confirm Network Password

---

IPv4 Address  
192.168.5.1

---

Captive Portal  
 Enable

Save Close

**Figure 64: Wi-Fi Direct Connect Configuration**

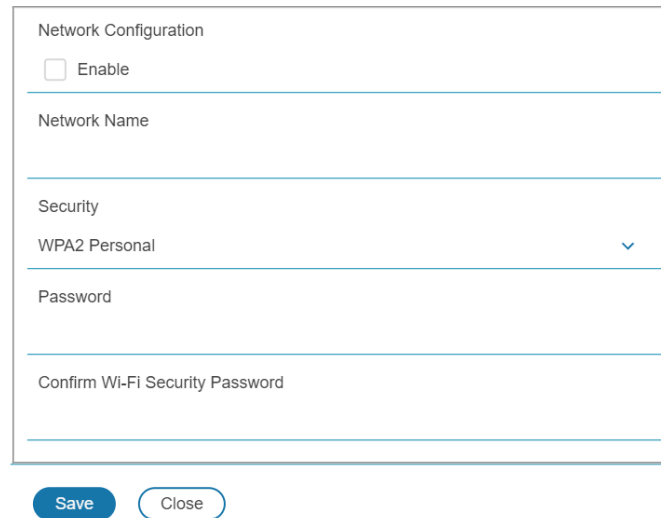
1. Select Start mode option
  - On Demand: Push the reset button to start the Direct Connect mode and it is available for the following 10 minutes.
  - Always On: Direct Connect is always active.
2. Fill in desirable Direct Connect network settings that mobile devices will use.
3. Click Save button.

### 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.

## Wi-Fi Network Configuration 1



The image shows a web form titled "Network Configuration". It contains the following fields and controls:

- An "Enable" checkbox, which is currently unchecked.
- A "Network Name" text input field.
- A "Security" dropdown menu currently set to "WPA2 Personal".
- A "Password" text input field.
- A "Confirm Wi-Fi Security Password" text input field.
- At the bottom, there are two buttons: "Save" (highlighted in blue) and "Close".

**Figure 65: 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.

## Wi-Fi Network Configuration 1

Network Configuration

Enable

---

Network Name

---

Security

WPA2 Enterprise ▼

---

Extensible Authentication Protocol

TTLS ▼

---

User Name

---

Password

---

Confirm Wi-Fi Security Password

---

Inner Authentication

MSCHAPv2 ▼

---

Outer Identity

---

Server Certificate

Choose File No file chosen

---

Verify Certificate

Verify Server Certificate

---

Save
Close

**Figure 66: 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.

## Wi-Fi Interface Configuration

IPv4 Enable	<input checked="" type="checkbox"/> Enable
IPv4 Configure Method	DHCP <span>▼</span>
IPv4 Static Address	
IPv4 Static Subnet Mask	
IPv4 Static Gateway	
IPv6 Enable	<input checked="" type="checkbox"/> Enable
IPv6 Configure Method	Autoconfiguration <span>▼</span>
IPv6 Static Address	
IPv6 Static Prefix Length	64
IPv6 Static Router	

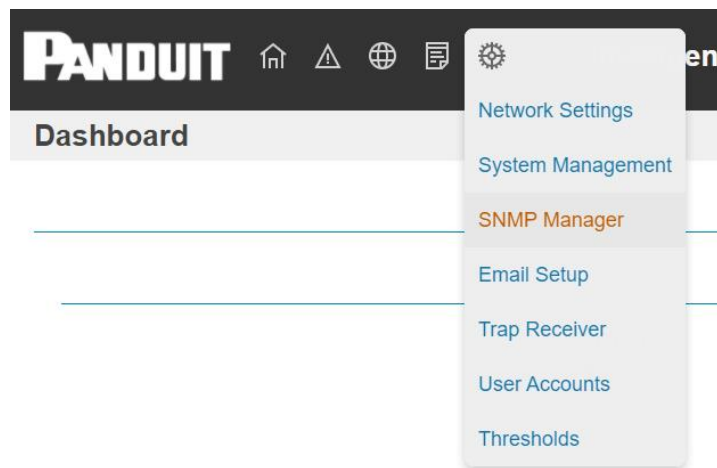
**Figure 67: Wi-Fi Interface Configuration**

## Section 3 – Simple Network Management Protocol (SNMP)

### SNMP Management Configuration

#### *Setup SNMP*

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



**Figure 68: SNMP Management**

3. The SNMP General includes SNMP Access and Version.

## SNMP General

Enable SNMP

Enable

---

SNMP Version

V12CV3 ▼

---

[Save](#) [Close](#)

**Figure 69: SNMP General**

### Setup SNMP Port

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

SNMP Port	
SNMP Port	161
SNMP Trap Port	162

**Figure 70: SNMP Port**

3. Set up SNMP Port and SNMP Trap Port.



# SNMP Port

SNMP Port

**161**

---

SNMP Trap Port

**162**

---

Save
Close

**Figure 71: Setup SNMP Port and Trap Port**

## Configuring Users for SNMP V1/V2c

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

### SNMP v1/v2c Manager

IP Address	Read Community	Write Community	Enabled	
0.0.0.0	public	private	Enabled	
0.0.0.0	public	private	Disabled	
0.0.0.0	public	private	Disabled	
0.0.0.0	public	private	Disabled	
0.0.0.0	public	private	Disabled	

**Figure 72: Define SNMP V1/V2c User**

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

### Edit v2 User

IP Address
0.0.0.0
Read Community
public
Write Community
private
Enabled
<input checked="" type="checkbox"/> Enable






**Figure 73: Edit V1/2c Manager**

- 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.
- Click **Enable** and **Save**.

## Configuring Users for SNMP v3

- Access the Web interface and log in.
- Under Settings, select **SNMP Manager**.
- 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 74: SNMP v3 Manager**

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

## Edit v3 User

Username
Security Level
AuthPriv <span>▼</span>
Authentication Password
Confirm Password
Authentication Algorithm
SHA <span>▼</span>
Privacy Key
Confirm Password
Privacy Algorithm
AES128 <span>▼</span>
Enabled
<input type="checkbox"/> Enable

[Save](#) [Close](#)

**Figure 75: 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
    - AES-192
    - AES-256
  11. Click **Enable** and **Save**.

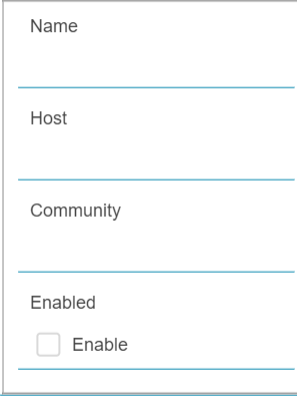
## Configuring SNMP Traps

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 > Trap Receiver
2. Click the pencil next to SNMPV2c Trap Receiver you want to update.

## Edit v2c Trap



Name

Host

Community

Enabled

Enable

Save Close

**Figure 76: 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 > Trap Receiver
2. Click the pencil next to SNMPV3 Trap Server you want to update.

## Edit v3 Trap

Name	
Host	
Security Level	AuthPriv
Authentication Password	
Confirm Password	
Authentication Algorithm	SHA
Privacy Key	
Confirm Password	
Privacy Algorithm	AES128
Enabled	<input type="checkbox"/> Enable

[Save](#) [Close](#)

**Figure 77: SNMPv3 Trap Server configuration Information.**

3. Enter the **Name** and **Host** name in the fields provided.
  - a. The name is a user assigned name to help distinguish the different receivers.
  - b. The host name is the IP Address to which the traps are sent by the SNMP system agent.
4. Choose a Security Level from the dropdown menu
  - NoAuthNoPriv: No authentication and no privacy. This is the default.
  - AuthNoPriv: Authentication and no privacy.
  - AuthPriv: Authentication and privacy.

5. Enter the **Authentication Password** from the SNMP Server to be used for authentication. Repeat the authentication password below it in **Confirm Password**.
6. Select the desired authentication algorithm.
  - MD5
  - SHA
7. Enter the **Privacy Key** from the SNMP Server for privacy algorithm. Repeat the privacy key below it in **Confirm Password**.
8. Select the desired privacy algorithm.
  - AES-128
  - AES-192
  - AES-256
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 – SmartZone G5 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 SmartZone G5 accessories are specially designed to interoperate The UPS NMC controller. Connecting unapproved sensors to the NMC controller or connecting SmartZone G5 Sensors to 3<sup>rd</sup> 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
SmartZone G5 Dry Contact Sensor (ACC01)	Input to the UPS NMC and designed to monitor a change in contact state.	1

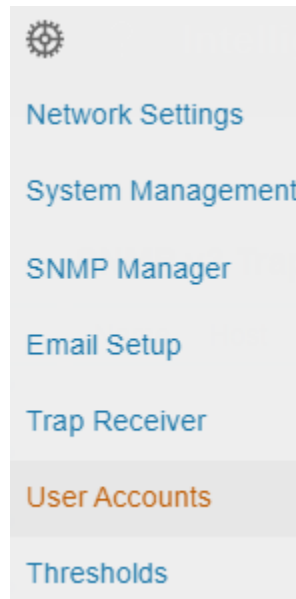


Figure 78: Sensor Port

## Configuring Temperature Scale

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

1. Go to **User Accounts**.



**Figure 79: User Accounts**

2. Select the pencil next to **Region**

## Region

A dialog box titled 'Region'. It contains a label 'Temperature Units' above a dropdown menu showing '°C'. Below the dropdown are two buttons: a blue 'Save' button and a white 'Close' button with a grey border.

**Figure 80: 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.

## Thresholds

### Environmental Sensors

Sensor Name	Type	Serial Number	Low Critical	Low Warning	High Warning	High Critical	
	Temperature	CN0111901B EB001 1B T1	18°C	15°C	27°C	32°C	
Sensor Name	Type	Serial Number	Low Critical	Low Warning	High Warning	High Critical	
	Humidity	CN0111901B EB001 1B RH	10	30	60	80	

**Figure 81: 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

## Edit Temperature Sensors

Sensor Name

---

Type

Temperature ▼

---

Serial Number

CN0145911B T1

---

Low Critical Enable

High Critical Enable

Enable

---

High Critical (celsius)

32

---

Delete

Delete

**Save**
Close

**Figure 82: Temperature Sensor Edit dialog**



## Configuring Security Sensors

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

1. Open the **Settings**.

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

**Security Sensors**

Sensor Name	Type	Serial Number	Alarm Enable	Alarm Level	
	Door	CN0048966C DOOR SWITCH	Enabled	CRITICAL	
Sensor Name	Type	Serial Number	Alarm Enable	Alarm Level	Alarm State
	Dry	CN0140914E DRYCONTACT	Enabled	CRITICAL	Open 

**Figure 83: Security Sensor Alarm Configuration view**

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

## Edit Dry Contact Sensor

Sensor Name	
Type	Dry <span>▼</span>
Serial Number	<b>CN0140914E DRYCONTACT</b>
Alarm Enable	<input checked="" type="checkbox"/> Enable
Alarm Level	CRITICAL <span>▼</span>
Alarm State	Open <span>▼</span>
Delete	<input type="checkbox"/> Delete

Figure 84: Dry Contact Sensor Edit dialog

### Deleting Sensors

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

## Section 6 – 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.

### 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 reset to defaults feature erases the flash memory that is used to temporarily store firmware update uploads.
- The reset to defaults feature causes the SSH RSA 2048-bit private host key to be regenerated.

### 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.



## Authentication Data

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

## Network Transport Security

- The product generates a random SSH RSA 2048-bit private host key the first time the product starts up.
- The product has a randomly generated RSA 2048-bit private key configured by the factory. This key is used to generate a HTTPS certificate the first time the product starts up.
- The user may upload a custom HTTPS certificate and private key.
  - The HTTPS certificate should use a SHA-256 signature.
  - The private key should be RSA 2048-bit or prime256v1 (SECP256R1).
  - Other private key types may work, but performance may be negatively impacted if greater private key sizes are used: RSA 3072-bit, RSA 4096-bit; ECC curves: SECP192R1, SECP224R1, SECP256R1, SECP384R1, SECP521R1, SECP192K1, SECP224K1, SECP256K1, BP256R1, BP384R1, BP512R1, CURVE25519.
- The product uses TLS 1.2 to communicate with HTTPS web browser clients.
- Secure communication cipher negotiation with HTTPS clients uses these Cipher Suites:
  - Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256 (0xc02b)
  - Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 (0xc02f)
  - Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384 (0xc02c)
  - Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 (0xc030)

- Cipher Suite:  
TLS\_ECDHE\_ECDSA\_WITH\_CHACHA20\_POLY1305\_SHA256 (0xcca9)
- Cipher Suite:  
TLS\_ECDHE\_RSA\_WITH\_CHACHA20\_POLY1305\_SHA256 (0xcca8)
- Cipher Suite: TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 (0x009e)
- Cipher Suite: TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 (0x009f)
- The product uses TLS 1.2 to communicate with LDAPS servers.
- The product uses TLS 1.2 to communicate with SMTP+STARTTLS and SMTPS servers.
- Secure communication cipher negotiation with SMTP servers and LDAP servers uses these Cipher Suites:
  - Cipher Suite:  
TLS\_ECDHE\_RSA\_WITH\_CHACHA20\_POLY1305\_SHA256 (0xcca8)
  - Cipher Suite:  
TLS\_ECDHE\_ECDSA\_WITH\_CHACHA20\_POLY1305\_SHA256 (0xcca9)
  - Cipher Suite: TLS\_DHE\_RSA\_WITH\_CHACHA20\_POLY1305\_SHA256 (0xcca)
  - Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384 (0xc02c)
  - Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 (0xc030)
  - Cipher Suite: TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 (0x009f)
  - Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384 (0xc024)
  - Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384 (0xc028)
  - Cipher Suite: TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA256 (0x006b)
  - Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA (0xc00a)
  - Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA (0xc014)
  - Cipher Suite: TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA (0x0039)
  - Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256 (0xc02b)
  - Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 (0xc02f)
  - Cipher Suite: TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 (0x009e)
  - Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256 (0xc023)
  - Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 (0xc027)

- Cipher Suite: TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 (0x0067)
- Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA (0xc009)
- Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA (0xc013)
- Cipher Suite: TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA (0x0033)
- Cipher Suite: TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384 (0x009d)
- Cipher Suite: TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256 (0x003d)
- Cipher Suite: TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA (0x0035)
- Cipher Suite: TLS\_ECDH\_RSA\_WITH\_AES\_256\_GCM\_SHA384 (0xc032)
- Cipher Suite: TLS\_ECDH\_RSA\_WITH\_AES\_256\_CBC\_SHA384 (0xc02a)
- Cipher Suite: TLS\_ECDH\_RSA\_WITH\_AES\_256\_CBC\_SHA (0xc00f)
- Cipher Suite: TLS\_ECDH\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384 (0xc02e)
- Cipher Suite: TLS\_ECDH\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384 (0xc026)
- Cipher Suite: TLS\_ECDH\_ECDSA\_WITH\_AES\_256\_CBC\_SHA (0xc005)
- Cipher Suite: TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256 (0x009c)
- Cipher Suite: TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256 (0x003c)
- Cipher Suite: TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA (0x002f)
- Cipher Suite: TLS\_ECDH\_RSA\_WITH\_AES\_128\_GCM\_SHA256 (0xc031)
- Cipher Suite: TLS\_ECDH\_RSA\_WITH\_AES\_128\_CBC\_SHA256 (0xc029)
- Cipher Suite: TLS\_ECDH\_RSA\_WITH\_AES\_128\_CBC\_SHA (0xc00e)
- Cipher Suite: TLS\_ECDH\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256 (0xc02d)
- Cipher Suite: TLS\_ECDH\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256 (0xc025)
- Cipher Suite: TLS\_ECDH\_ECDSA\_WITH\_AES\_128\_CBC\_SHA (0xc004)
- The product provides a SSH server with these algorithms to communicate with SSH clients:
  - Key exchange algorithms:
    - curve25519-sha256, curve25519-sha256@libssh.org, diffie-hellman-group-exchange-sha256 (2048-bit), diffie-hellman-group16-sha512, diffie-hellman-group18-sha512, diffie-hellman-group14-sha256
    - For compatibility: ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521
  - Host key algorithms:
    - rsa-sha2-512 (3072-bit), rsa-sha2-256 (3072-bit), ssh-ed25519
    - For compatibility: ssh-rsa (3072-bit), ecdsa-sha2-nistp256

- Encryption algorithms:
  - chacha20-poly1305@openssh.com, aes128-ctr, aes192-ctr, aes256-ctr, aes128-gcm@openssh.com, aes256-gcm@openssh.com
- MAC algorithms:
  - umac-128-etm@openssh.com, hmac-sha2-256-etm@openssh.com, hmac-sha2-512-etm@openssh.com
  - For compatibility: umac-64-etm@openssh.com, hmac-sha1-etm@openssh.com, umac-64@openssh.com, umac-128@openssh.com, hmac-sha2-256, hmac-sha2-512, hmac-sha1
- 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-group1-sha1, diffie-hellman-group-exchange-sha1
  - Host key algorithms:
    - ecdsa-sha2-nistp256
  - Encryption algorithms:
    - aes128-ctr, aes192-ctr, aes256-ctr, aes256-cbc, rijndael-cbc@lysator.liu.se, aes192-cbc, aes128-cbc, blowfish-cbc, arcfour128, arcfour, 3des-cbc
  - MAC algorithms:
    - hmac-sha2-256, hmac-sha2-512, hmac-sha1, hmac-sha1-96, hmac-md5, hmac-md5-96, hmac-ripemd160, hmac-ripemd160@openssh.com

## 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 these following Wi-Fi Extensible Authentication Protocols: TLS, PEAP, TTLS.
- The product supports these following Wi-Fi inner authentication methods: MSCHAPv2, MSCHAP, PAP, CHAP.
- The product communicates using Wi-Fi and provides user configurable WPA3 Personal encryption support.
- The product communicates using Wi-Fi and provides user configurable WPA3 Enterprise encryption support.

## Network Configuration Data

- Network Configuration, including Static IP addresses and addresses obtained by DHCP are exposed on an “Identification” page and on a Network Configuration page, to aid in network management of the product.
- The product implements an internal authentication mechanism, authorization events generate “Event Logs” containing the IP address and username of successful logins, and the IP address of failed logins.

## External Authorization Mechanisms

- 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.
- LDAP is not encrypted over the network.
- LDAPS is encrypted over the network.
- The remote LDAP server authenticity (fingerprint) is not validated.
- The Radius protocol is designed to only transmit hashed and obfuscated passwords over the network.

## 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 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.

## Secure deployment

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

### Upload Certificate

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

## Web Access Configuration

The screenshot shows a configuration window titled "Web Access Configuration". It contains the following sections:

- HTTP Access:** A checkbox labeled "Enable" is unchecked.
- HTTP Port:** A text field containing the value "80".
- HTTPS Access:** A checkbox labeled "Enable" is checked.
- HTTPS Port:** A text field containing the value "443".
- HTTPS Certificate:** A "Choose File" button followed by the text "No file chosen".
- HTTPS Private Key:** A "Choose File" button followed by the text "No file chosen".

At the bottom of the window, there are two buttons: "Save" (highlighted in blue) and "Close".

**Figure 85: SSL Certificate Load Screen**

### Use SNMPv3c

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

### Disabling unused interfaces

The default setting is to have HTTPS and SSH enabled. If these interfaces are not in

use, it is recommended to disable these interfaces.

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

*Review Session management*

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



---

## Warranty and Regulatory Information

### Warranty Information

(<https://www.panduit.com>)

### 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](mailto:cs@panduit.com)

##### UPS Technical Support:

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

Email: [TechSupport@panduit.com](mailto:TechSupport@panduit.com)

#### Europe / Middle East

##### Customer Service

- Price & Availability
- Expedites

0044-(0)208-6017219 or [EMEA-CustomerServices@panduit.com](mailto:EMEA-CustomerServices@panduit.com)

##### UPS Technical Support:

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

Email: [TechSupportEMEA@panduit.com](mailto: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

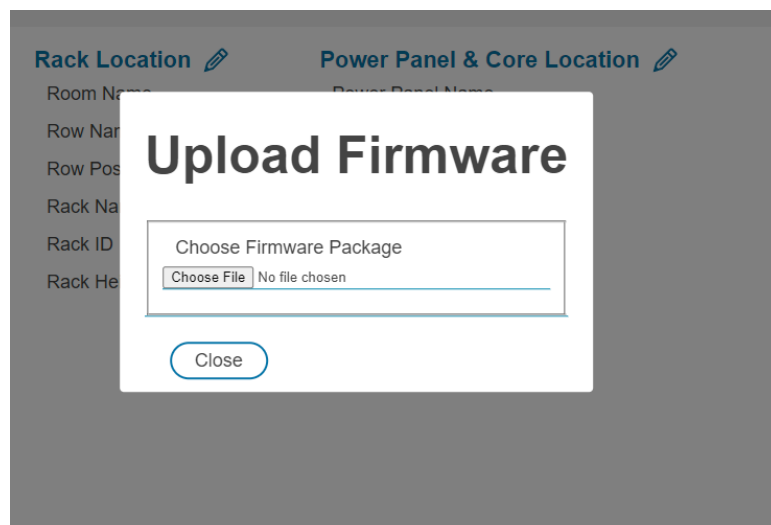
### W

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 SmartZone *mPower* tool, and the firmware can be bulk updated with the *mPower* tool

1. Open the User interface in a web browser by entering the NMC IP address.
2. Login to with Administration credentials.
3. Go to **Settings > System Management > Actions > Update Firmware**.
4. In the Firmware Update dialog box, click on 'Choose File', then browse to the firmware file.



**Figure 86: Upload Firmware**

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

## Appendix B: System Reset or Password Recovery

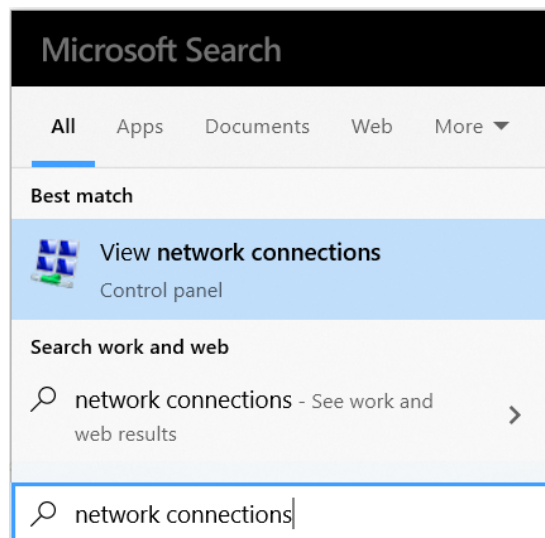
Press and hold the Reset Button for 8 seconds to recover from a NMC controller communication failure. The green LED will flash slowly indicating the controller will reset. This will cause a reset of the NMC controller, all configuration(s) will be retained.

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

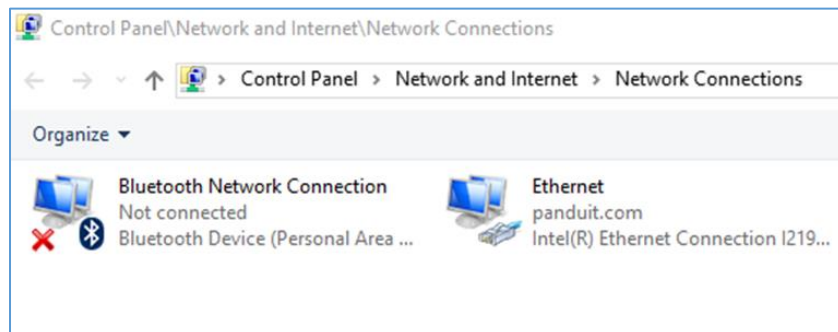
**Note:** Instructions refer specifically to Windows 10. Please refer to your operating system documentation if you are not using Windows 10.

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

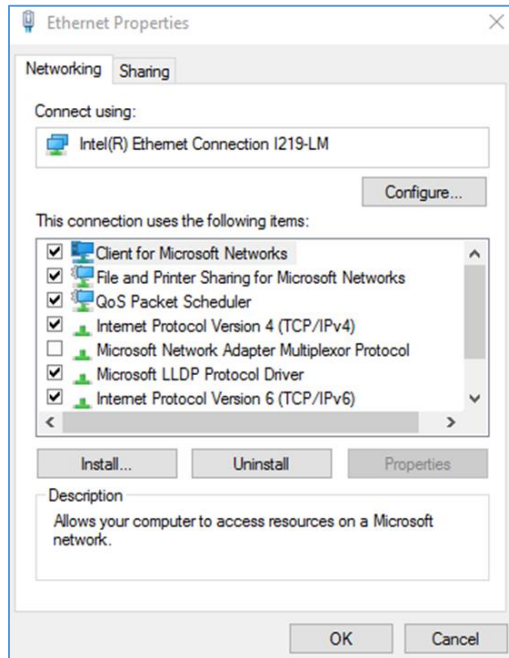


**Figure 87: View network Connections**

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

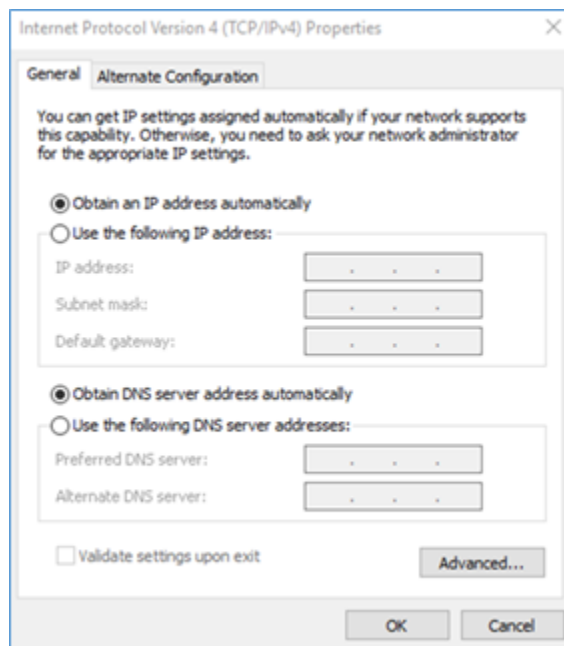


**Figure 88: Properties**



**Figure 89: Ethernet Properties**

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



**Figure 90: 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:

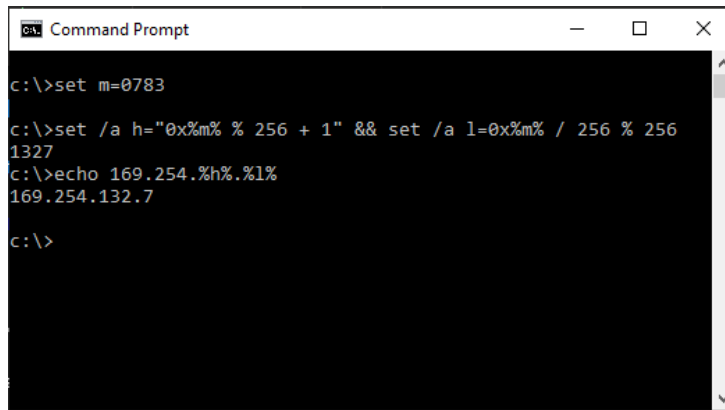
1. The MAC address of the NMC is printed on a label on the face plate of the card. Get the last two bytes of the MAC address.

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%
```





```
Command Prompt
c:\>set m=0783
c:\>set /a h="0x%m% % 256 + 1" && set /a l=0x%m% / 256 % 256
1327
c:\>echo 169.254.%h%.%l%
169.254.132.7
c:\>
```

Figure 91: 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

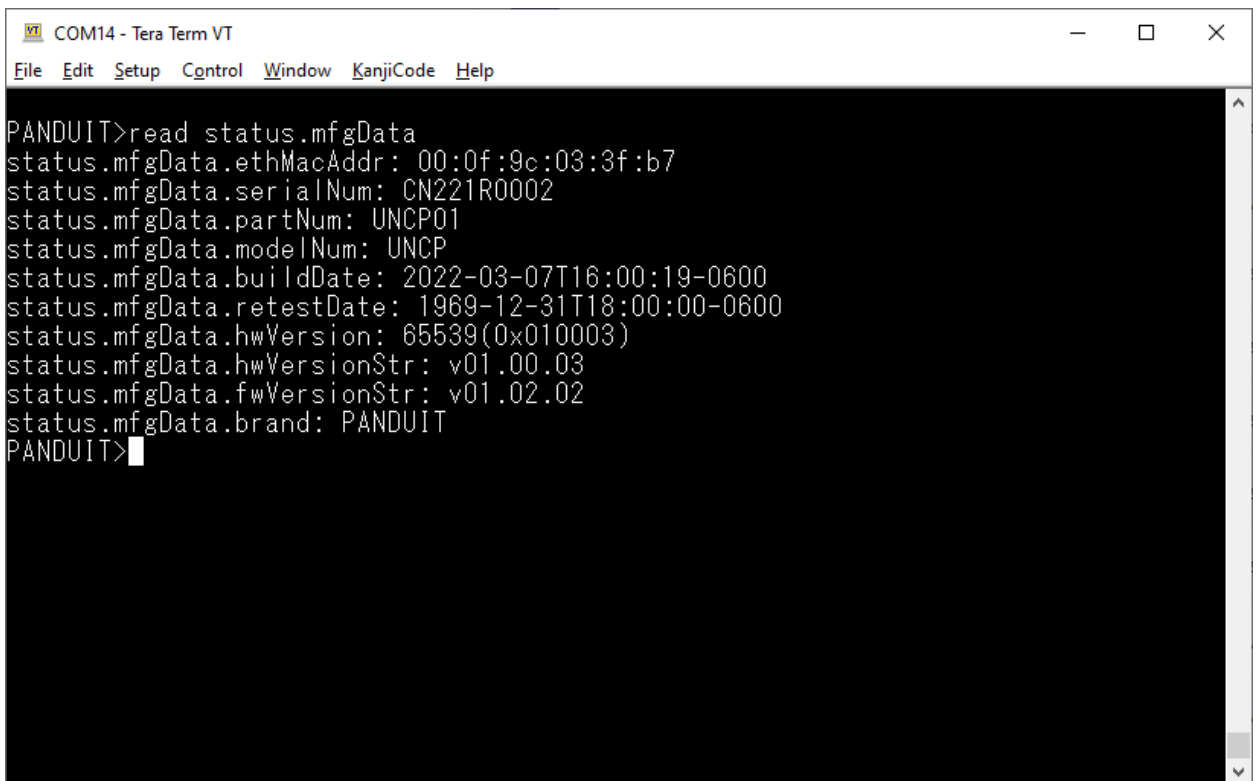
*Command list*

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

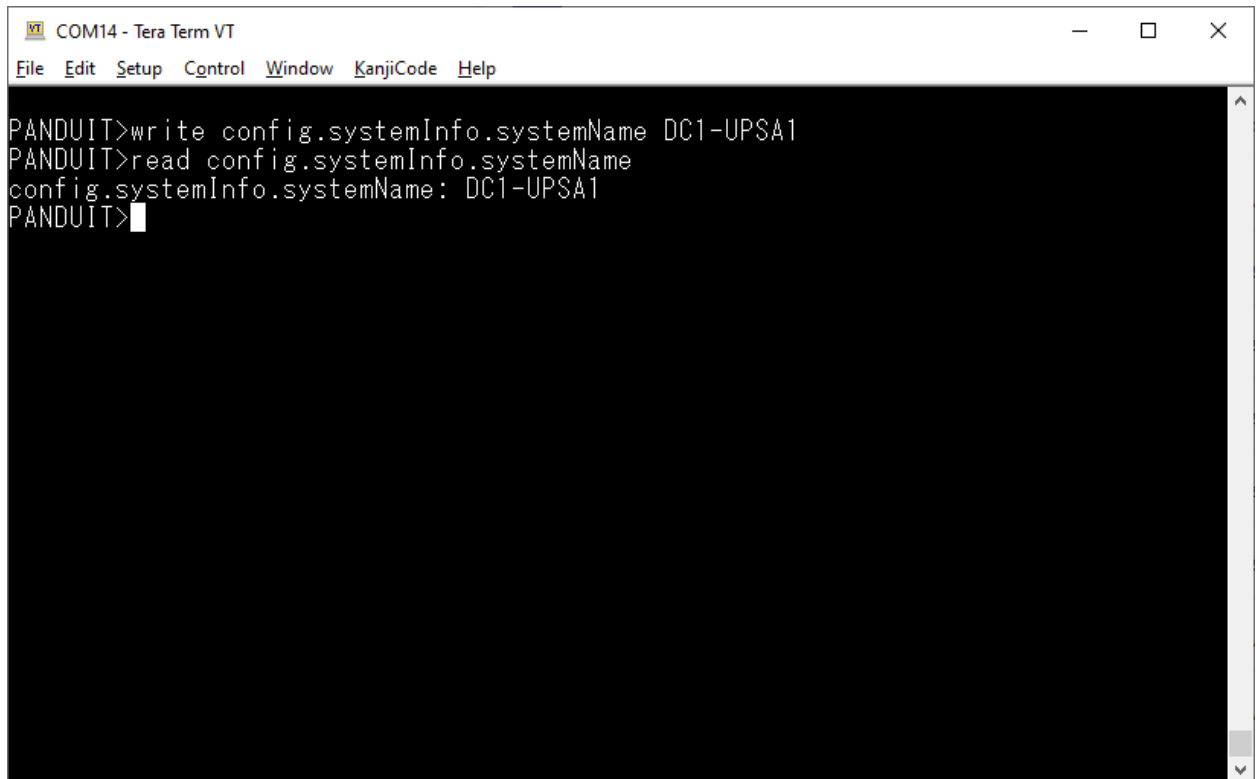


**Figure 92: Reading from CLI**

- **write**

Set a value to an individual item in the data model

Example: write config.systemInfo.systemName DC1-UPSA1



```
COM14 - Tera Term VT
File Edit Setup Control Window KanjiCode Help
PANDUIT>write config.systemInfo.systemName DC1-UPSA1
PANDUIT>read config.systemInfo.systemName
config.systemInfo.systemName: DC1-UPSA1
PANDUIT>
```

Figure 93: Writing from CLI

- **list**  
List all objects 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 an 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
```

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

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

- 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)