Panduit FMPS

User Manual

FMPS Network Management Card

Version 2.1.0

Table of Contents

Section 1 – System Overview

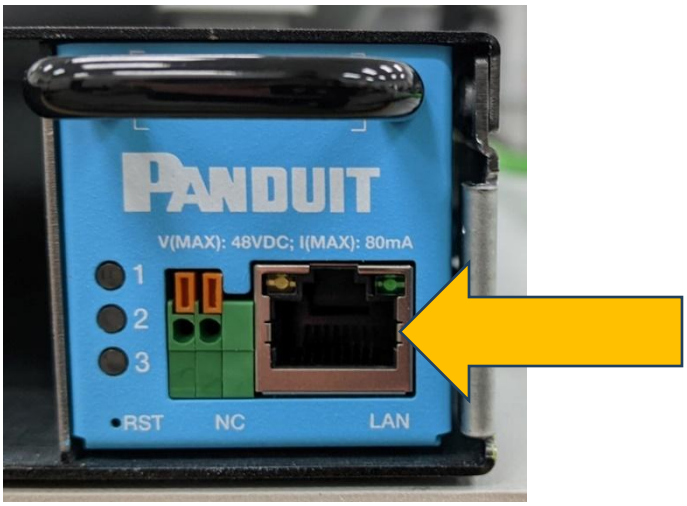
NMC Controller

This centralized piece of intelligent hardware receives an IP address, contains a Graphical Web Interface, handles the Dry Contact port, 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.
2. Connect the other end of the cable to the Network port on the switch (or another valid LAN device). A separate VLAN for this solution is recommended.

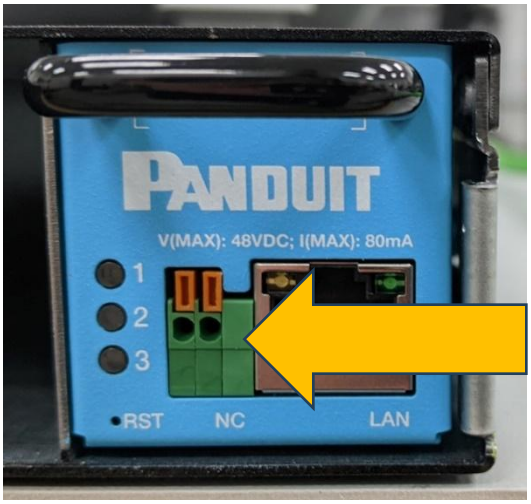


From the factory, the NMC defaults to DHCP and HTTPS connection. If the network has a DHCP server, the NMC automatically receives an IP address. If there is no DHCP server, the NMC will assign an IP (Auto IP). The Auto IP address will be a link-local IP address, and it can be obtained using the instructions in Appendix C: Direct connect to the FMPS via Ethernet without Bonjour. The NMC supports mDNS to discover the DHCP IP or the Auto IP. The mDNS address format is “fmps-<macaddress>.local”. For example, “fmps-000f9c03000b.local” is valid for a MAC address of 00:0F:9C:03:00:0B.

Connecting to the Dry Contact port

The Dry Contact port is a set of contacts that are **closed** when the FMPS system is operating without issue. The contact will **open** when the system is faulted. These

contacts are rated for 48VDC at 80mA.



Reset button

The paperclip reset button can be used in the event of a lost password or unresponsive system. See Appendix B for details on how to reset the system.

LEDs

The LEDs show the status of various states of the system. Refer to Section 4 for details.

Section 2 – Web Graphical User Interface (GUI)

Internet Protocol (IP) Addressing

After the NMC receives an IP address, log in to the Web interface to configure the NMC and assign a static IP address (if desired). NOTE: modifying the IP address will require the user to reenter the IP address in the web browser and log in.

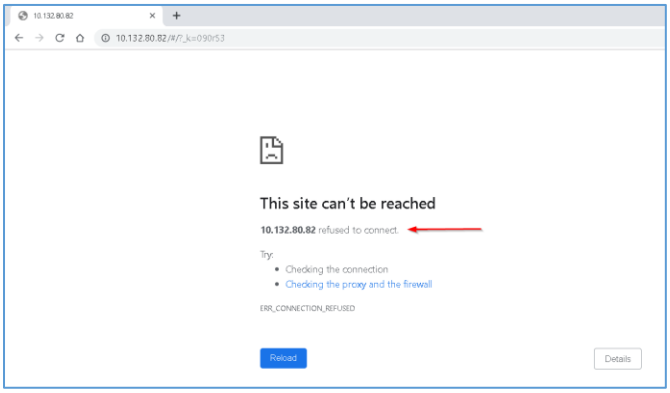
Web Connection

Supported Web Browsers

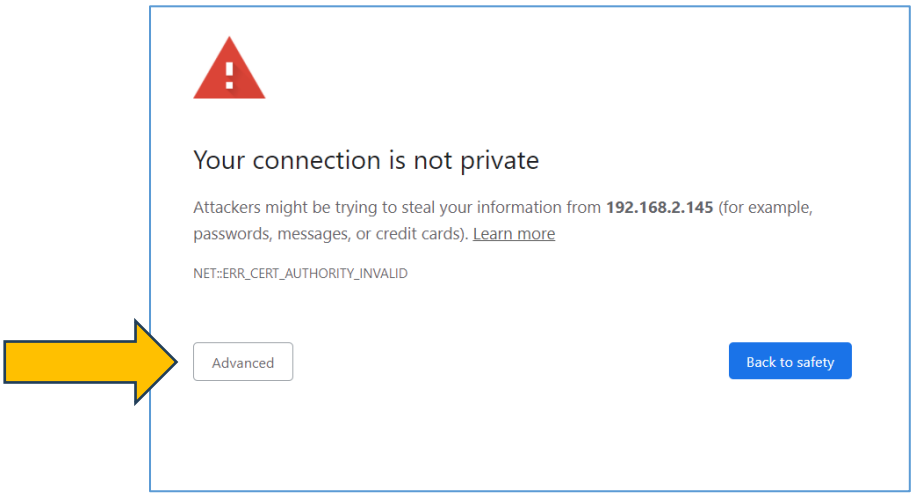
The supported Web browsers are Google Chrome (mobile and desktop), Mozilla Firefox, Microsoft Edge, and Apple Safari (mobile and desktop).

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 “https://” protocol is used, not “http://”



- 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” hyperlink.



- 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 B_Appendix_C:_System to factory reset the NMC.

Changing the Password

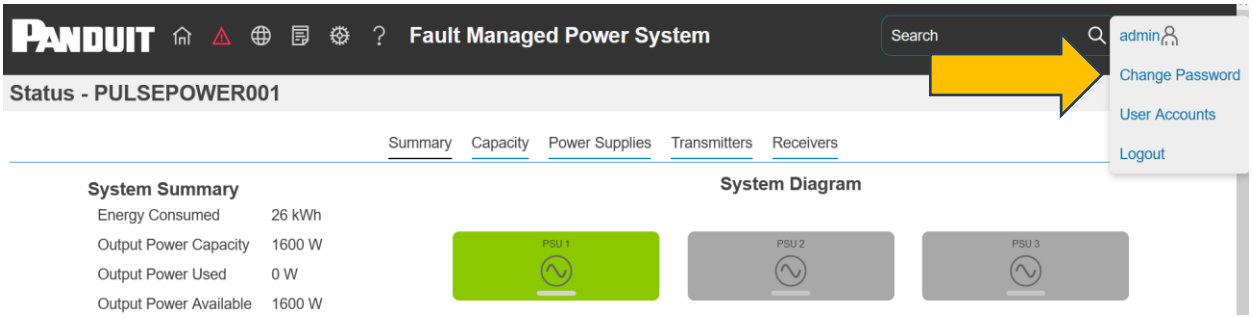
At initial login, it is required to change the default password.

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

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

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

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

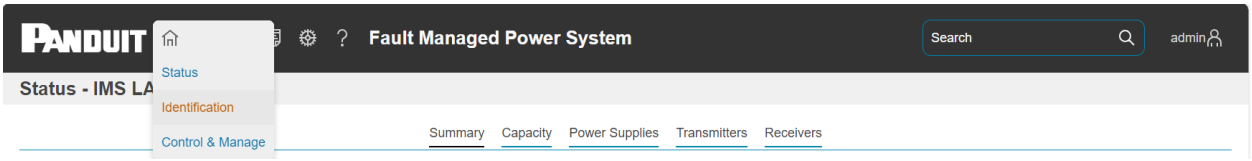


2. The **Change Password** window opens. See this section beginning for details on how to change the password.

Introduction to the Web GUI

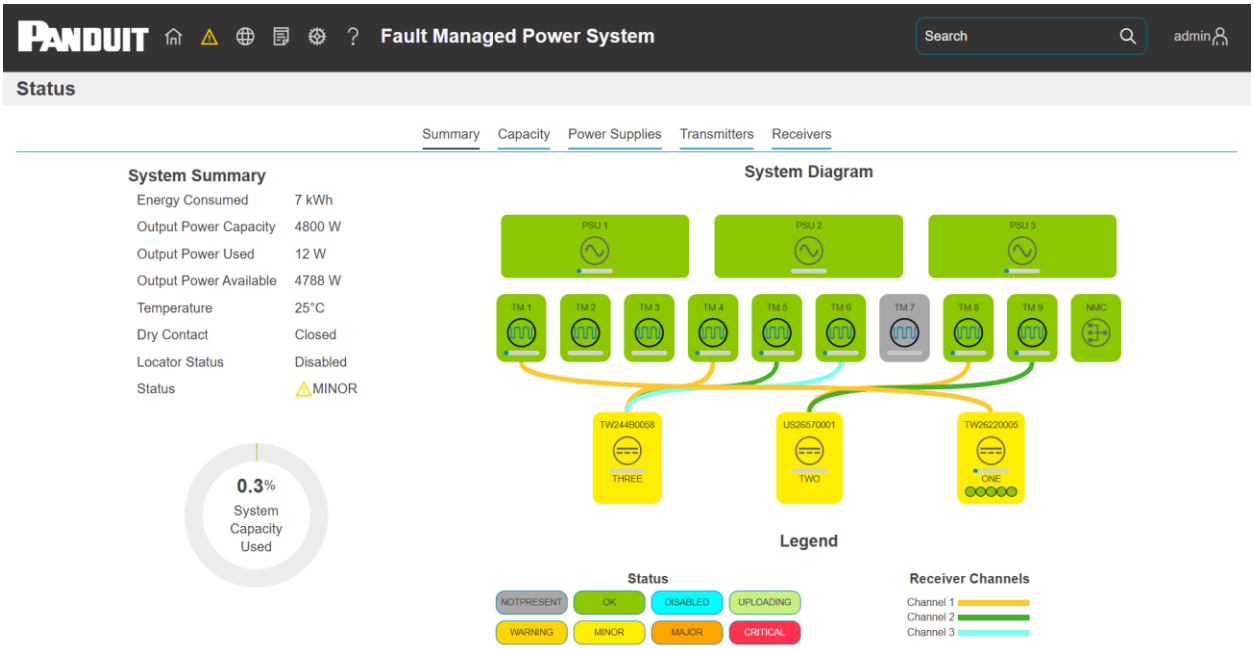
Home

The Home dropdown menu includes Status, Identification, and Control & Manage options.



Status

The Status screen shows the overall health of the Panduit FMPS Modules along with tabs providing detailed information.



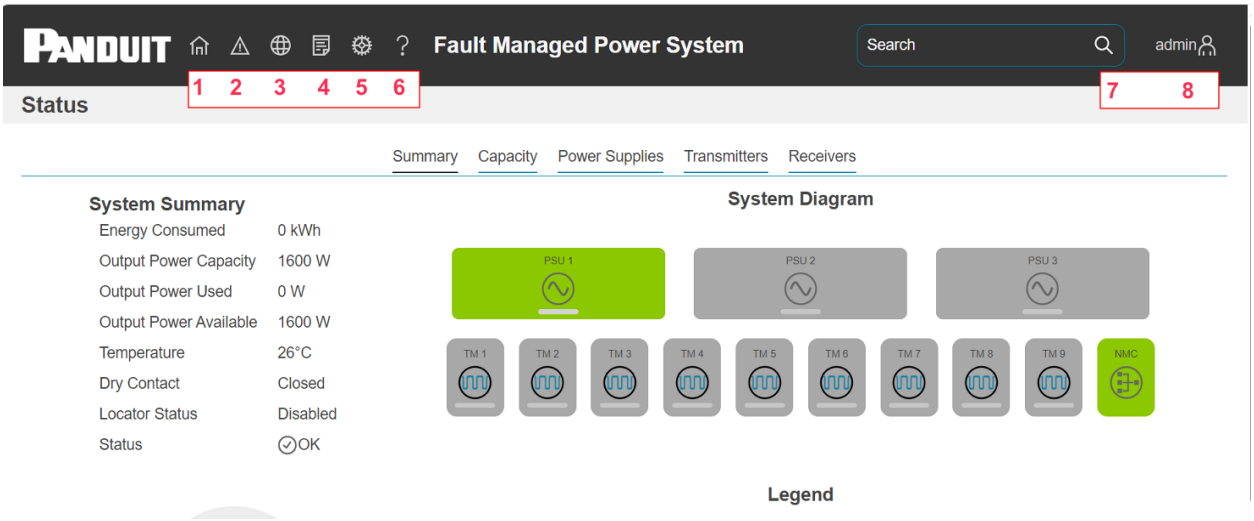
At the top of the screen for the Summary tab, the left pane provides a quick-glance summary of the overall system health, power statistics, and available capacity. Each box represents a module in the system. Consult the color legend on the center-bottom of this screen for information on the colors. This section also provides summary information for:

- Energy Consumed
- Output Power Capacity
- Output Power Used
- Output Power Available
- Temperature
- Dry Contact
- Locator Status
- Status

The Status screen also contains data tabs with details for System Capacity, Power

Supply Modules, Transmitter Modules, and Receivers.

Landing Page/Dashboard



Number	Icon	Description
1		The home icon provides the user with access to an overview of the FMPS via the Status page, an Identification Details page, and Control & Manage functions page.
2		The Alarm icon provides details of the active alarms.
3		This icon allows Language selection. Available languages: English, French, German, and Spanish.
4		This icon provides the logs of the FMPS, which can be viewed and downloaded.
5		The settings icon allows a user to configure items such as the System Management, the Network, SNMP , Email Setup, Syslog, User Accounts and Date & Time.
6		Information about the FMPS can be found using this icon. Users can also click user guide and license for additional information about the system.
7		The search icon allows users to input key words and search for the related results.
8		This icon shows who is logged in (user or admin). Account passwords can be changed, and user accounts managed through this page.

Menu Dropdowns

Overview
- Status
- Identification
- Control & Manage

Alarms
- Active Alarms

Language
- English
- Françcais
- Deutsch
- Español

Logs
- Event Log
- Data Log

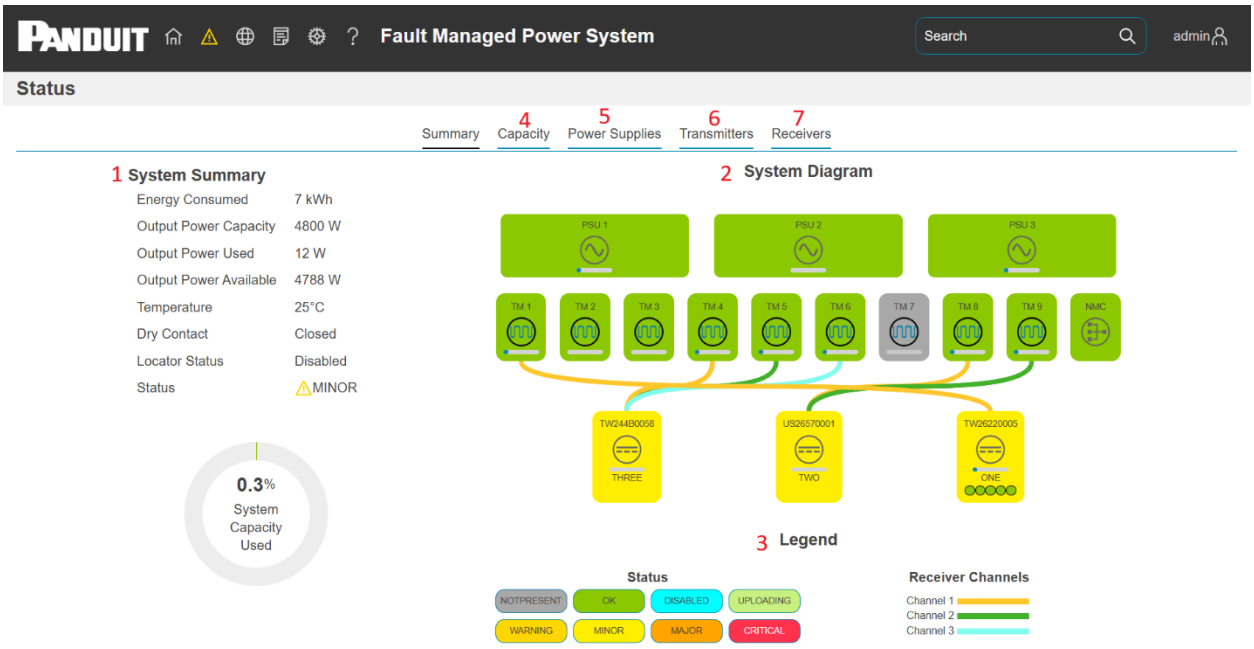
Setting
- System Management
- Device Firmware Update
- Network
- Date & Time
- User Accounts
- SNMP
- Syslog
- Email

Help
- Support

User
- admin
- Change Password
- User Accounts
- Logout

Introduction to the Dashboard

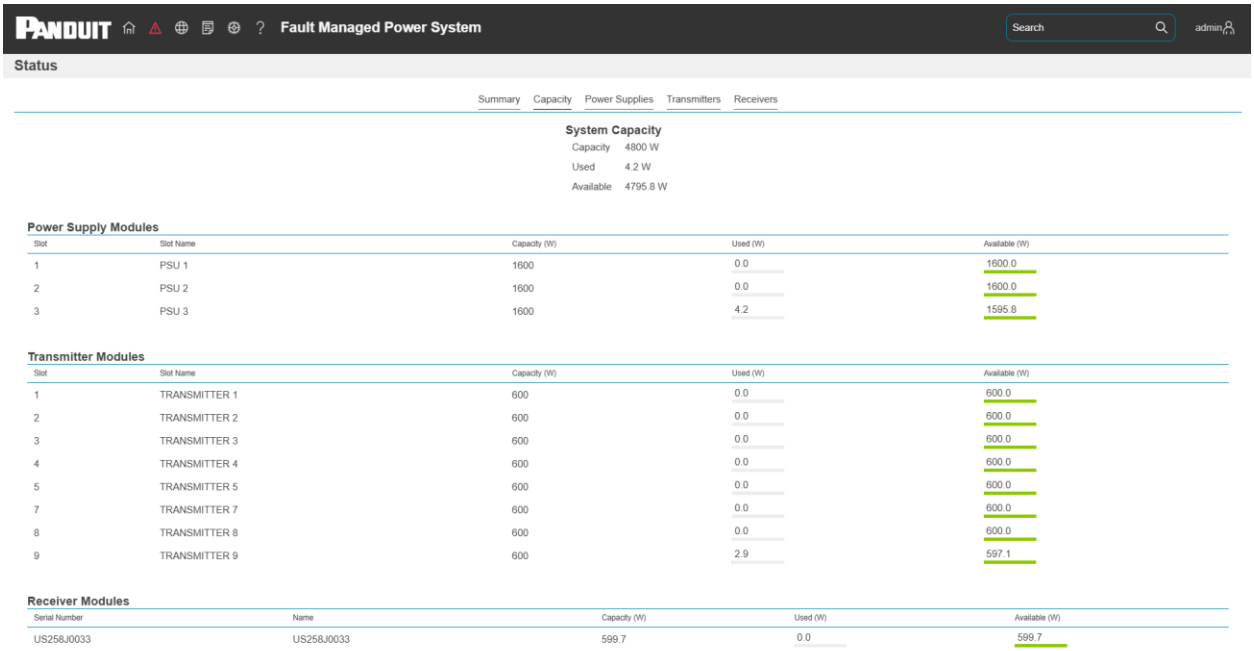
Power Summary Page



NUMBER	DESCRIPTION
1	The System Summary section of the page provides a high-level overview of the system including energy consumption,

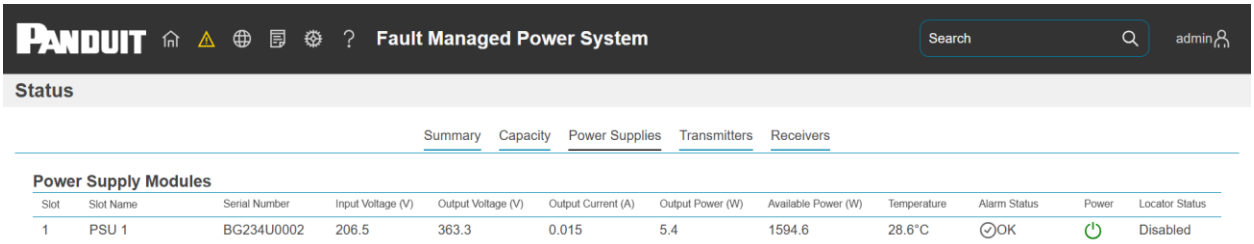
	capacity, temperature, overall system status, and other summary details.
2	The System Diagram section of the dashboard shows the state of the Power Supplies, Transmitters, Receivers, and NMC for this system.
3	The Legend shown what each status color means and which colored line is associated with which channel to the Receiver.
4	The Capacity Tab brings up the capacity page that has detailed capacity information on system elements.
5	Clicking on the Power Supplies tab brings up a detailed view of the power supplies.
6	Clicking the Transmitter tab brings up a detailed view of the Transmitters of the system and how they are performing.
7	Clicking the Receivers tab brings up a detailed view of the Receivers of the system and how they are performing.

FMPS Capacity Page



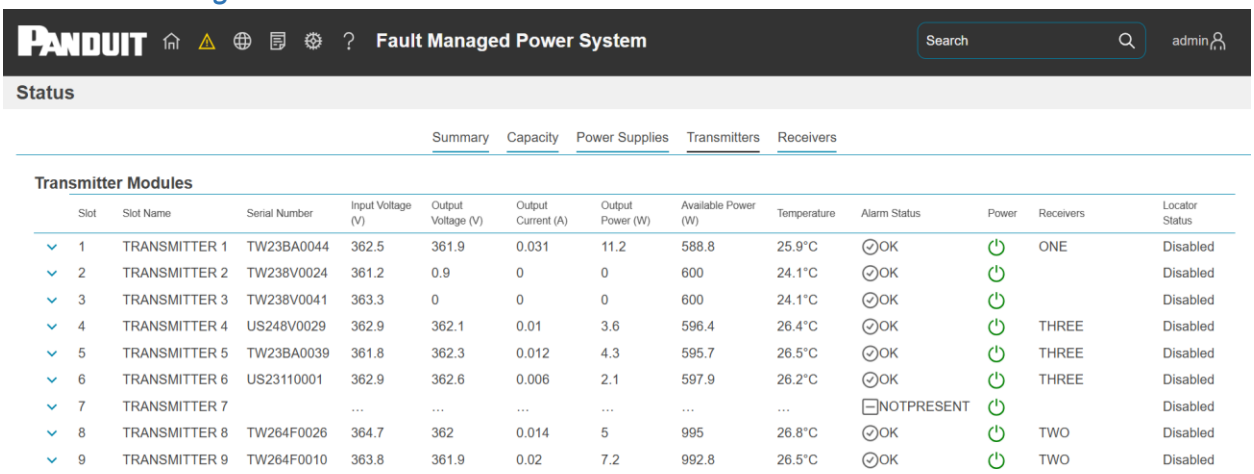
This page shows the system power capacity (total available), how much of this capacity is being used, and available power for edge devices (in watts). It also provides power details on each part of the system which includes Power Supplies, Transmitters, and Receivers.

Power Supplies Page



This page provides several additional details that are not shown on the capacity page such as alarm status of the power supply modules, internal temperature, serial number, power status, input and output voltage, and output amps.

Transmitter Page

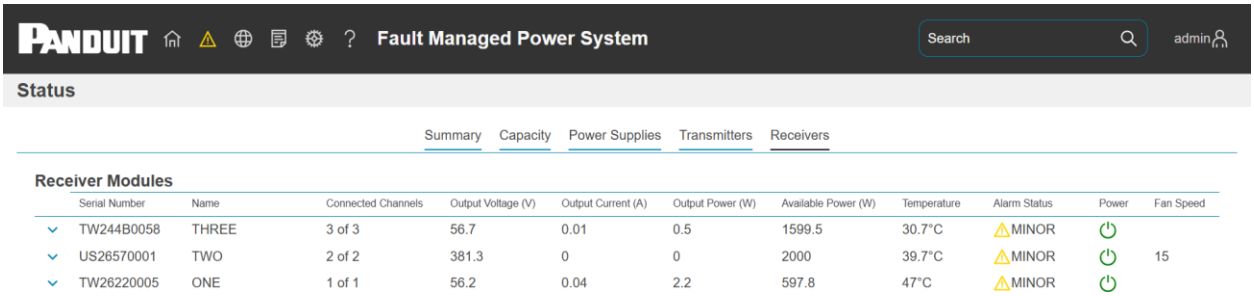


	Slot	Slot Name	Serial Number	Input Voltage (V)	Output Voltage (V)	Output Current (A)	Output Power (W)	Available Power (W)	Temperature	Alarm Status	Power	Receivers	Locator Status
⌄	1	TRANSMITTER 1	TW23BA0044	362.5	361.9	0.031	11.2	588.8	25.9°C	OK		ONE	Disabled
⌄	2	TRANSMITTER 2	TW238V0024	361.2	0.9	0	0	600	24.1°C	OK			Disabled
⌄	3	TRANSMITTER 3	TW238V0041	363.3	0	0	0	600	24.1°C	OK			Disabled
⌄	4	TRANSMITTER 4	US248V0029	362.9	362.1	0.01	3.6	596.4	26.4°C	OK		THREE	Disabled
⌄	5	TRANSMITTER 5	TW23BA0039	361.8	362.3	0.012	4.3	595.7	26.5°C	OK		THREE	Disabled
⌄	6	TRANSMITTER 6	US23110001	362.9	362.6	0.006	2.1	597.9	26.2°C	OK		THREE	Disabled
⌄	7	TRANSMITTER 7		...	...	...	...	...	...	NOTPRESENT			Disabled
⌄	8	TRANSMITTER 8	TW264F0026	364.7	362	0.014	5	995	26.8°C	OK		TWO	Disabled
⌄	9	TRANSMITTER 9	TW264F0010	363.8	361.9	0.02	7.2	992.8	26.5°C	OK		TWO	Disabled

This page provides details on each Transmitter module such as serial number, input voltage, output voltage, output current, output power (watts), available power (watts), internal temperature, alarm status, power status, connected Receiver id, and locator status.

Alarm status options are OK (no alarms) and NOTPRESENT (no Transmitter detected). Power status will be either enabled or disabled and can be changed on the control page. Locator status can be activated on the control page and will blink the Transmitter light blue and green.

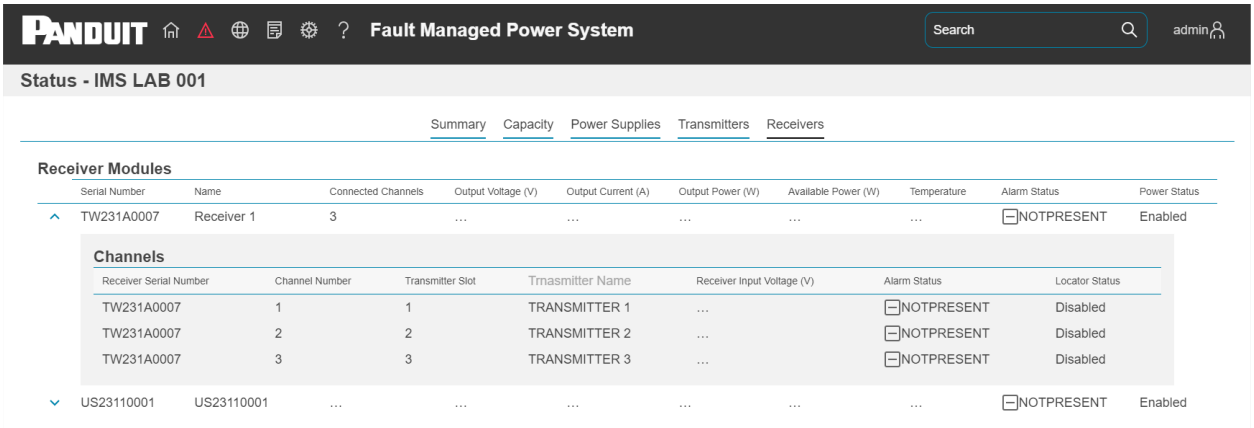
Receiver Page



This page shows details about each Receiver connected to the system. This includes serial number, Name (user configurable on the Control and Manage > Pencil page), connected channels, output voltage, output current, output power (watts), internal temperature, alarm status, power status, and fan speed.

Alarm status options are OK (no alarms) and NOTPRESENT. The power status will normally show as enabled but can be disabled via the control page for maintenance work. A disabled Receiver will not deliver output power to the load.

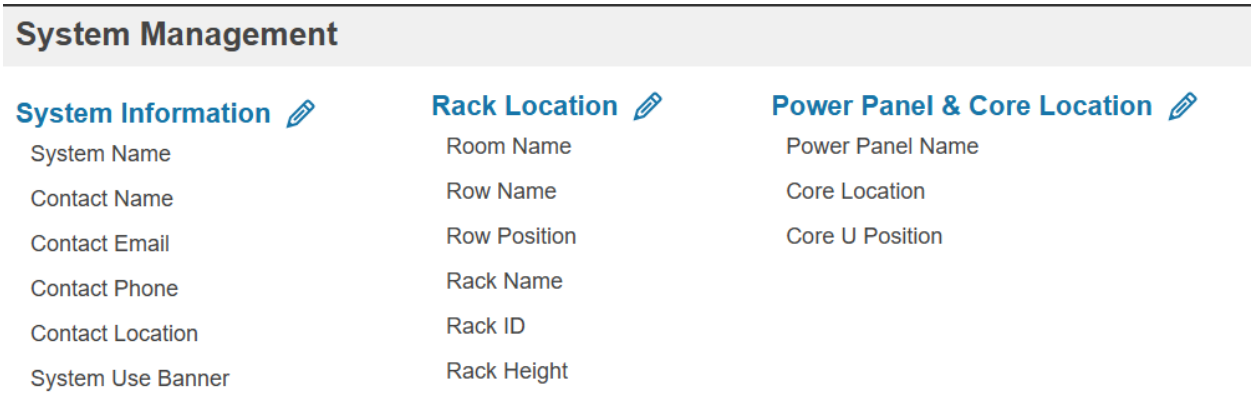
- To view detailed channel information for each Receiver, click the down chevron (v) in the leftmost column and the following will be displayed:



System Management Information

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

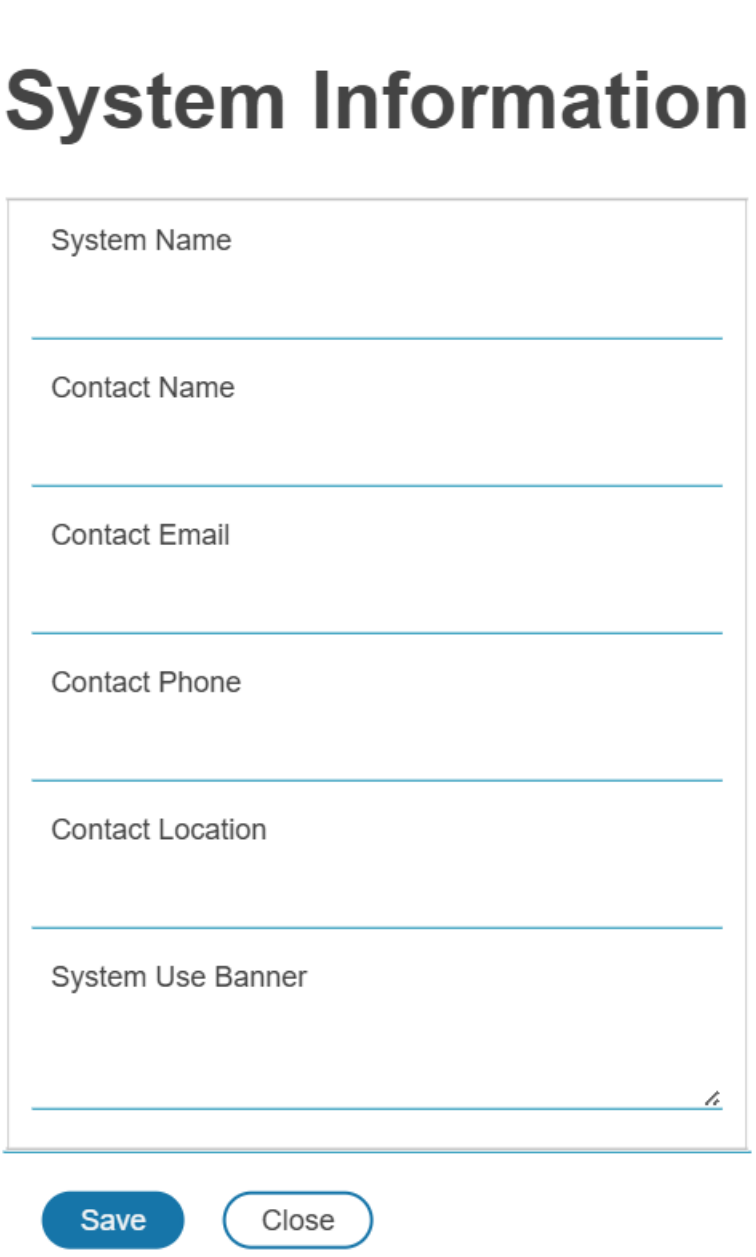
To configure the system management information, select **System Management** under the **gear** icon.



System Info

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



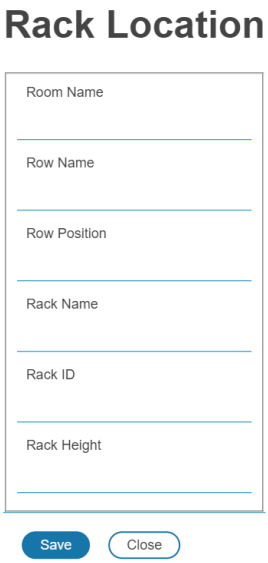
2. Enter the **System Name**
3. Enter the name of the person who should be contacted if there is a problem with the system into the **Contact Name** section.
4. Enter the email of the contact person into the **Contact Email**.
5. Enter the phone number of the contact person into **Contact Phone**.
6. Enter the location of the contact person into the **Contact Location**.
7. Enter a **System Use Banner** if desired.

8. Press **Save**.

Rack Location

The rack location describes the physical location of the rack or cabinet where the FMPS system resides. To set up the system information, follow these steps.

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

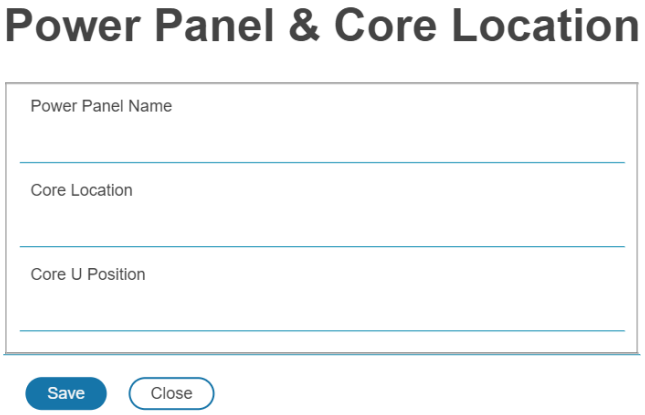


2. Enter the room location of the rack or cabinet that contains the NMC system into **Room Name.**
3. Enter the **Row Name** where the NMC is located.
4. Enter the position of the row where the NMC is positioned in **Row Position**.
5. Enter the ID of the rack/cabinet where the NMC is located into **Rack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

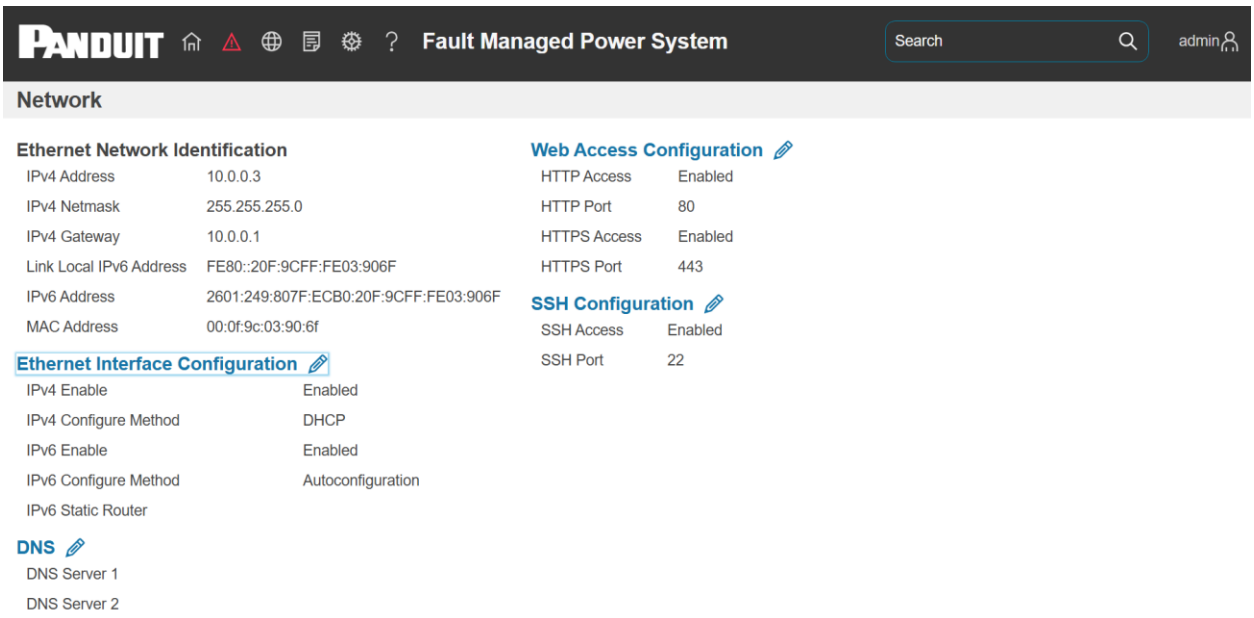
1. Select the **pencil** icon next to **Power Panel & Core Location**.



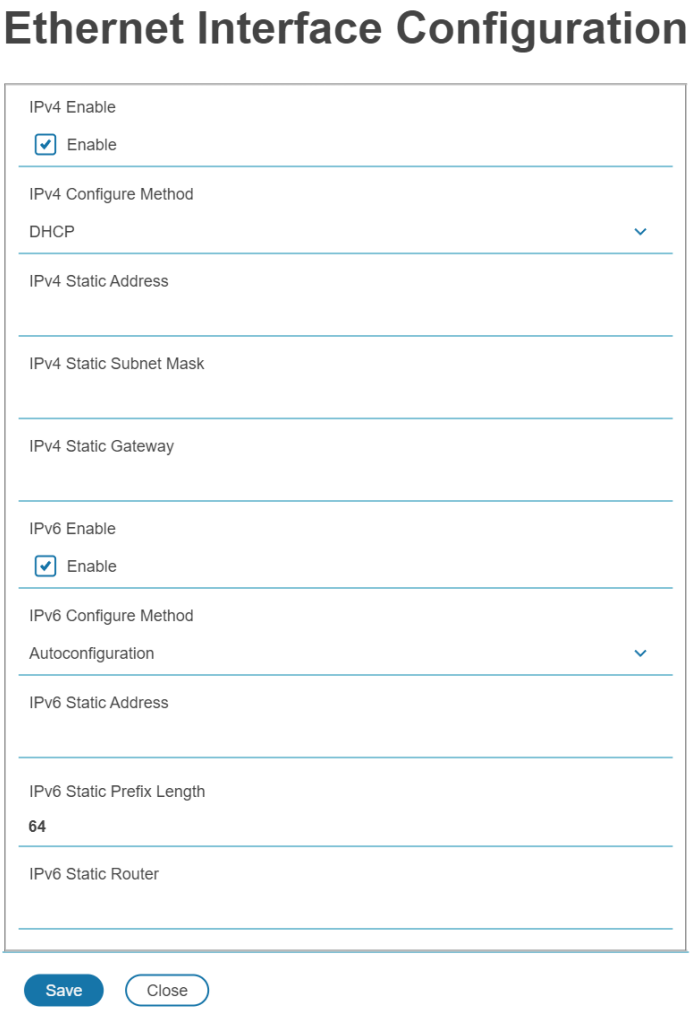
2. Enter the name of the NMC in the **Power Panel Name**.
3. Select **Front** or **Back** for the **Core Location.** The **Core Location** is the side of the rack/cabinet where the NMCs are installed.
4. Enter the rack unit (RU) location into the **Core U Position**.
5. Press **Save**.

Network Settings

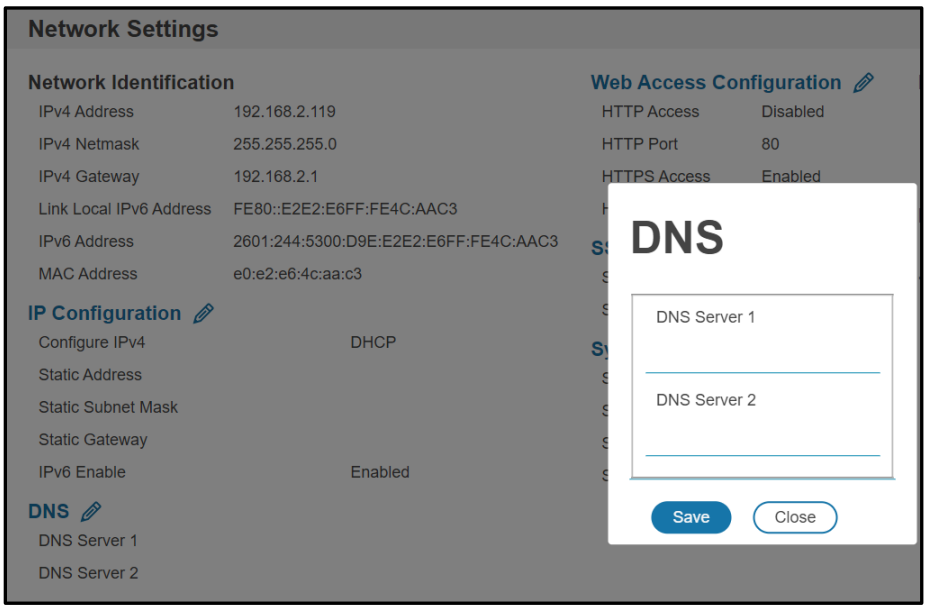
The Network Settings allow management of IP Configuration, DNS, Web Access, SSH Configuration.



Ethernet Interface Configuration:

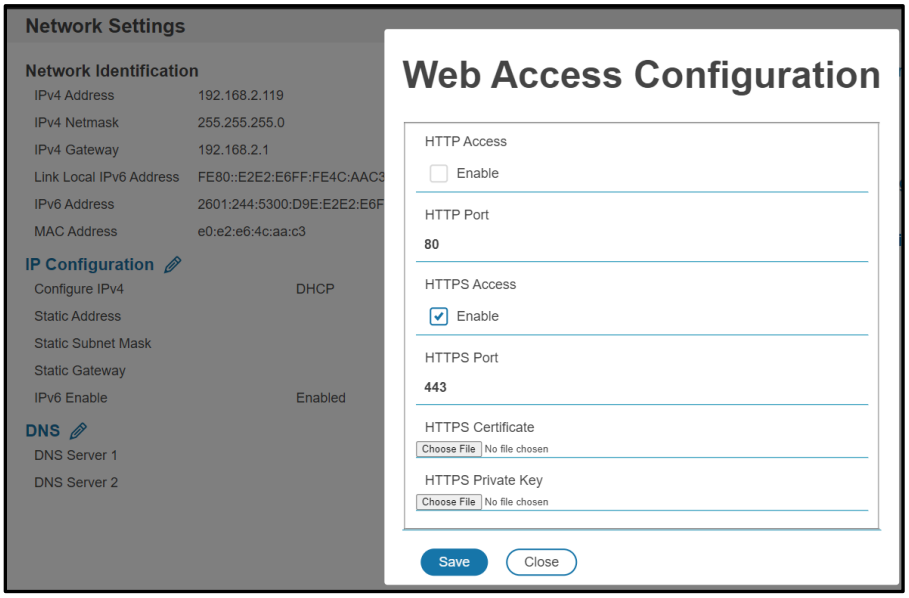


DNS configuration:

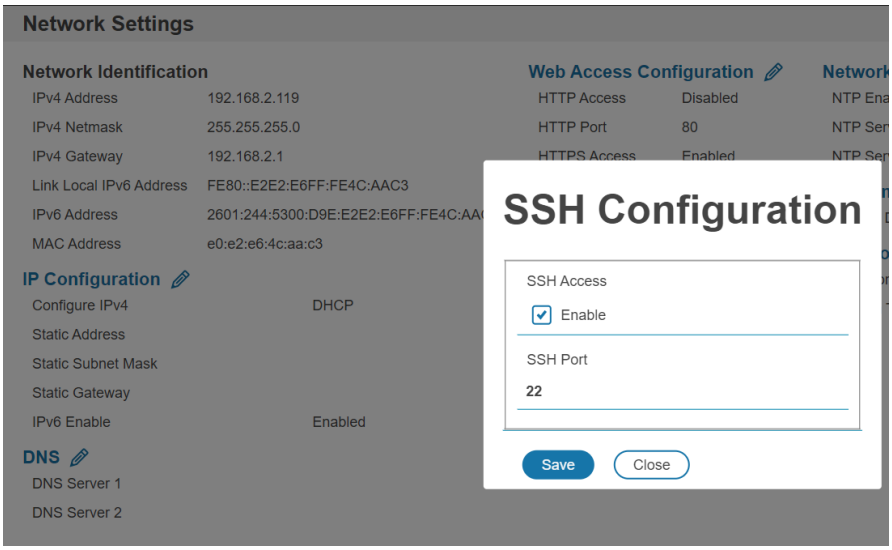


Web Access Configuration

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



SSH Configuration:

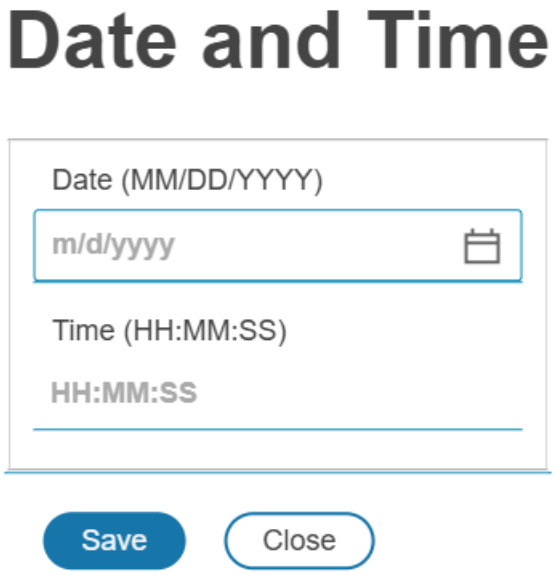


Setting Time and Date on the NMC

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

Manually Setting Time and Date

1. Go to **Date & Time Settings** and select **Date and Time**.



2. Enter the date using the MM/DD/YYYY format or use the calendar icon to select a date.

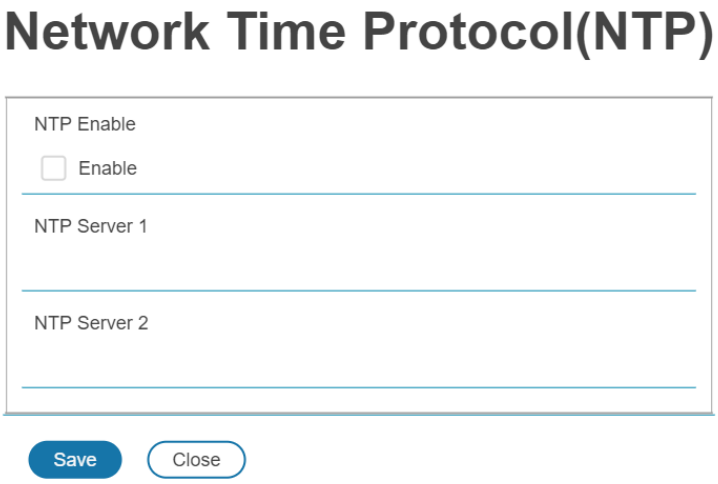
3. Enter the time in the three fields provided: the hour in the first field, minutes in the

next field, and seconds in the third field. Time is displayed in 24-hour format. Enter 2 for 2:00am, 14 for 2:00pm, etc.

4. Press **Save**.

Configure Network Time Protocol (NTP)

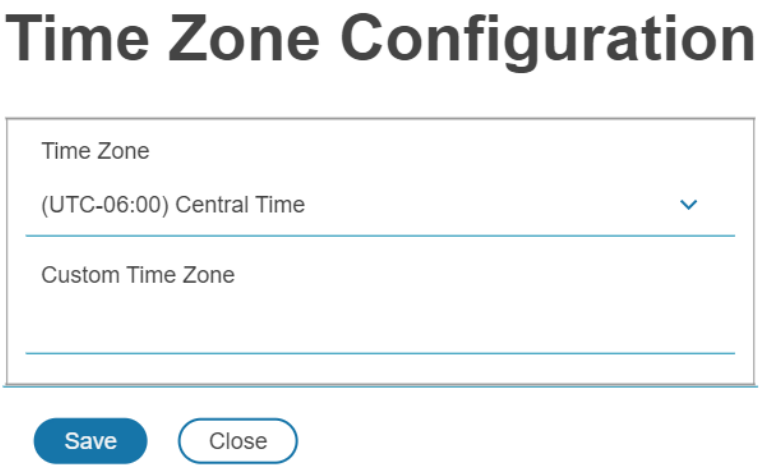
1. Go to **Data & Time Settings** and select **Network Time Protocol** (NTP).



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

Time Zone Configuration

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

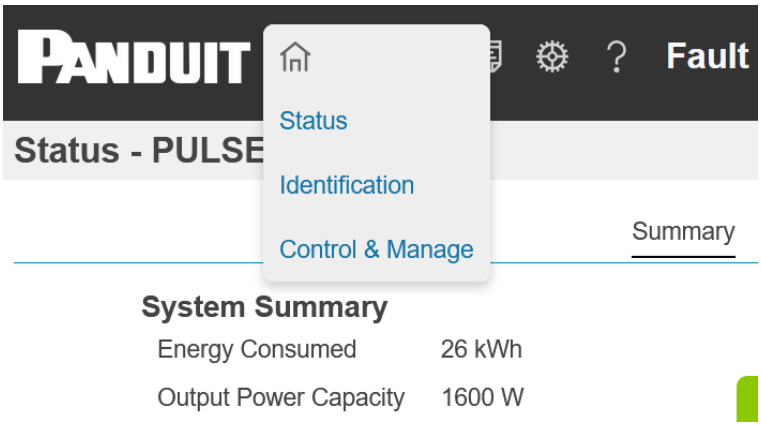


2. Select a predefined time zone from the pull-down menu.
3. If the desired time zone is not in pull down menu, enter the POSIX time zone in the **Custom Time Zone**:
   - The POSIX format is local_timezone,date/time,date/time.
   - For more information on the POSIX time zone formats see Appendix F: POSIX Time Zone Information.

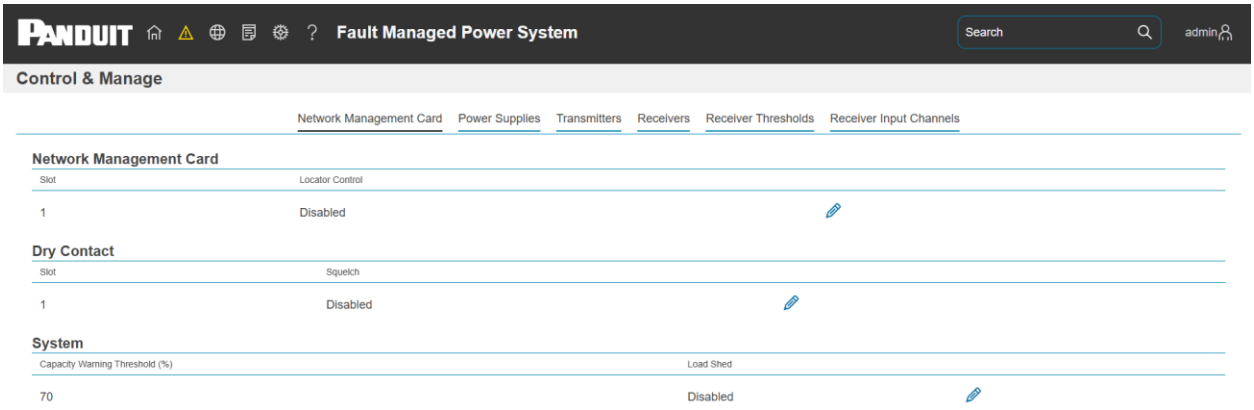
Control & Manage

The Control & Manage section of the Web GUI will allow a user to control the functionality of the system. These areas include the NMC, Power Supply, Transmitter output, Receiver Output, and Receiver Channels.

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



Control & Manage: Network Management Card



The Control & Manage Page has six tabs that can be selected:

*Network Management Cards

*Power Supplies

*Transmitters

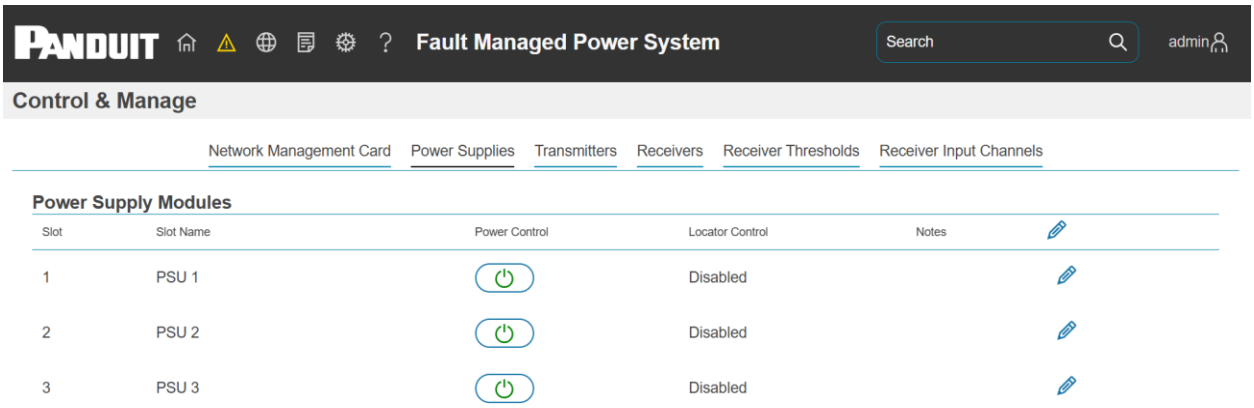
*Receivers

*Receiver Thresholds

*Receiver Input Channels

The "**Network Management Card" tab** allows users to activate the locator function on the NMC (blinking the LED blue and green), allow or ignore the Dry Contacts, set the System Capacity Warning Threshold (%), and enable the Load Shed feature. Click the pencil icon to modify settings and select Save or Close when done.

Control & Manage: Power Supplies

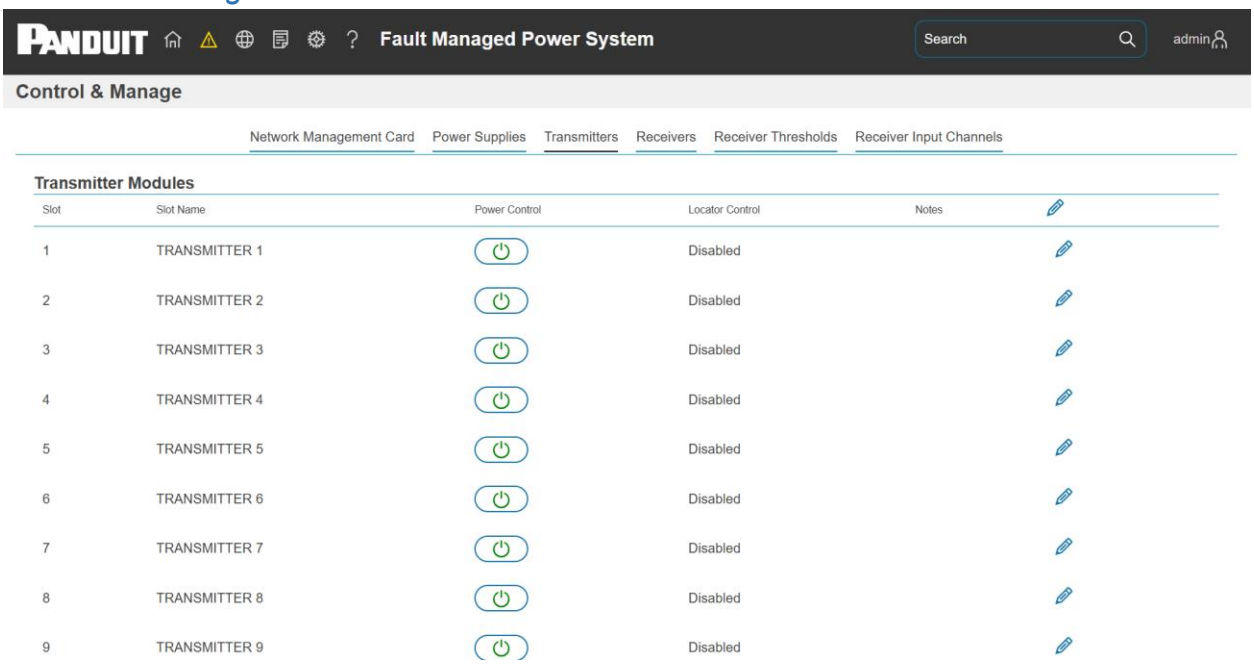


The **"Power Supplies" tab** allows users to provide a unique name to each Supply, enable or disable the Supply, enable the locator control function, and include a custom note about the Supply.

Enable and disabling the Supply is a maintenance function and is typically done when troubleshooting.

The locator control feature will blink the rear LED on the Supply blue and green, making this Supply stand out from others installed. Select the pencil icon to edit the setting(s) then click on Save or Close when completed.

Control & Manage: Transmitters



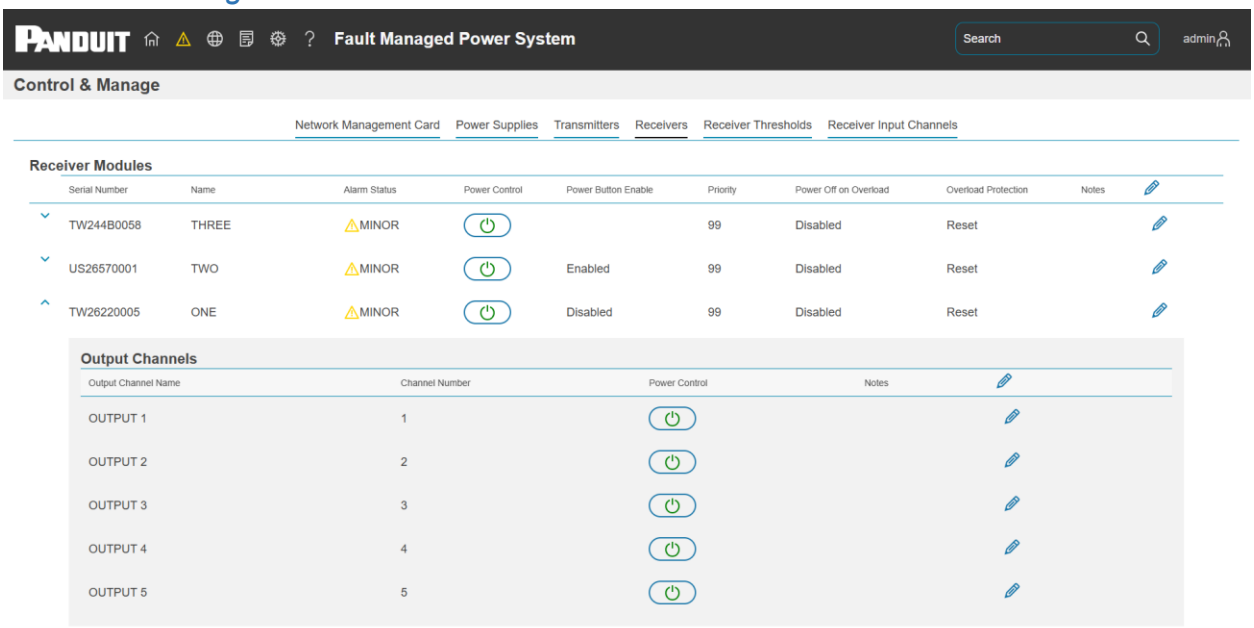
The **"Transmitters" tab** allows users to customize the Transmitters name,

enable/disable the Transmitter, activate the locator control feature, and provide a detailed note about the Transmitter. It is a best practice to disable a Transmitter before performing work on the cabling system connected to it.

The locator control function can be used to flash the LED on the Transmitter blue and green to make it stand out from its neighbors.

The custom notes field is provided to allow users to document the devices fed by this particular Transmitter.

Control & Manage: Receivers



The **"Receivers" tab** of the Control & Manage page allows the user to modify the name of the Receiver, enable or disable output power, enable or disable the on-device power button if supported, assign priority, enable or disable power off on Overload, reset tripped receivers due to Overload Protection, and record a custom note regarding this Receiver. If a receiver supports individually configurable output channels, the drop down arrow will reveal the channels and allow modifying the name of the output channel, enabling or disabling output power, and recording a custom note. Best practice is to record the device(s) being powered by the Receiver and the typical load of these device(s).

Priority

The **Priority** of the Receiver is the priority of which the Receiver will turned off if Load Shedding is turned on.

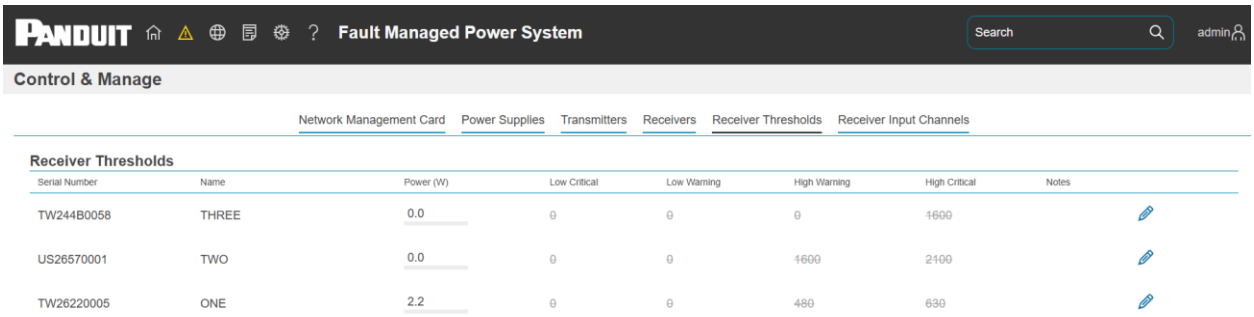
Power Off on Overload

If **Power Off on Overload** is enabled, the Receiver will automatically power off if the power crosses the **High Critical** setting.

Overload Protection

The **Overload Protection** will show if the Receiver has been autonomously powered off due to either an overload condition after having crossed the configured critical threshold or a load shed condition if the feature is enabled during a system level overload. To clear the “tripped” status back to the default value of “reset”, select the pencil and un-select the **Tripped box.**

Control & Manage: Receiver Thresholds



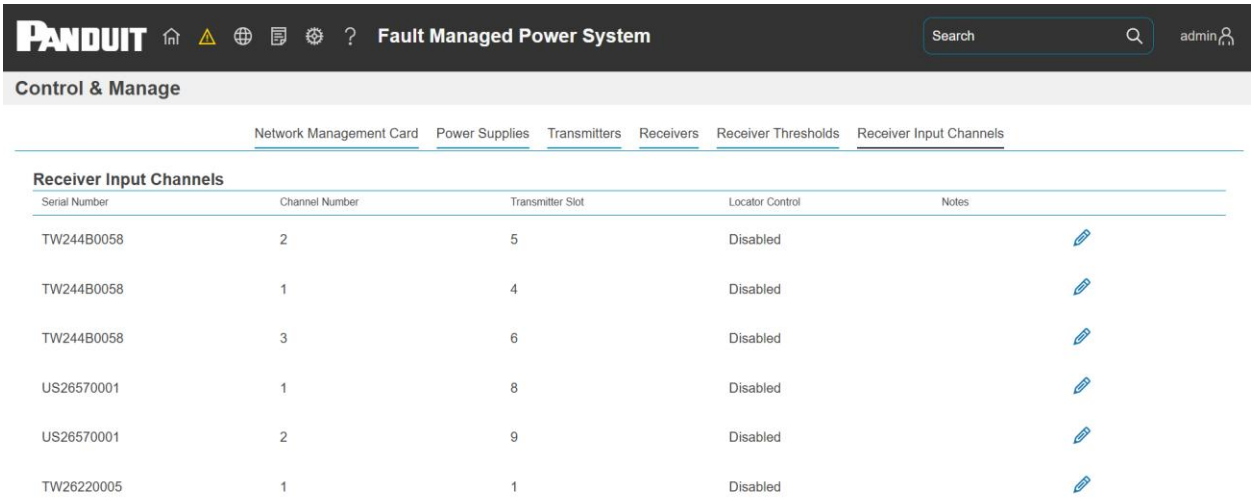
The **"Receiver Thresholds" tab** of the Control & Manage page allows the user to modify the values for different threshold severities and enable or disable the alarming related to them.

Threshold Settings

- **Low Critical / High Critical** These settings trigger a critical-level alarm when the Receiver's power falls below the Low Critical value or exceeds the High Critical value. If high critical threshold is surpassed and Power Off on Overload is enabled, the receiver will stop outputting power and need to be un-tripped.

- **Low Warning / High Warning** These settings trigger a warning-level alarm when the Receiver's power falls below the Low Warning value or exceeds the High Warning value.

Control & Manage: Receiver Input Channels

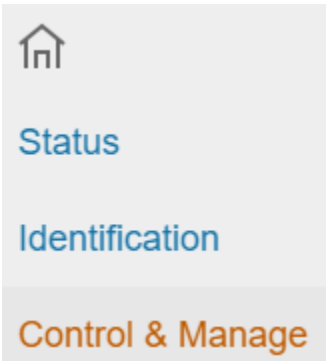


The **"Receiver Input Channels" tab** of the Control & Manage page allows the user to activate the Locator control feature for each channel and record a custom note about each channel.

Load Shedding configuration

Before enabling Load Shedding, all the Receivers need to be assigned a priority. By default, all Receivers have the same priority of 99. To assign the Receiver priorities:

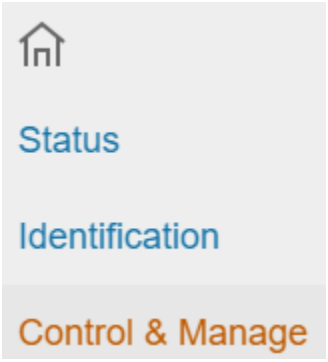
1. Select the Home icon and select **Control & Manage**



2. Go to the **Receivers** tab.
3. Assign all the **Receivers** a priority. The **Receiver** with the lowest number will be disabled first.

After all the Receivers are assigned a priority, enable the Load Shedding feature.

1. Select the Home icon and select **Control & Manage**



2. Go to the **Network Management Card** tab.
3. Click on the pencil under **System** and enable **Load Shed**.

Acknowledging Load Shedding

1. In the case **load shed** disables a Receiver, **Overload Protection** for that Receiver will change to “tripped” on the **Control & Manage** page and an alarm will be generated.
2. Power will not be output until either the **Overload Protection** box is un-selected or Power Output is turned off and then on.

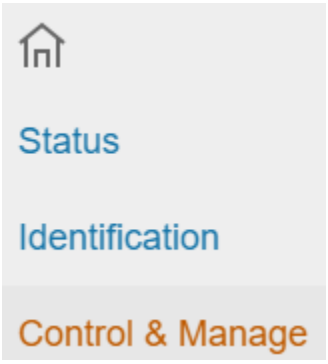
Power off on Overload

To protect a Receiver from using too much power, a user can enable **Power off on Overload**. When a Receiver crosses its configured critical threshold, the system will shut it down.

Power off on Overload configuration

To configure **Power off on Overload**.

1. Select the Home icon and select Control & Manage



2. Go to the **Receivers** tab.

3. Select the Receiver to enable the feature by clicking the pencil.
4. Configure the **High Critical** threshold to the value to disable the receiver.
5. Enable **Power Off on Overload**
6. Select **Save**.

Acknowledging Power Off On Overload

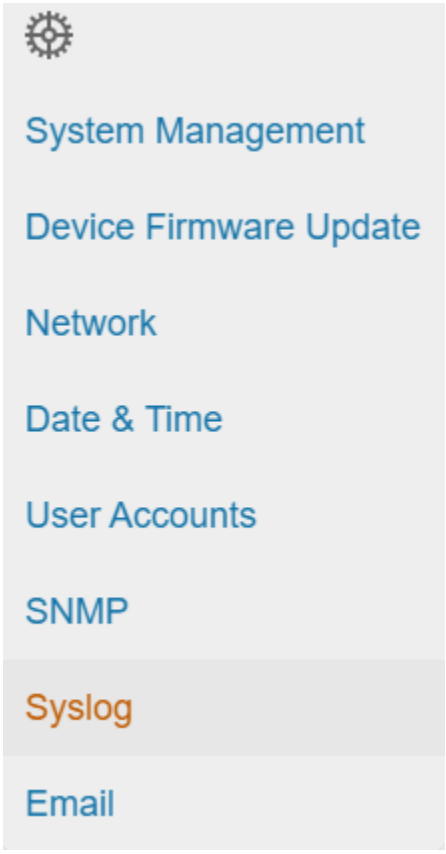
1. In the case **Power Off on Overload** disables a receiver, **Overload Protection** for that Receiver will change to “tripped” on the **Control & Manage** page and an alarm will be generated.
2. Power will not be output until either the **Overload Protection** box is un-selected or **Power Output** is turned off and then on.

Syslog Setup

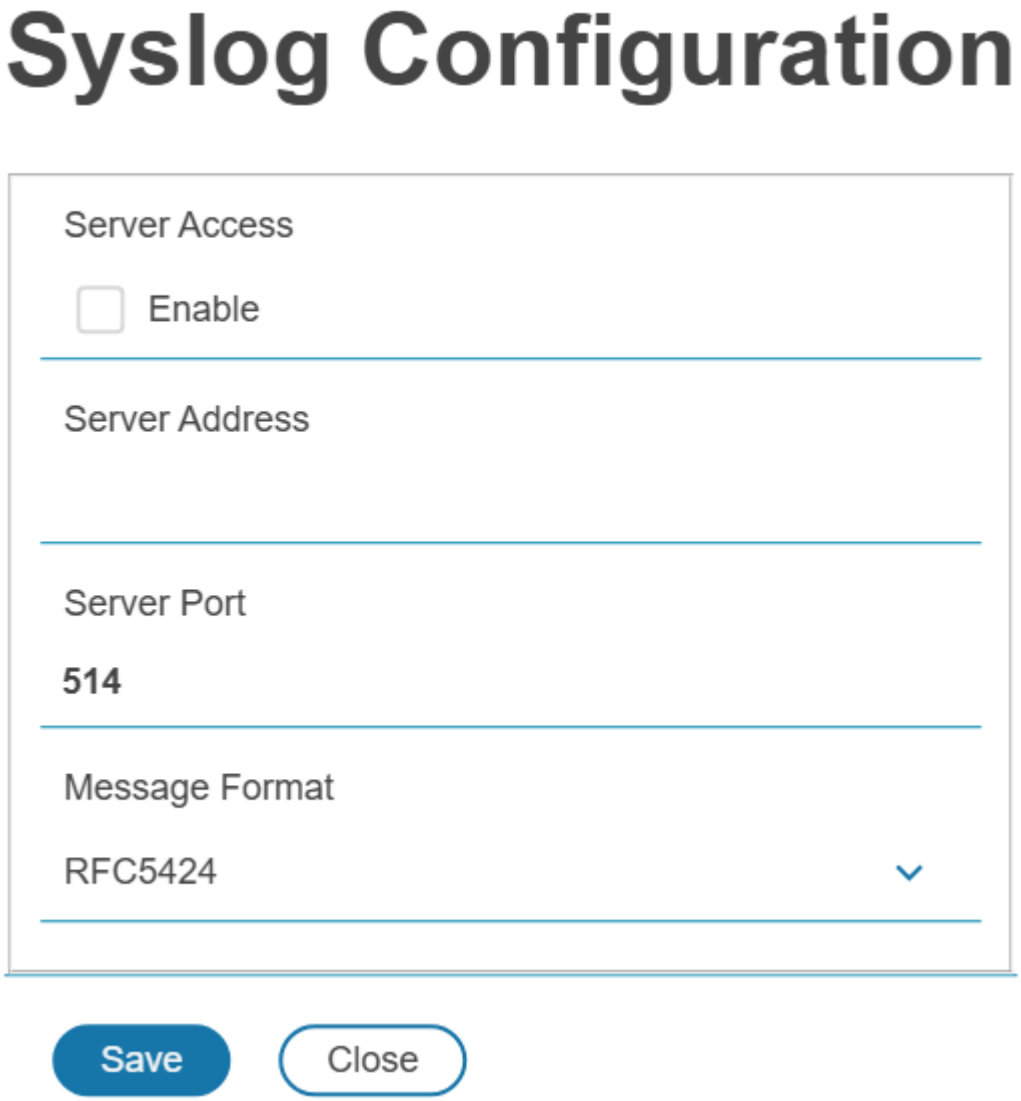
The Panduit FMPS NMC can be configured to send syslog messages to a syslog server when an event occurs. To do this, the information about the Syslog server needs to be configured.

Syslog Server Configuration

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



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



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

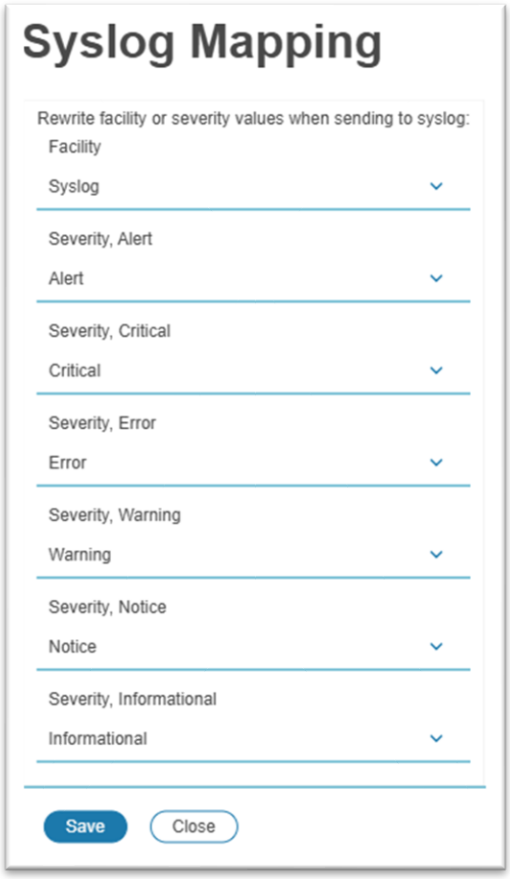
3. Press **Save** when done.

Syslog Mapping

The Syslog Facility and Severity fields can be mapped to other values to allow for easier

traceability on the Syslog sever. To edit the field

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

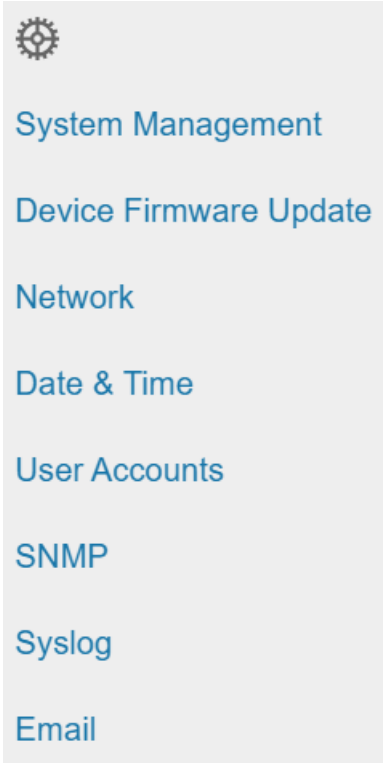


3. Select save to apply the settings.

Email Setup

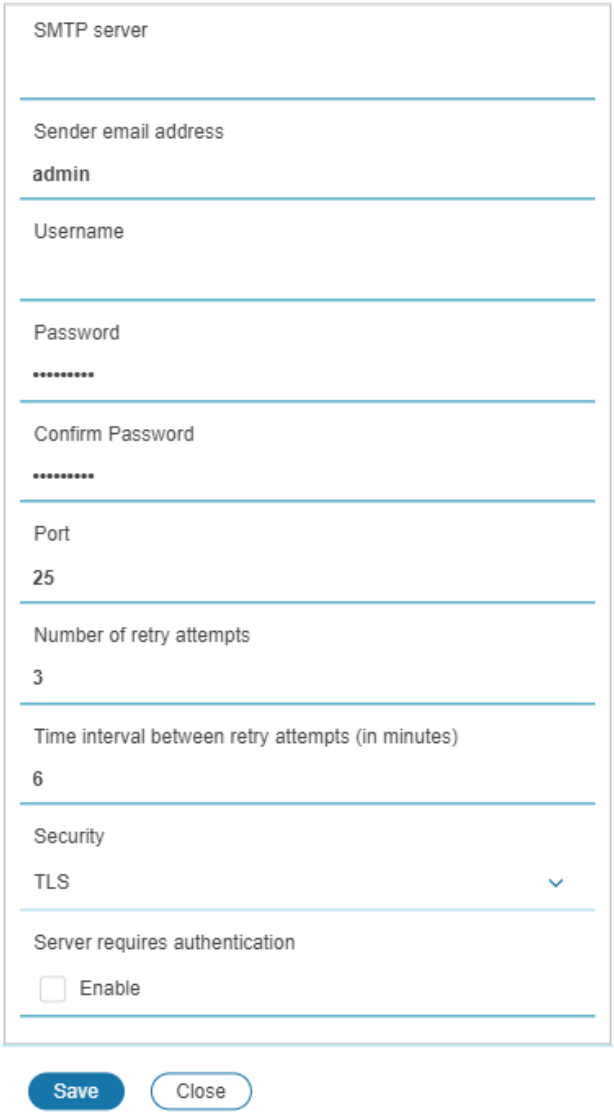
The Panduit FMPS NMC can be configured to send emails to specific users when an event occurs. To do this, the information about the SMTP (Simple Mail Transfer Protocol) server needs to be configured.

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



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

SMTP Account Settings



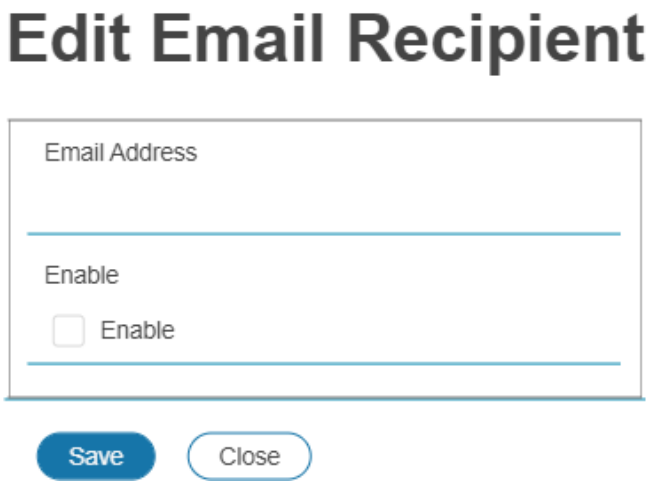
- Set the **SMTP server**. This is the address of the SMTP relay server that is going to accept the messages.
- Set the **Sender email address.** This is the email address from which the email is sent. Users can use a unique email address on each FMPS or the same email address across all FMPSs.
- Configure 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 FMPS 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.

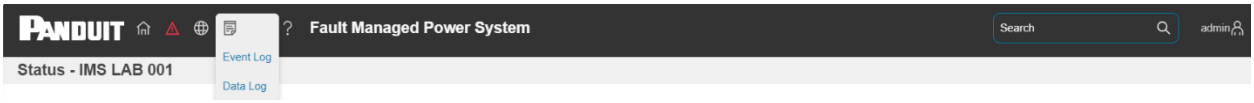


2. Enter the desired email address and press **Enable**.
3. Press **Save**.

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

Logs

The Panduit FMPS Network Management Card supports an Event Log as well as a Data Log which can be accessed from the Logs dropdown menu.



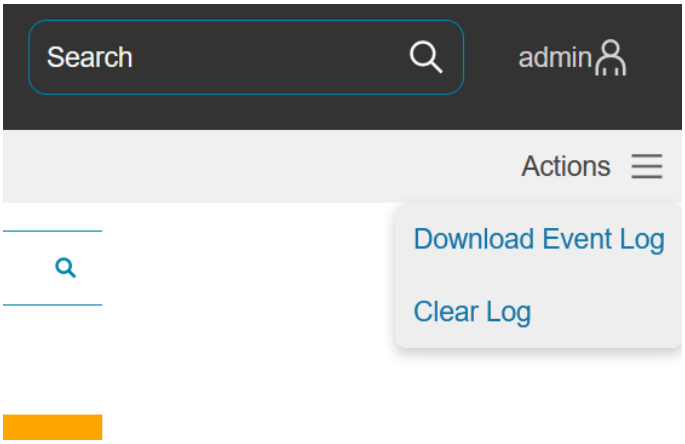
Event Log

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

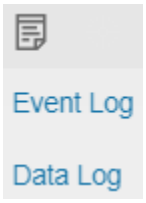
Event log can be downloaded or cleared from the Actions menu.



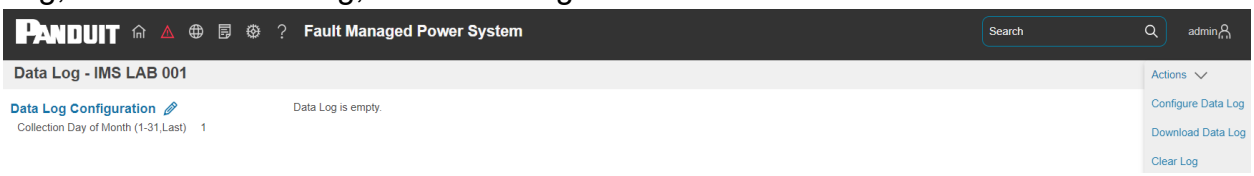
Data Log

The data log will collect a snapshot of the energy of the system on a given day of the month. The day the data will be collected is configurable.

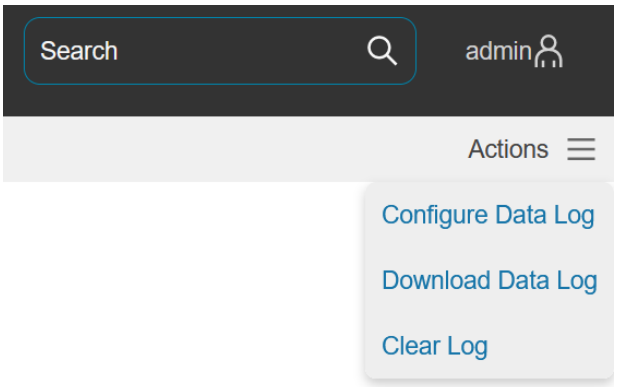
1. Go to **Logs** and select **Data Log**.



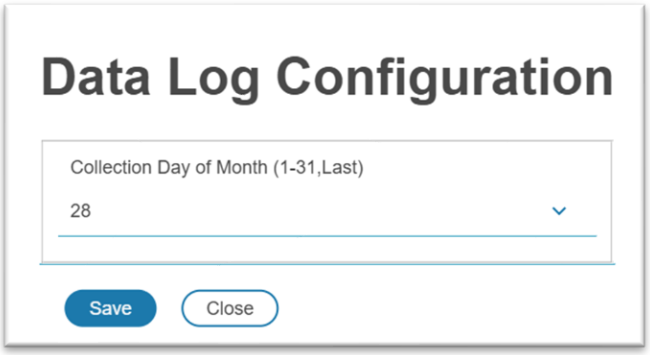
Features are accessed from the Actions dropdown menu and include: Configure Data Log, Download Data Log, and Clear Log.



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



3. Select the day of the month to be collected.



4. Select **Save**.

Web Interface Access

Logging Out

Users should logout after each session to prevent unauthorized changes to the system.

1. Click the **username 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

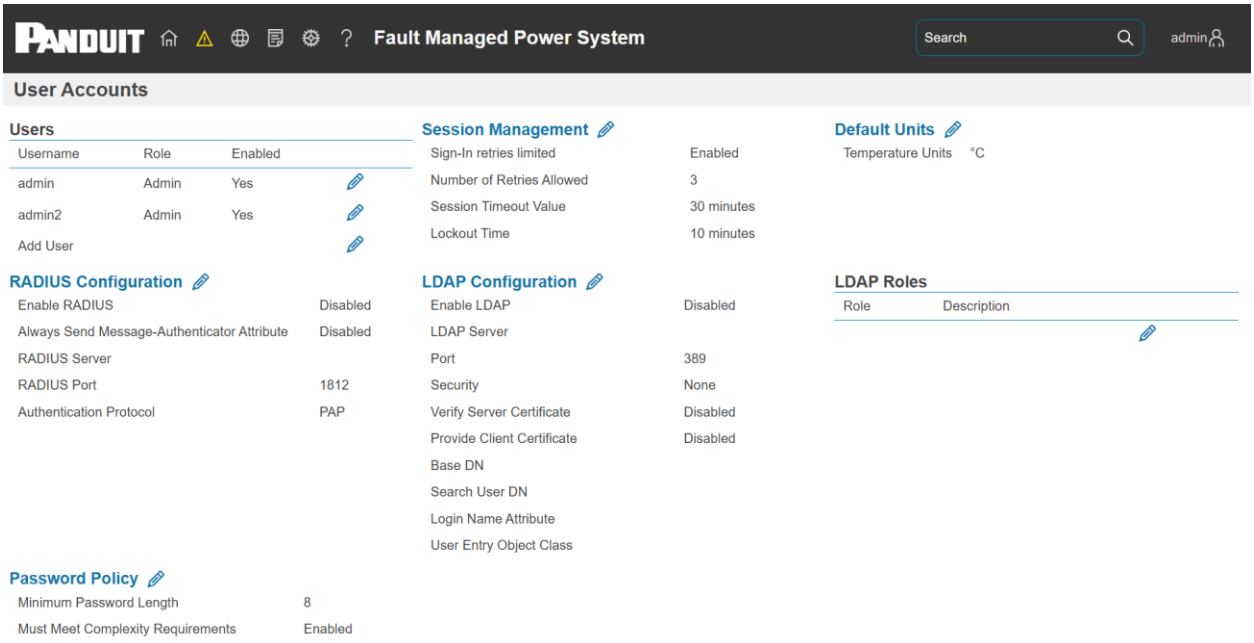
The FMPS comes with an **Admin, Controller,** and **Viewer** profile. The **Admin** role is typically the system administrator and has the Administrator Privileges with full operating permissions. The **Viewer** role is a Read Only profile. All other users must be added by a user with administrator privileges. The **Controller** role can control the FMPS functionality, like Receiver output power, 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 FMPS system but cannot change any configuration
viewer	Read-only permissions. Can monitor the system but cannot change any configuration

User Accounts

The User Accounts interface displays the following information which may be edited: Users, Roles, LDAP Configuration, Session Management, RADIUS Configuration, and Region. Click on the pencil icon to modify settings and select Save or Close when completed.



Add a user with the following steps. NOTE: must be logged in as an Admin to change settings.

1. Go to **Settings** and select **User Accounts**.
2. Click on the pencil next to the 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. NOTE: must be logged in as an Admin to change settings.

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. NOTE: must be logged in as an Admin to change settings.

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.**

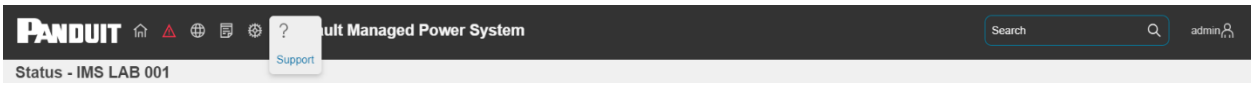
Change Password

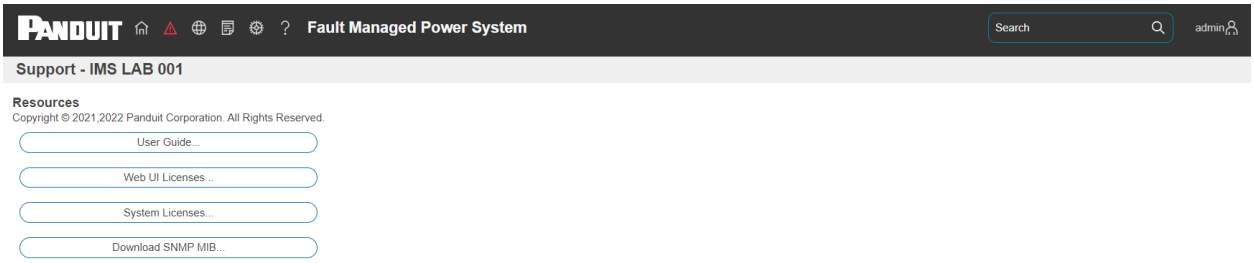
The Change Password feature can be used to modify the password used to access the system's user interface. At the Change Password screen, enter the required information, then click on Log In.

Help

The Help dropdown menu includes a Support option which provides links to the following resources:

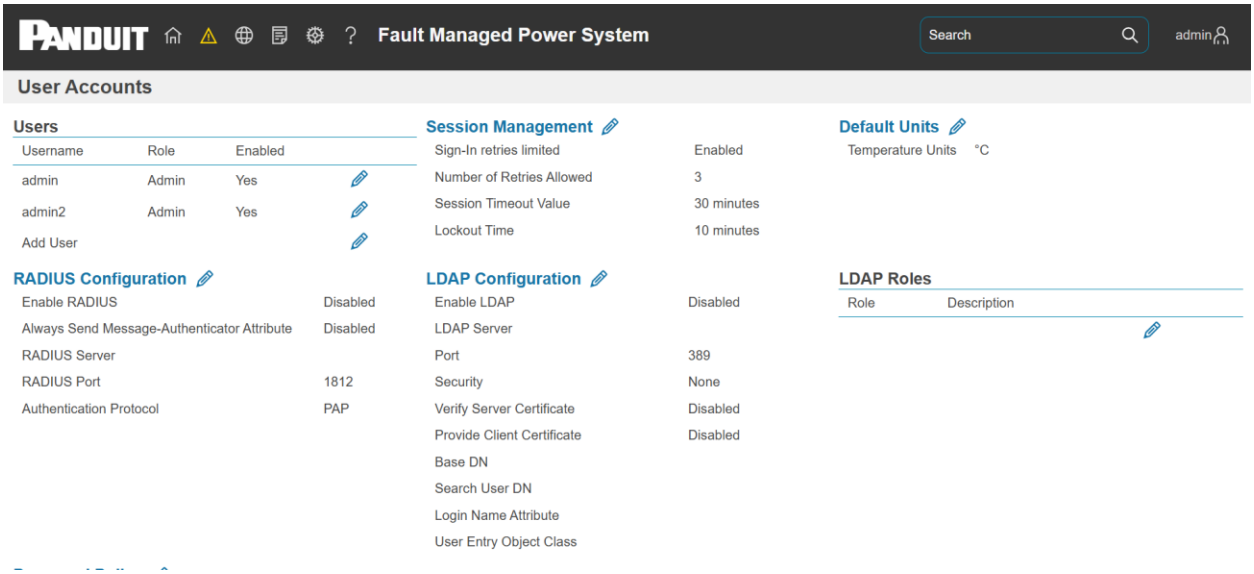
- User Guide
- Web UI Licenses
- System Licenses
- Download SNMP MIB



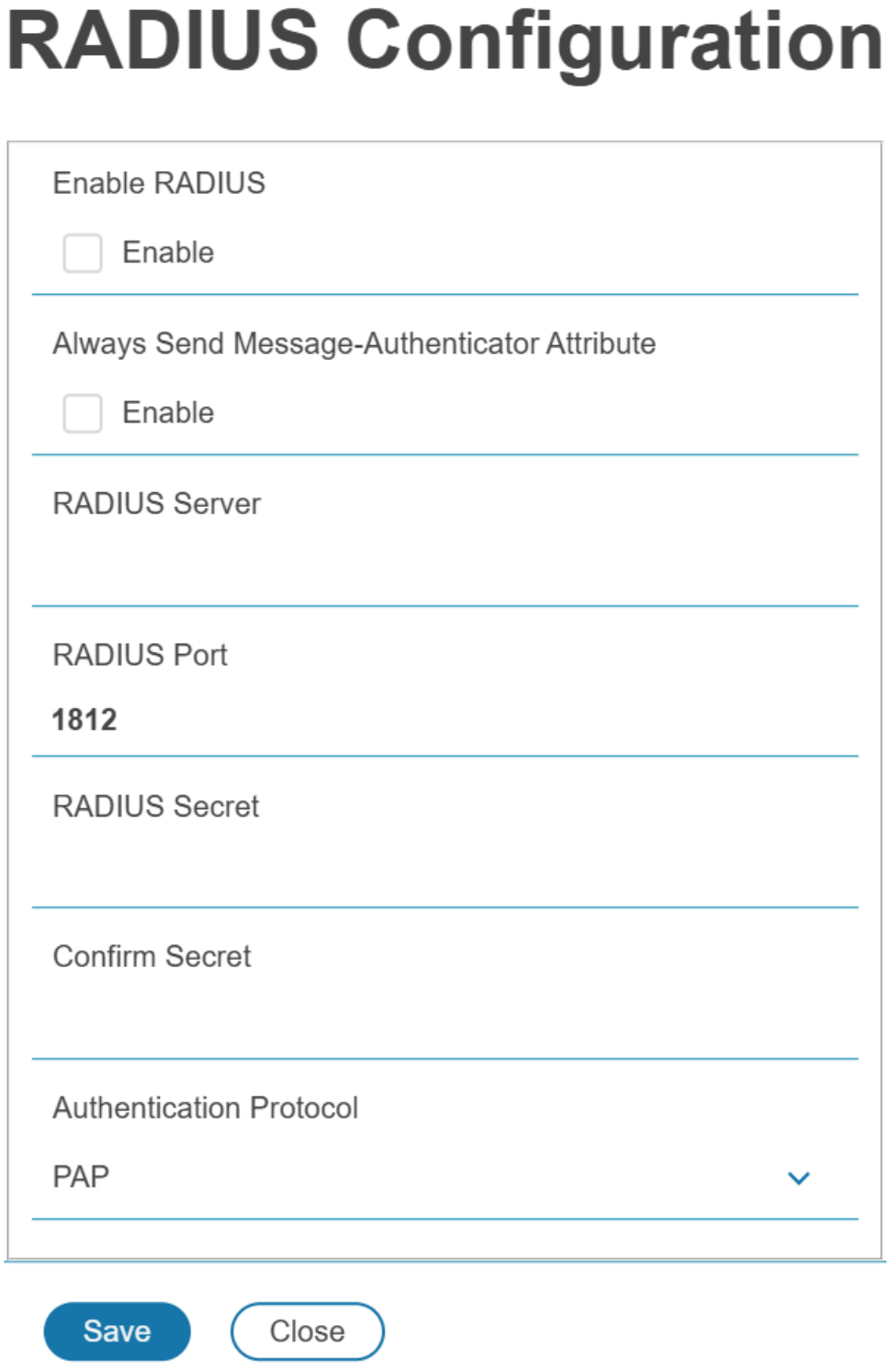


Setting Up the System for RADIUS Authentication

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



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



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

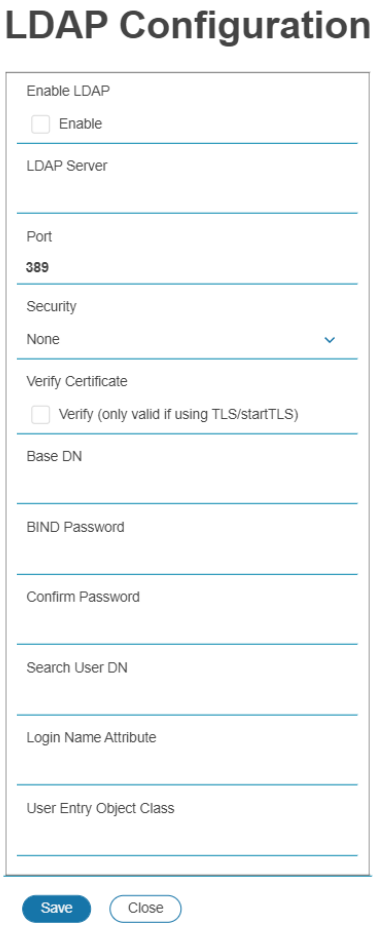
   Note: By default, a RADIUS user will have the “viewer” role if one is not specified. The administrator of the RADIUS server may configure a Panduit vendor (19536) dictionary, with a “User-Role” integer attribute set to User (1) or Admin (2) or Control(3). For complete details, see Appendix E: RADIUS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

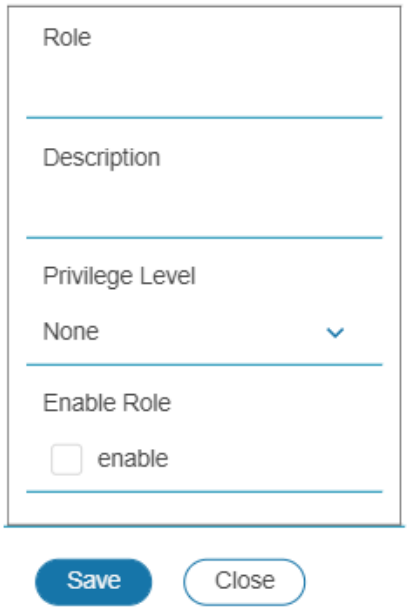


Once LDAP is configured, the FMPS must understand for which group authentication occurs. A role must be created on the FMPS to reference a group within the Active Directory (AD).

1. Within the Active Directory, create a group for the users that wish to be NMC administrators. *i.e. admins*

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

2. Within the FMPS 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).



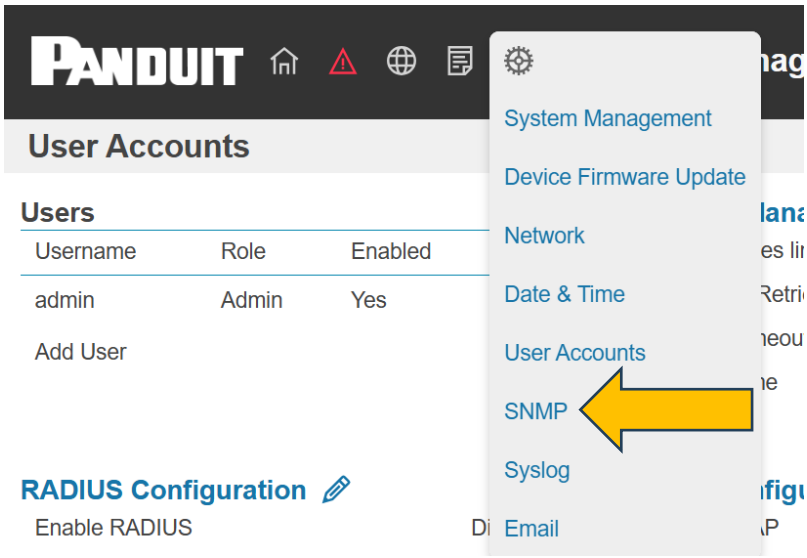
4. LDAP authentication is ready to use.

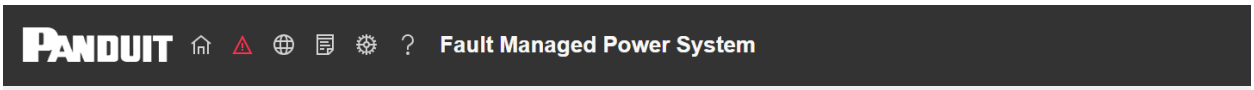
Section 3 – Simple Network Management Protocol (SNMP)

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.


PANDUIT
User Accounts
Users
Username
Role
Enabled
admin
Admin
Yes
Add User
RADIUS Configuration
Enable RADIUS
System Management
Device Firmware Update
Network
Date & Time
User Accounts
SNMP
Syslog
Email



SNMP

SNMP General

Enable SNMP	Disabled
SNMP Version	V3
Engine ID	80004c5003000f9c03906f

SNMP Port

SNMP Port	161
SNMP Trap Port	162

Download SNMP MIB...

SNMP v1/v2c Manager

IP Address	Read Community	Write Community	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
0.0.0.0	public	private	Disabled

SNMP v3 Manager

Username	Security Level	Authentication Algorithm	Privacy Algorithm	Enabled
	AuthPriv	SHA	AES128	Disabled
	AuthPriv	SHA	AES128	Disabled
	AuthPriv	SHA	AES128	Disabled
	AuthPriv	SHA	AES128	Disabled
	AuthPriv	SHA	AES128	Disabled

SNMP v2c Trap Receiver

Name	Host	Community	Enabled
			Disabled
			Disabled
			Disabled
			Disabled
			Disabled

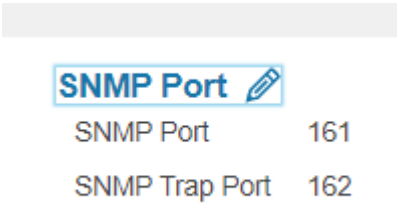
SNMP v3 Trap Server

Name	Host	Security Level	Authentication Algorithm	Privacy Algorithm	Enabled
		AuthPriv	SHA	AES128	Disabled
		AuthPriv	SHA	AES128	Disabled
		AuthPriv	SHA	AES128	Disabled
		AuthPriv	SHA	AES128	Disabled
		AuthPriv	SHA	AES128	Disabled

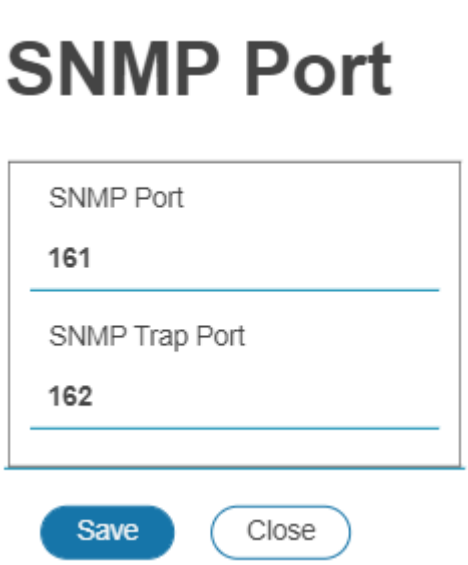
3. The SNMP General includes SNMP Access and Version.

Setup SNMP Port

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

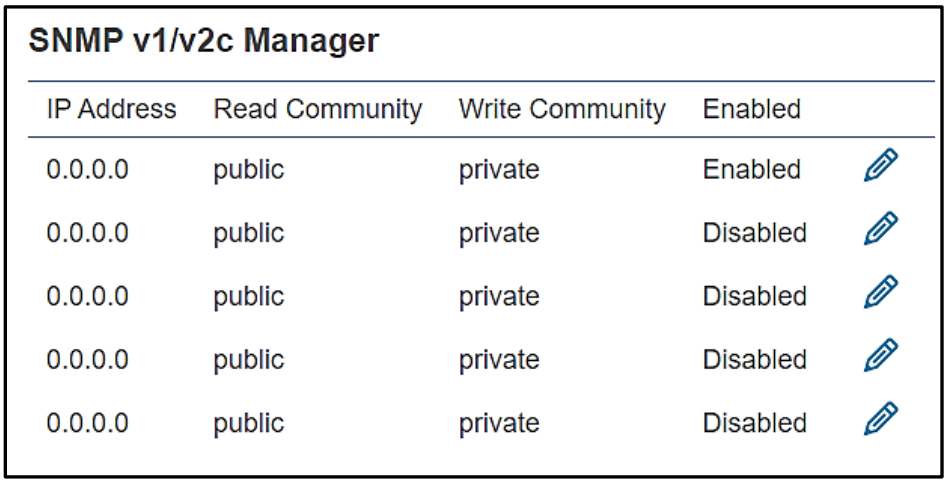


3. Set up SNMP Port and SNMP Trap Port.

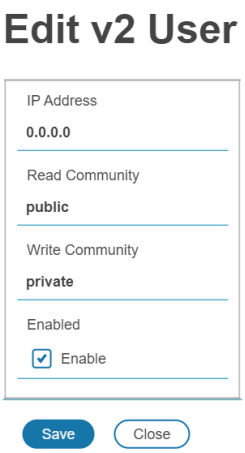


Configuring Users for SNMP V1/V2c

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.



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



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

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

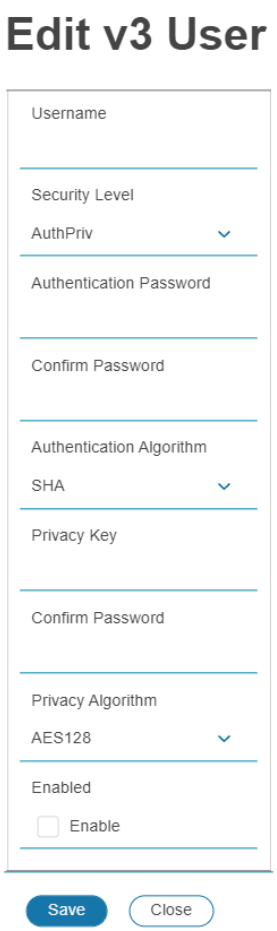
Configuring Users for SNMP v3

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

SNMP v3 Manager

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

4. The Edit panel pops up displaying the configurable options.



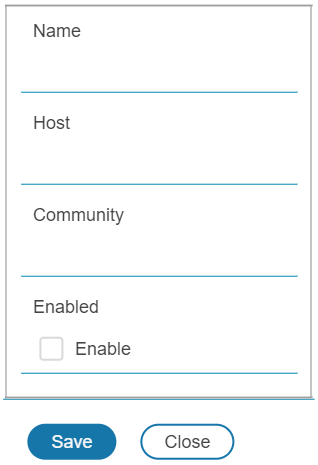
5. Configure the SNMP username.
6. Choose a Security Level from the dropdown menu.
   - NoAuthNoPriv: No authentication and no privacy. This is the default.
   - AuthNoPriv: Authentication and no privacy.
   - AuthPriv: Authentication and privacy.
7. Enter a new unique **Authentication Password** to be used for authentication. Repeat the authentication password below it in **Confirm Password**.
8. Select the desired authentication algorithm.
   - MD5
   - SHA
9. Enter a new unique Privacy Key to be used with the privacy algorithm. Repeat the privacy key below it in **Confirm Password**.
10. Select the desired privacy algorithm.
    - AES-128
11. Click **Enable** and **Save**.

Configuring SNMP Traps

The NMC keeps an internal log of all events. These events can be used to send SNMP traps to a third-party manager. To set up the NMC to send SNMP traps, follow the following procedure:

Configuring SNMP v1 Trap Settings

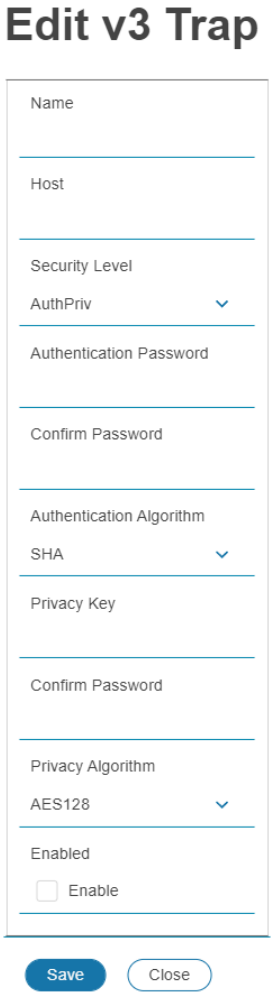
1. Go to **Settings > SNMP**.
2. Click the pencil next to SNMPV2c Trap Receiver that is to be updated.



3. Enter the **Name**, **Host**, and a **community** name in the fields provided.
   a. The name is a user assigned name to help distinguish the different receivers.
   b. The host name is the IP Address to which the traps are sent by the SNMP system agent.
   c. Community is the password on the SNMP management stations.
4. Select **Enable** to enable the receiver.
5. Select **Save** to save and exit.

Configuring SNMP v3 Trap Settings

1. Go to **Settings** > **SNMP.**
2. Click the pencil next to SNMPV3 Trap Server that is to be updated.



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

System Status LED (1)

The LED will change colors depending on the power usage of the FMPS.

LED State	Description
Green	Normal operation
Yellow	Capacity threshold (>90% system power)
Red	Capacity overload (100% system power)

Power Supply Status LED (2)

The LED will change colors depending on the Power Supply State.

LED State	Description
Green	Normal operation
Red	No communication with the Power Supply

NMC Status LED (3)

The LED will change colors depending on the NMC State.

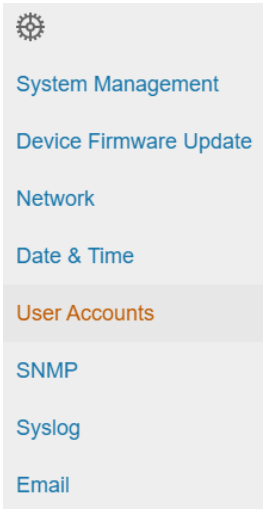
LED State	Description
Green	Normal operation
Red	Powering up
Slow Blinking Red (once per second)	System shutting down
Fast Blinking Red (three times per second)	Executing a factory reset
Yellow	Temperature out of range
Orange	Missing or damaged SD card (internal)

1

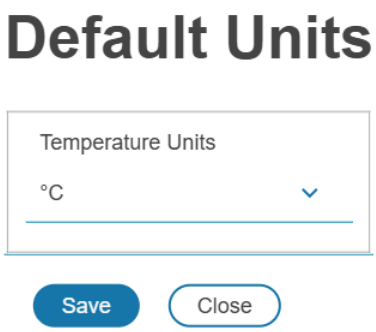
Configuring Temperature Scale

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

1. Go to **User Accounts.**



2. Select the pencil next to **Default Units.**
3. Select the correct units and select **Save.**



Section 5 – Security

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

API Access to Primary Features

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

Primary Features

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

- The API user may enable and disable power supplies, power transmitters and power receivers to manage power flow in the system.
- The API user may set thresholds to provide overload protection, which may turn off power to the affected load.

Secure Disposal Features

- The product provides a default settings feature that can be activated using a button press on the product, from the web user interface, from the SSH command line interface, or the USB serial interface.
- The default settings feature erases the encryption keys for the non-volatile storage used for configuration data and reinitializes the non-volatile storage area to default settings.
- The default settings feature erases the flash memory that stores the Event Log and Data Log.
- The default settings feature erases the flash memory that is used to temporarily store firmware update uploads.
- The default settings feature causes the SSH RSA 3072-bit private host key to be regenerated.
- The default settings feature causes the SSH ED25519 256-bit private host key to be regenerated.
- If the default settings feature cannot be activated OR the user does not want event log or data log files from being extracted from the flash memory on the device THEN the device PCBAs must be physically destroyed.

Non-volatile Storage

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

Authentication Data

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

Authentication Priority

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

- User Accounts
- RADIUS
- LDAP

The User Accounts authentication domain cannot be disabled.

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

Please do not define a valid username in multiple domains that has different passwords

with different expected permission levels as it may result in a user having unexpected permission granted to them.

Network Transport Security

- The product generates a random SSH RSA 3072-bit private host key the first time the product starts up.
- The product generates a random SSH ECDSA 256-bit private host key the first time the product starts up.
- The product has a randomly generated RSA 2048-bit private key configured by the factory. This key is used to generate a HTTPS certificate the first time the product starts up.
- The user may upload a custom HTTPS certificate and private key.
    - The HTTPS certificate should use a SHA-256 signature.
    - The private key should be RSA 2048-bit or prime256v1 (SECP256R1).
    - Other private key types may work, but performance may be negatively impacted if greater private key sizes are used: RSA 3072-bit, RSA 4096-bit; ECC curves: SECP192R1, SECP224R1, SECP256R1, SECP384R1, SECP521R1, SECP192K1, SECP224K1, SECP256K1, BP256R1, BP384R1, BP512R1, CURVE25519.
- The user may upload a custom HTTPS private key that is encrypted using a password. Private key decryption is compatible with openssl AES password encryption formats.
- If the private key is contained in a .pfx or .p12 file, you may convert that to the password encrypted PEM format using openssl. Please review the openssl documentation for more information. Example:
    - openssl pkcs12 -in [yourfile.p12] -nocerts -nodes -passin pass:[input_password] | openssl rsa –aes256 -out [privatekey.pem] -passout pass:[new_password]
- The product uses TLS 1.2 or TLS 1.3 to communicate with HTTPS web browser clients.
- Secure communication cipher negotiation with HTTPS clients uses these Cipher Suites:
    - Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
    - Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
    - Cipher Spec: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
    - Cipher Spec: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
    - Cipher Spec: TLS_AES_256_GCM_SHA384 (0x1302)
    - Cipher Spec: TLS_AES_128_GCM_SHA256 (0x1301)

- The product uses TLS 1.2 or TLS 1.3 to communicate with SMTP+STARTTLS (RFC 3702) and SMTPS servers (RFC 2487).
- Secure communication cipher negotiation with SMTP servers and LDAP servers uses these Cipher Suites:
    - Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
    - Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
    - Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)
    - Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
    - Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
    - Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
    - Cipher Suite: TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)
    - Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
    - Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
    - Cipher Suite: TLS_AES_128_CCM_SHA256 (0x1304)
    - Cipher Suite: TLS_AES_128_CCM_8_SHA256 (0x1305)
    - Cipher Suite: TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004)
    - Cipher Suite: TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005)
    - Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
    - Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
    - Cipher Suite: TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e)
    - Cipher Suite: TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f)
    - Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
    - Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
    - Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)
    - Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)
    - Cipher Suite: TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (0xc025)
    - Cipher Suite: TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026)
    - Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)
    - Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
    - Cipher Suite: TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 (0xc029)
    - Cipher Suite: TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 (0xc02a)
    - Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
    - Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)

- Cipher Suite: TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02d)
- Cipher Suite: TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02e)
- Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
- Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
- Cipher Suite: TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 (0xc031)
- Cipher Suite: TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 (0xc032)
- Cipher Suite: TLS_RSA_WITH_ARIA_128_CBC_SHA256 (0xc03c)
- Cipher Suite: TLS_RSA_WITH_ARIA_256_CBC_SHA384 (0xc03d)
- Cipher Suite: TLS_ECDHE_ECDSA_WITH_ARIA_128_CBC_SHA256 (0xc048)
- Cipher Suite: TLS_ECDHE_ECDSA_WITH_ARIA_256_CBC_SHA384 (0xc049)
- Cipher Suite: TLS_ECDH_ECDSA_WITH_ARIA_128_CBC_SHA256 (0xc04a)
- Cipher Suite: TLS_ECDH_ECDSA_WITH_ARIA_256_CBC_SHA384 (0xc04b)
- Cipher Suite: TLS_ECDHE_RSA_WITH_ARIA_128_CBC_SHA256 (0xc04c)
- Cipher Suite: TLS_ECDHE_RSA_WITH_ARIA_256_CBC_SHA384 (0xc04d)
- Cipher Suite: TLS_ECDH_RSA_WITH_ARIA_128_CBC_SHA256 (0xc04e)
- Cipher Suite: TLS_ECDH_RSA_WITH_ARIA_256_CBC_SHA384 (0xc04f)
- Cipher Suite: TLS_RSA_WITH_ARIA_128_GCM_SHA256 (0xc050)
- Cipher Suite: TLS_RSA_WITH_ARIA_256_GCM_SHA384 (0xc051)
- Cipher Suite: TLS_ECDHE_ECDSA_WITH_ARIA_128_GCM_SHA256 (0xc05c)
- Cipher Suite: TLS_ECDHE_ECDSA_WITH_ARIA_256_GCM_SHA384 (0xc05d)
- Cipher Suite: TLS_ECDH_ECDSA_WITH_ARIA_128_GCM_SHA256 (0xc05e)
- Cipher Suite: TLS_ECDH_ECDSA_WITH_ARIA_256_GCM_SHA384 (0xc05f)
- Cipher Suite: TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256 (0xc060)
- Cipher Suite: TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384 (0xc061)

  - Cipher Suite: TLS_ECDH_RSA_WITH_ARIA_128_GCM_SHA256 (0xc062)
  - Cipher Suite: TLS_ECDH_RSA_WITH_ARIA_256_GCM_SHA384 (0xc063)
  - Cipher Suite: TLS_RSA_WITH_AES_128_CCM (0xc09c)
  - Cipher Suite: TLS_RSA_WITH_AES_256_CCM (0xc09d)
  - Cipher Suite: TLS_RSA_WITH_AES_128_CCM_8 (0xc0a0)
  - Cipher Suite: TLS_RSA_WITH_AES_256_CCM_8 (0xc0a1)
  - Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CCM (0xc0ac)
  - Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CCM (0xc0ad)
  - Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8 (0xc0ae)
  - Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8 (0xc0af)
- The product provides a SSH (RFC 4253) server with these algorithms to communicate with SSH clients:
  - Key exchange algorithms:
    - curve25519-sha256
    - curve25519-sha256@libssh.org
    - ecdh-sha2-nistp521
    - ecdh-sha2-nistp384
    - ecdh-sha2-nistp256
    - diffie-hellman-group14-sha256
    - diffie-hellman-group16-sha512
    - kexguess2@matt.ucc.asn.au
    - kex-strict-s-v00@openssh.com
  - Host key algorithms:
    - ssh-ed25519
    - rsa-sha2-256 (2048-bit)
  - Encryption algorithms:
    - chacha20-poly1305@openssh.com
    - aes128-ctr
    - aes256-ctr
  - MAC algorithms:
    - hmac-sha2-256
    - hmac-sha2-512

Network Configuration Data

- Network Configuration, including Static IP addresses and addresses obtained by DHCP are exposed on an “Identification” page and on a Network Configuration page, to aid in network management of the product.

- The product implements an internal authentication mechanism, authorization events generate “Event Logs” containing the IP address and username of successful logins, and the IP address of failed logins.

Logging

- Event log messages and alarm messages sent to the Event Log, Syslog Remote (RFC 3164, RFC 5424), Email (RFC 5321) and SNMP trap (RFC 3416, RFC 3413) may contain the IP address and username of the user performing the action.
- The data log and event log produce a “Log is downloaded by user” message each time the log has changed and a new viewer has accessed it.

External Authentication Mechanisms

- LDAP & RADIUS – username & password are stored on encrypted non-volatile storage.
- CVE-2024-3596 BlastRADIUS: The firmware includes a “Always send Message-Authenticator attribute” feature that must be enabled to mitigate the BlastRADIUS vulnerability.
- LDAP (RFC 4511) is not encrypted over the network.
- LDAPS (RFC 4513) and LDAP with StartTLS (RFC 4511) are encrypted over the network.
- If a “Server Certificate” is configured and “Verify Server Certificate” is enabled, then the remote LDAP server authenticity is validated.
- The user may upload a custom LDAP Client Private Key that is encrypted using a LDAP Client Private Key Password. Private key decryption is compatible with default openssl key generation password encryption formats.
- RADIUS (RFC 2865) does not transmit the password as cleartext in the User-Password attribute, but its native protections are not equivalent to modern TLS-based transport security. Use Message-Authenticator protections and deploy RADIUS only on trusted/segmented networks.

Secure Boot Protection

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

- The bootloader continues the chain of trust by verifying the authenticity and integrity of the application executable, by applying the same algorithm as used by the ROM bootloader to load the bootloader.

Firmware Update Protection

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

Other Features

- The product includes a real-time clock and a replaceable battery. When combined with NTP, accurate timestamps on logs are provided.

Protocols

- The product provides mDNS (UDP port 5353) to enable MacOS and Windows to easily connect to the device via “panduit-fmps-nmc-<macaddress>.local”.

Intended Use Security Context

This product is designed for deployment in physically secure environments such as a secured room or container. The assumed physical security baseline includes:

- Room entry controls: security lobby, access badges and/or key locks.
- Container controls: restricted physical access via key locks or electronic access control.

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

Secure deployment

Configure the NMC regarding the following settings:

User Roles

The “Web Interface Access” section describes Roles of system users. Choose the least-

privileged role that provides the access required for the user's responsibilities.

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

NTP

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

Upload HTTPS Certificate and Private Key

Certificates ensure authenticity of the encrypted connection to the device's HTTPS server. It is recommended that an X.509 Server certificate is uploaded to the NMC and that the certificate use a RSA 2048-bit key. The HTTPS Certificate and HTTPS Private Key can be accessed from **Settings → Network settings → Web Access Configuration**

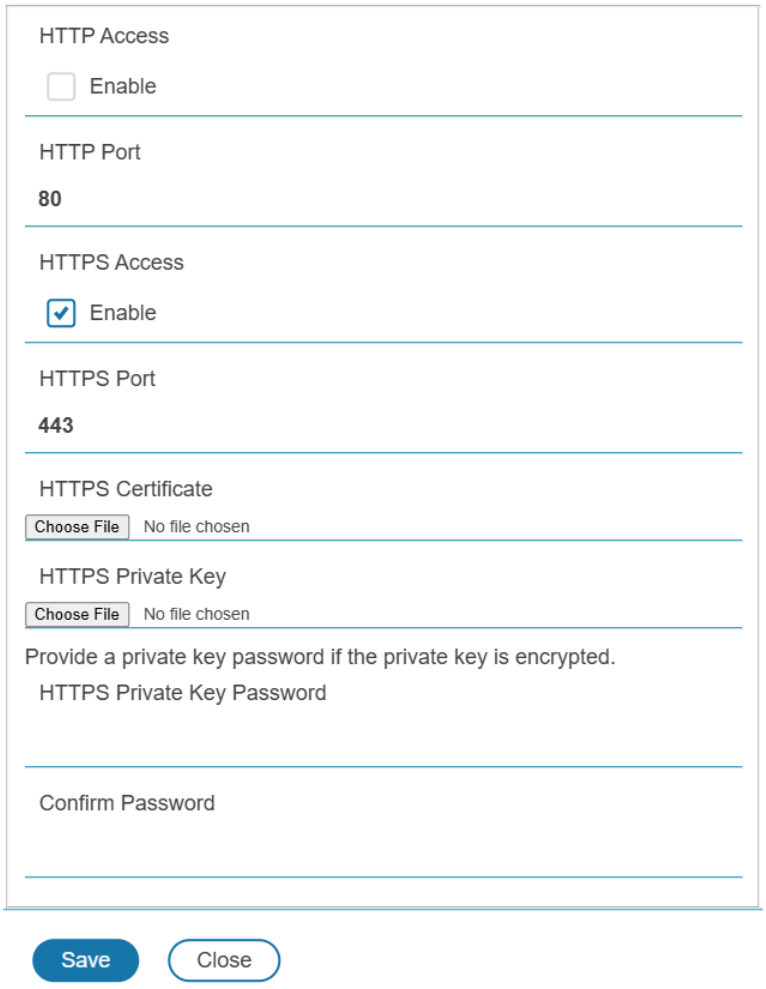


Figure 2: SSL Certificate Load Screen

Use SNMPv3

The NMC comes with support for both SNMPv2c and SNMPv3. For a higher security deployment, it is recommended to disable SNMPv2c. Another recommendation is to configure all SNMPv3 user and traps receiver with an “Auth Priv” security level, authentication algorithm of SHA and a privacy algorithm of AES128.

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

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

Disabling unused interfaces

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

use, it is recommended to disable these interfaces.

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

Review Session management

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

TLS Server Certificate Verification

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

TLS Client Certificate and Client Private Key

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

SSH Algorithm Strength

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

The REST /api/login provides info about password policy

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

Secure Operation Summary

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

Administrators are responsible for configuring accounts, roles, authentication domains, secure communication options, time sources, logging/notification destinations, firmware update sources, and enabled interfaces according to site security policy. Periodic maintenance should be performed by ensuring the firmware is upgraded when a new

release is available. Firmware upgrade automation can be achieved by using a DCIM or the Auto Upgrade feature on products that provide the feature. Administrators should also periodically review local accounts and assigned roles, external authentication server configuration, certificate validity and expiration dates, enabled services and interfaces, and security-relevant configuration changes. If remote Event Notification is not used, the Data Log and Event Log may be reviewed periodically, as the logs roll over based on log usage.

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

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

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

Defense-in-Depth Strategy Summary

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

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

Defense-in-depth layer (Applicability)	Applicable Security chapter sections	Threats or risks addressed	User mitigation strategy
Security context and physical deployment **(Platform-**	Intended Use Security Context; Secure deployment	Physical access to exposed ports, removable media, local interfaces, logs, configuration data, and	Deploy the product in the intended physically secured environment, local peripheral interfaces (e.g. serial, accessories, USB), and use compensating controls such as network segmentation, enhanced logging, and external monitoring

specific)		storage devices.	when the baseline environment is not met.
Interface and API access control **(Feature-dependent)**	API Access to Primary Features; Primary Features; Secure deployment	Unauthorized control of configuration, firmware update, outlet power, power flow, or other product functions exposed through APIs or local interfaces.	Limit API and interface use to authorized users and roles, review API documentation, disable unused APIs or interfaces where supported, and protect physical ports when not required.
Identity, authentication, and authorization **(Platform-specific)**	Authentication Data; Authentication Priority; User Account Changes; External Authorization Mechanisms	Credential misuse, unexpected privilege assignment, weak account management, duplicate usernames across authentication domains, and unauthorized access.	Manage user accounts and roles carefully, avoid defining the same username in multiple authentication domains with different permissions, protect administrator access, and use the configured authentication domains according to local security policy.
Credential and secret protection at rest **(Platform-specific)**	Non-volatile Storage; Authentication Data; External Authorization Mechanisms; Wireless Communication	Disclosure of stored configuration data, passwords, SNMP community strings, remote authentication secrets, Wi-Fi configuration, firmware images, or other sensitive data.	Be aware of product features and configuration options that protect sensitive data at rest where available, maintain physical protection for the device, and follow secure disposal or destruction guidance when stored data must not be recoverable.
Network confidentiality, integrity, and endpoint authenticity **(Platform- and version-specific)**	Network Transport Security; HTTPS Certificate Upload / Replacement; TLS Server Certificate Verification; TLS Client Certificate and Client Private Key; External Authorization Mechanisms	Eavesdropping, credential exposure, server impersonation, weak certificate trust, downgrade to unencrypted protocols, and use of obsolete or compatibility algorithms.	Prefer HTTPS, SSH, LDAPS, StartTLS, SMTPS, and other encrypted protocol options; upload trusted certificates; enable server certificate verification where supported; provide client certificates where required; and configure clients to avoid weak SSH algorithms.
Legacy and compatibility protocol risk management **(Feature-dependent)**	Network Transport Security; Security Implications of Configuration Changes; External Authorization Mechanisms; Protocols; Secure deployment	Plaintext management access, weak or legacy authentication and integrity mechanisms, exposure from SNMPv1/v2c, Telnet, LDAP without TLS, RADIUS compatibility behavior, TACACS+ native protection limits, legacy SSH algorithms, discovery protocols, and other compatibility	Disable legacy or unused protocols where possible, prefer SNMPv3 AuthPriv, encrypted LDAP variants, HTTPS, SSH, and TLS-protected services, enable RADIUS Message-Authenticator protection where applicable, and restrict legacy protocol use to trusted and segmented networks when it cannot be disabled.

		features.	
Secure configuration and hardening **(Common with platform-specific details)**	Security Implications of Configuration Changes; Secure deployment; Review Session management; Disabling unused interfaces	Insecure defaults, unnecessary exposed services, misconfiguration, loss of alerts, insecure session settings, and accidental use of less secure communication paths.	Review security-relevant configuration changes before use, disable unused services and physical interfaces where supported, configure session settings to match local policy, use secure notification paths, and periodically review the deployment configuration.
Logging, monitoring, and time accuracy **(Platform-specific)**	Logging; Network Configuration Data; Security Implications of Configuration Changes; NTP; Syslog Remote Forwarding; Security Response	Loss of audit evidence, inaccurate timestamps, inability to investigate unauthorized access, local log destruction after reset, and missed security notifications.	Configure a trusted NTP source, enable remote syslog or other remote notification channels where supported, protect log destinations, review event notifications, and report suspected security incidents and vulnerabilities through Technical Support.
Firmware authenticity, integrity, and update control **(Platform- and version-specific)**	Secure Boot Protection; Firmware Update Protection; Automatic Firmware Upgrade; Auto Update Config URI	Execution of unauthorized firmware, tampered update packages, corrupted boot or application images, unauthorized update repositories, and exposure of secrets in update configuration files.	Use the authenticated firmware update process, keep firmware current, restrict access to configured firmware and configuration update repositories, use HTTPS for update resources, and protect update configuration files that may contain sensitive information.
Wireless exposure control **(Feature-dependent)**	Wireless Communication; Direct Connect; Secure deployment	Unauthorized wireless access, unintended access point exposure, weak wireless configuration, and exposure of wireless credentials or configuration.	On products that have Wi-Fi, keep Wi-Fi disabled unless required, understand Direct Connect activation behavior, use supported WPA security options appropriate for the deployment, and protect any physical action required to activate wireless access.
Discovery and network visibility **(Platform-specific)**	Protocols; Network Configuration Data	Unwanted local network discoverability, disclosure of hostnames or addressing information, and increased visibility on shared networks.	Account for mDNS, LLMNR, DHCP, DNS, and exposed network identification behavior in network design and segmentation, and enable discovery behavior only where it supports the intended deployment.
Secure disposal and data sanitization **(Platform- and feature-dependent)**	Secure Disposal Features; Secure Erase — NIST SP 800-88 Media Sanitization; Non-volatile Storage	Residual data exposure after decommissioning, inability to erase local storage, recovery of logs or configuration data, and reuse of device identity keys after reset.	Use reset-to-defaults or secure erase features where available, verify the disposal procedure appropriate to the storage type, and physically destroy PCBAs or media when software-based disposal cannot be completed or residual data must not be recoverable.

Security Response

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

Warranty and Regulatory Information

Warranty Information

(https://www.panduit.com)

Regulatory Information

Safety and regulatory compliance

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

Panduit Support and Other Resources

The majority of support needs can be met by visiting Panduit.com and navigating to the respective product page. If additional assistance is required, we are here to help.

Accessing Panduit Support

North America

Customer Service

- Price & Availability
- Expedites

800-777-3300 or cs@panduit.com

FMPS Technical Support:

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

Email: TechSupport@panduit.com

Europe / Middle East

Customer Service

- Price & Availability
- Expedites

0044-(0)208-6017219 or EMEA-CustomerServices@panduit.com

FMPS Technical Support:

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

Email: TechSupportEMEA@panduit.com

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

Acronyms and Abbreviations

A

Amps/Amperes

AC

Alternating Current

AES

Advanced Encryption Standard

CLI

Command Line Interface

DHCP

Dynamic Host Configuration Protocol

FMPS

Fault Managed Power System

GUI

Graphical User Interface

IP

Internet Protocol

kW

Kilowatts

LAN

Local Area Network

LDAP

Lightweight Directory Access Protocol

SHA

Secure Hash Algorithms

SNMP

Simple Network Management Protocol

TCP/IP

Transmission Control Protocol/Internet Protocol

V

Volts

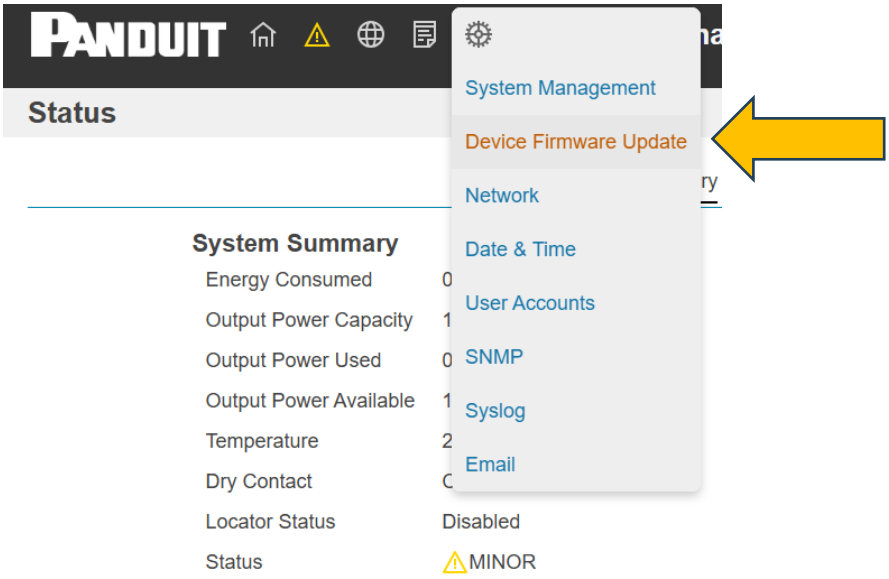
W

Watts

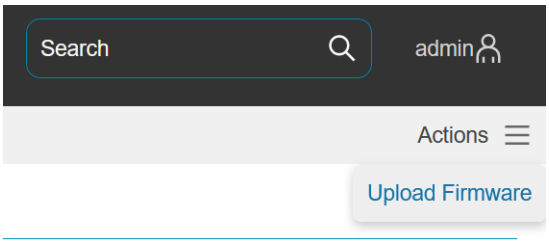
Appendix A: Firmware Update Procedure

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 of the Fault Managed Power System. For the latest firmware please visit: panduit.com → Support → Download Center → FMPS

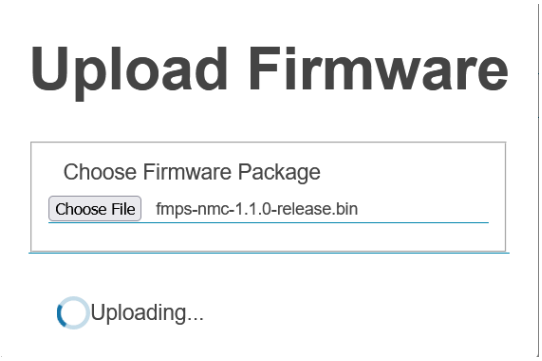
1. Download the firmware file from the Panduit web page.
2. Unzip the downloaded file.
3. Open the User interface in a web browser by entering the NMC IP address.
4. Login with Administration credentials.
5. Go to **Settings > Device Firmware Update**.



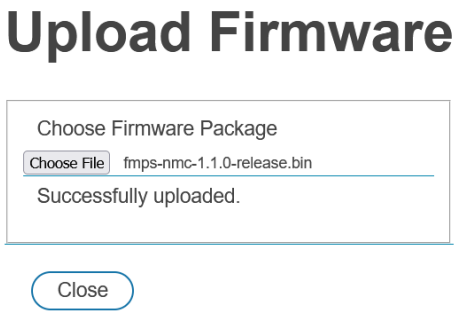
6. In the upper right, transfer the new Firmware onto the NMC using the Update Firmware command from the dropdown.



7. In the Firmware Update dialog box, click on ‘Choose File’, then browse to the Firmware file named fmps-nmc-vx.x.x-release.bin. When the file is selected, the dialog box will display “Uploading” text at the bottom.

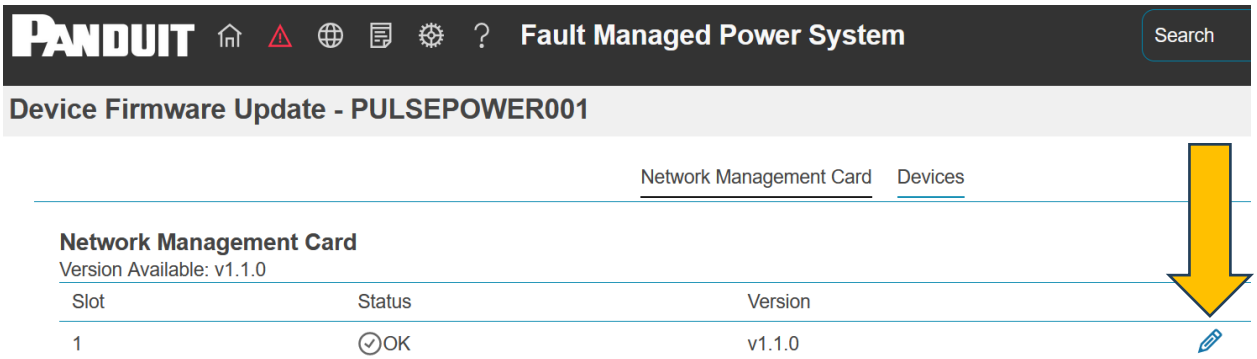


8. The screen will then change to “Successfully Uploaded”. The dialog box can be closed.

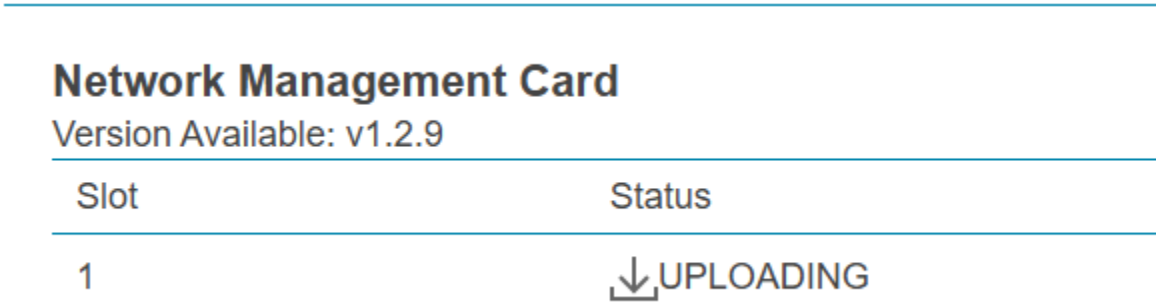


NOTE: The firmware has not been installed to any device yet. The Version Available will be displayed below the device name and will match the file name uploaded.

9. **To update the NMC**, click on the pencil icon to the right of the screen.

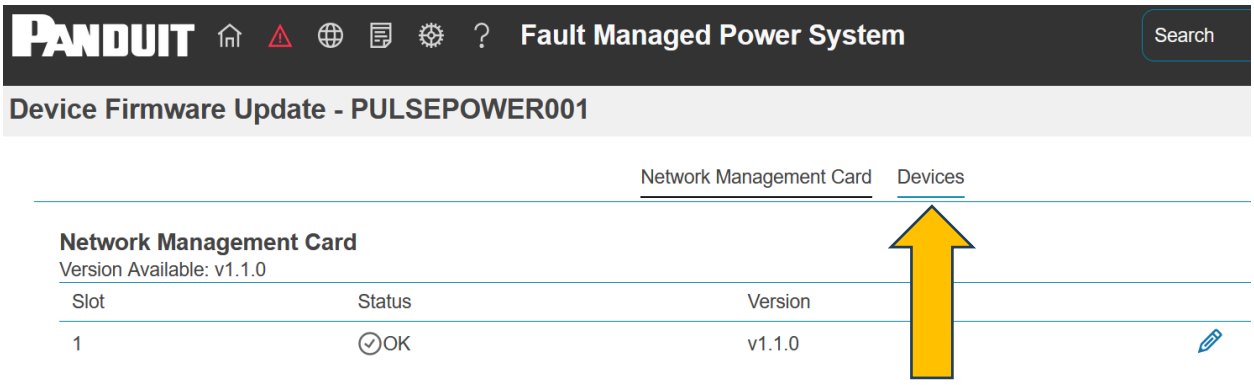


When the dialog box opens, click on Upload.

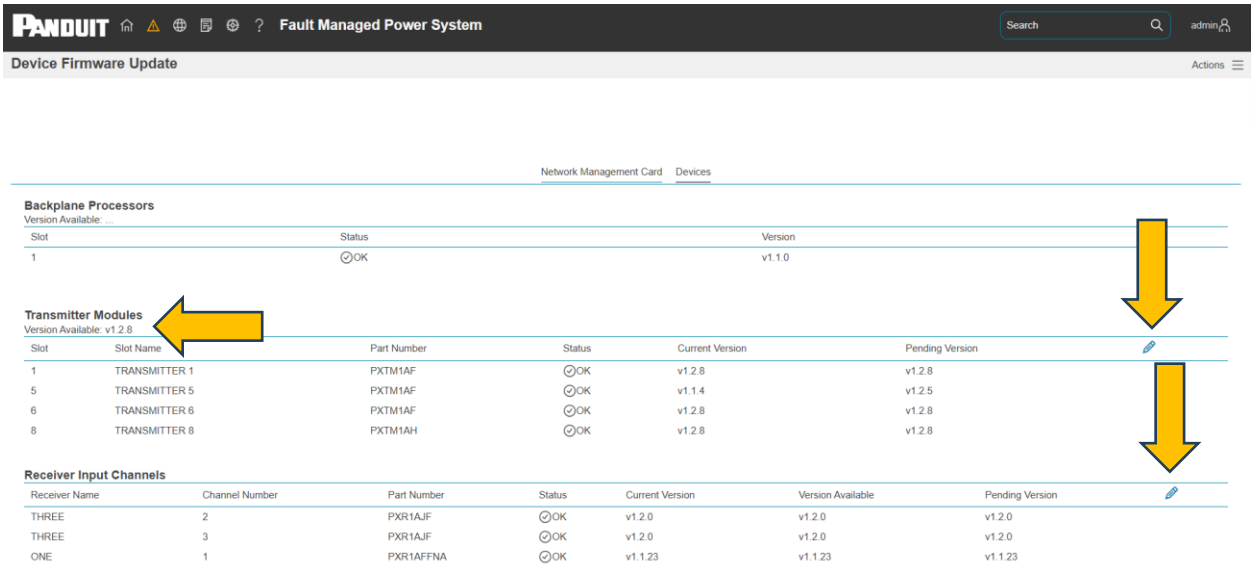


The Firmware is now being installed onto the NMC. After the file is installed, the NMC will **automatically reboot**.

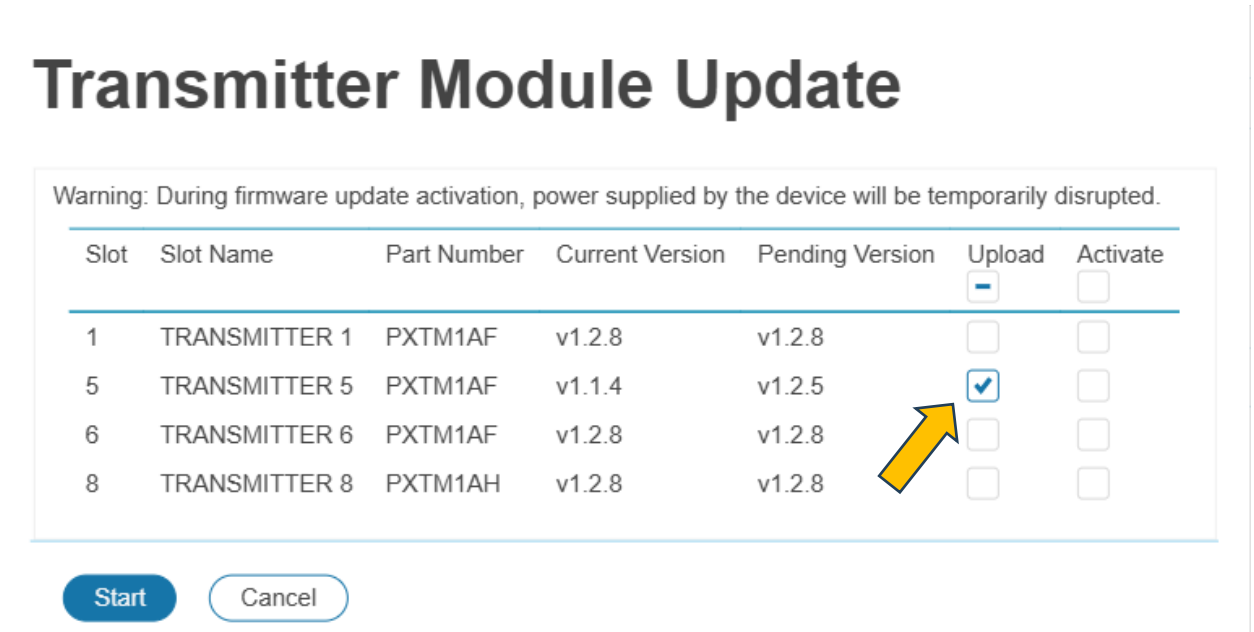
To update the Transmitter and/or Receiver, click on Devices from the main page.



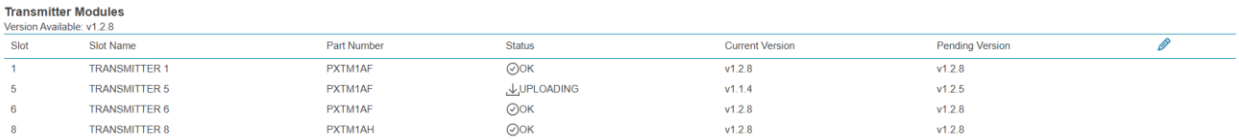
Select the device to be updated using the pencil icon.



As an example, updating the firmware of Transmitter 5 is shown below.



Select the Upload checkbox of the Transmitter that is to be updated then press Start. The dialog box will close and the status of the Transmitter will change to "Uploading". The Pending Version will match the Available Version after completion.



Transmitter Modules

Version Available: v1.2.8

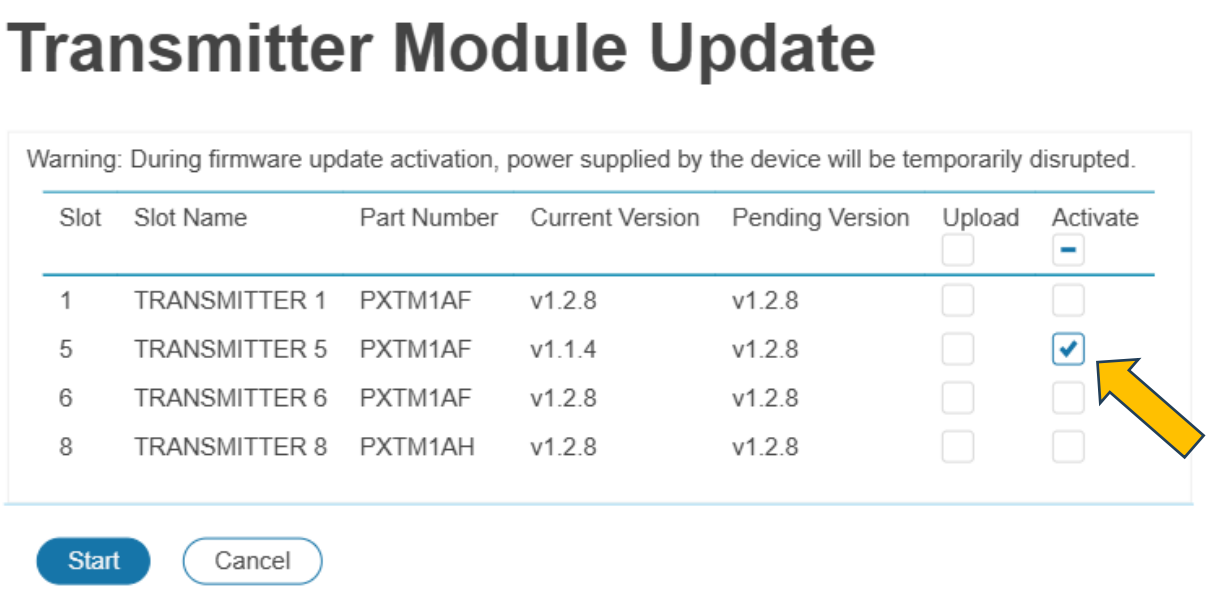
Slot	Slot Name	Part Number	Status	Current Version	Pending Version
1	TRANSMITTER 1	PXTM1AF	OK	v1.2.8	v1.2.8
5	TRANSMITTER 5	PXTM1AF	UPLOADING	v1.1.4	v1.2.5
6	TRANSMITTER 6	PXTM1AF	OK	v1.2.8	v1.2.8
8	TRANSMITTER 8	PXTM1AH	OK	v1.2.8	v1.2.8

NOTE: The Transmitter and Backplane firmware will take less than a minute to download. **The Receiver may take over an hour to download and there will be a persistent alarm relaying "Sending firmware upgrade to receiver in progress" that will clear upon completion.**

NOTE: Multiple Transmitters or Receivers can be selected by checking the box next to the desired device or by using the select all button at the top. In this case, one device will download then another until all are completed.

NOTE: The system is still fully functional at this point and the Update Device Firmware screen can be left without affecting the download.

To apply the firmware update (after Uploading completes), reenter the Update screen using the pencil icon and check the Activate button then press Start.



Transmitter Module Update

Warning: During firmware update activation, power supplied by the device will be temporarily disrupted.

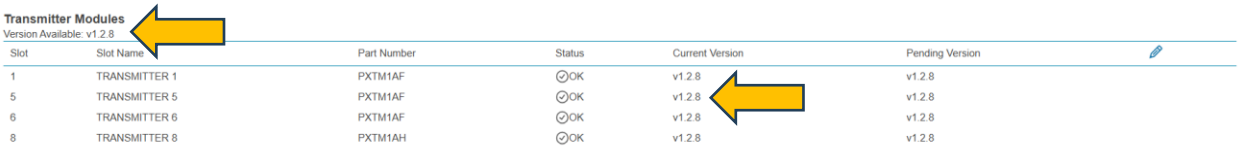
Slot	Slot Name	Part Number	Current Version	Pending Version	Upload	Activate
1	TRANSMITTER 1	PXTM1AF	v1.2.8	v1.2.8	☐	☐
5	TRANSMITTER 5	PXTM1AF	v1.1.4	v1.2.8	☐	☑
6	TRANSMITTER 6	PXTM1AF	v1.2.8	v1.2.8	☐	☐
8	TRANSMITTER 8	PXTM1AH	v1.2.8	v1.2.8	☐	☐

Start Cancel

CAUTION: The device being Activated/Updated will power-cycle briefly to apply the update. During this time, the Transmitter and connected Receiver channels

will disable output. It is recommended to take the final connected device offline before Activation. If updating a Receiver, all three Receiver channels will be activated at the same time.

10. When the Activation completes, the Current Version will match the Version Available.



Appendix B: System Reset or Password Recovery

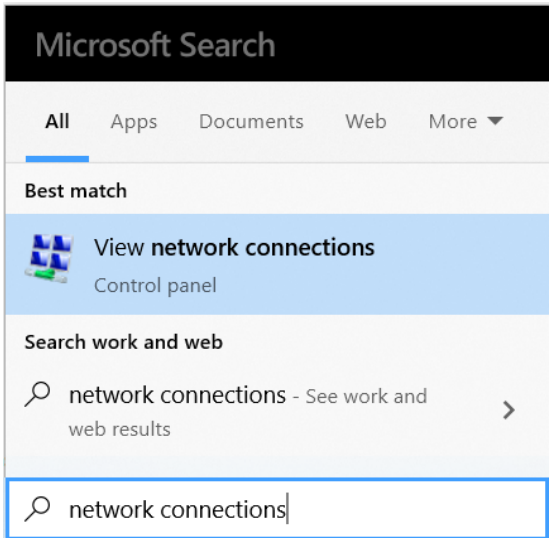
Press and hold the Reset Button for 2 seconds to recover from an NMC controller communication failure. The green LED will flash slowly, indicating the controller will reset. This will cause a reset of the NMC controller, all configuration(s) will be retained.

To Default the controller to factory settings, press and hold the Reset Button for at least 10 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).

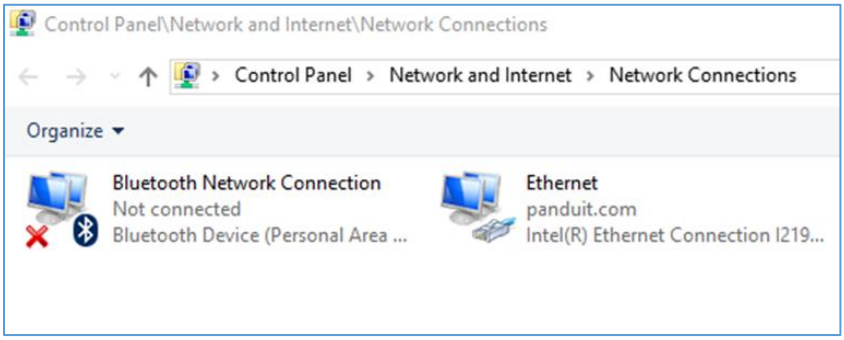
Appendix C: Direct connect to the FMPS via Ethernet without Bonjour

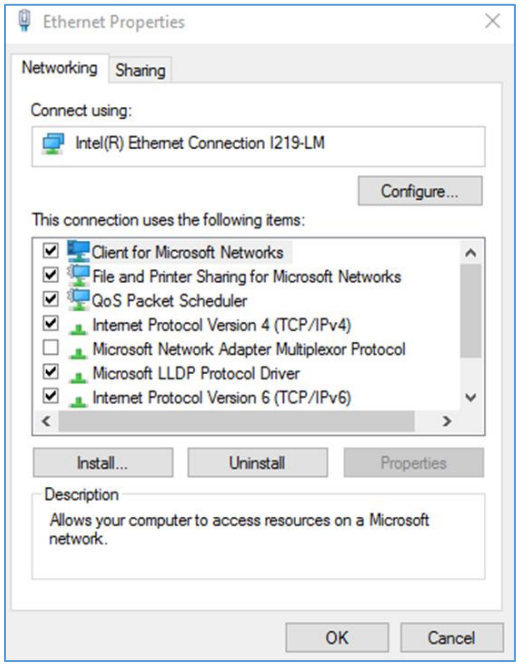
Note: Instructions refer specifically to Windows 10. Please refer to operating system documentation if not using Windows 10.

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



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





3. Select **Internet Protocol (TCP/IP) Version 4** in the list. Then click the **Properties** button.

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. This error is expected and can be ignored.

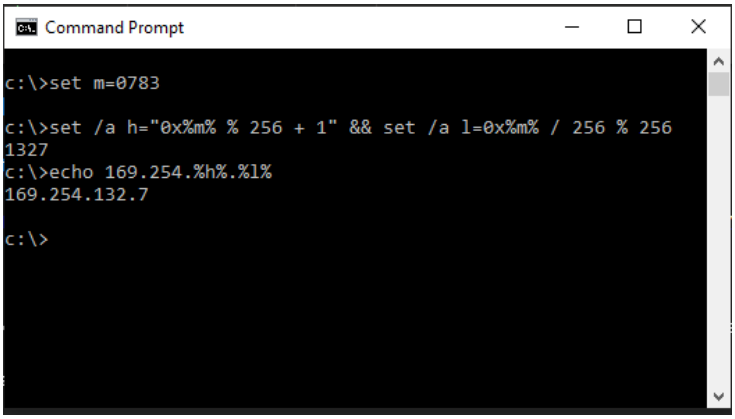
Note: If the browser does not connect, the device may have older firmware. Try again with the following additional steps:

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%



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. This error is expected and can be ignored.

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 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 The Password

At initial login, it is 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 password 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

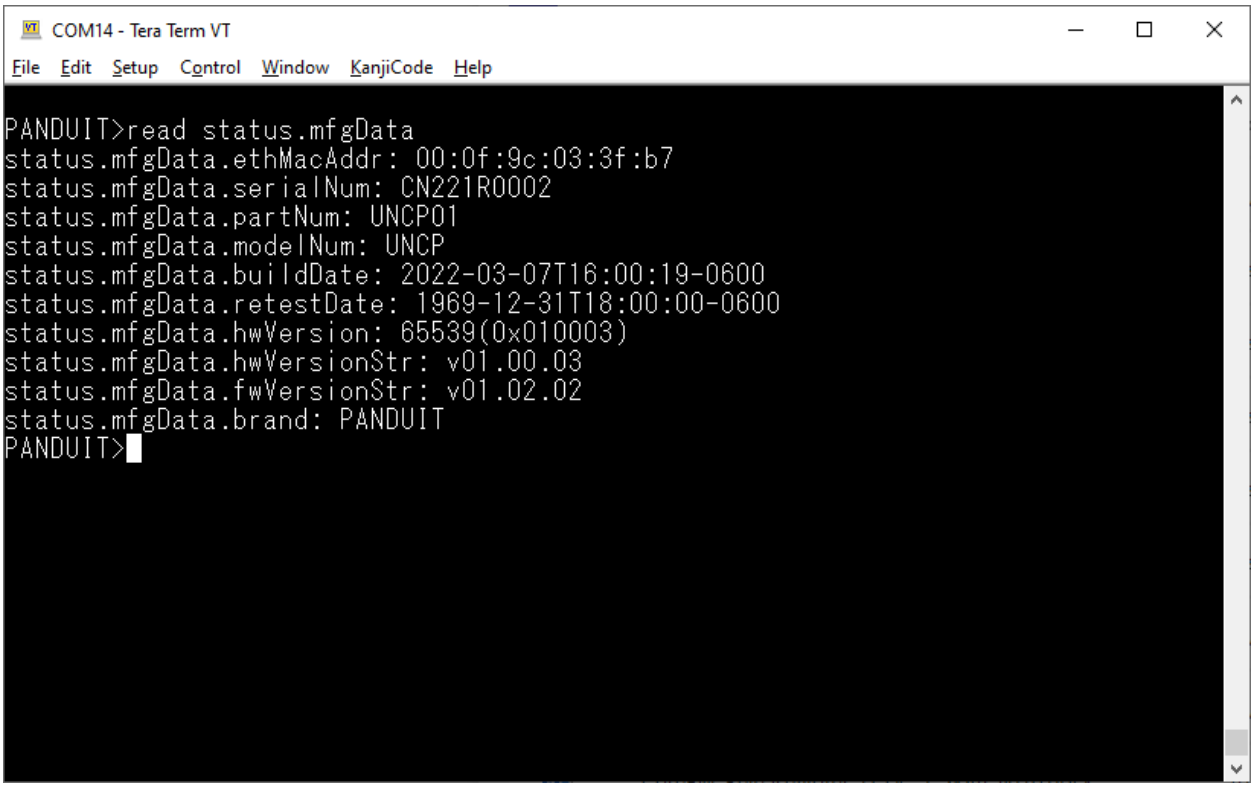
Command list

After logging in 'PANDUIT>' prompt is shown and waiting for commands. Only the 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.

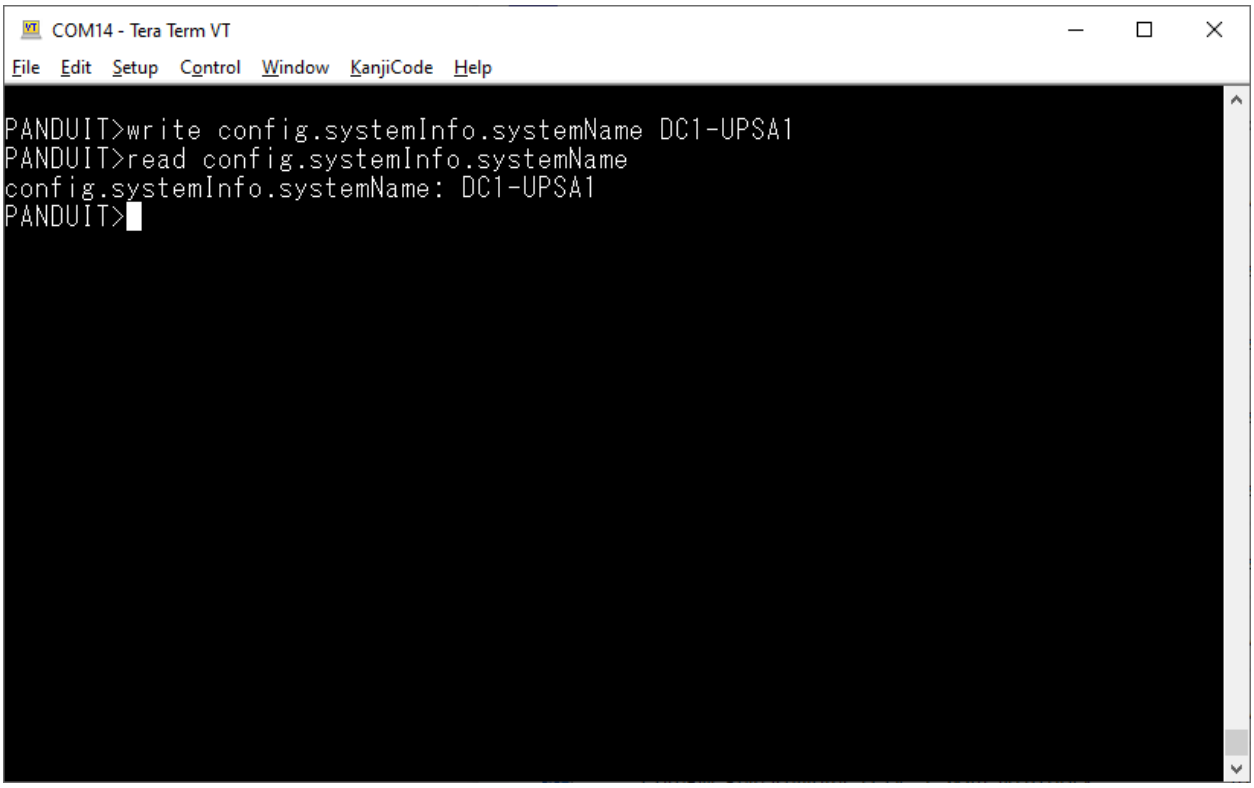
  Example: read status.mfgData



- **write**

  Set a value to an individual item in the data model

  Example: write config.systemInfo.systemName DC1-FMPSA1



- **list**

  List all objects in the data model

- **list *object***

  Display options for an *object* in the data model

- **help, ?**

  Display all command list and usage

- **logout, quit**

  Log out the user

Appendix E: RADIUS Server Configuration

This functionality allows 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 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 security requirements.
    a. User-Role is not specified: (This user logs in as the default “viewer” Role)

```
raduser         Cleartext-Password := "23456789"
                 Service-Type = 1
```

    b. User-Role is set to Admin: (This user logs in as the “admin” Role)

```
radroleadmin    Cleartext-Password := "34567890"
                 Panduit-User-Role = Admin,
                 Service-Type = 1
```

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

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

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

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

7. Verify the server is able to perform authentication and returns the configured User-Role. Note: Users 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 time zone 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 time zone 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.)