PANDUIT
infrastructure for a connected world

Panduit FMPS

User Manual

FMPS Network Management Card

Version 2.0.0

Table of Contents

Section 1 – System Overview

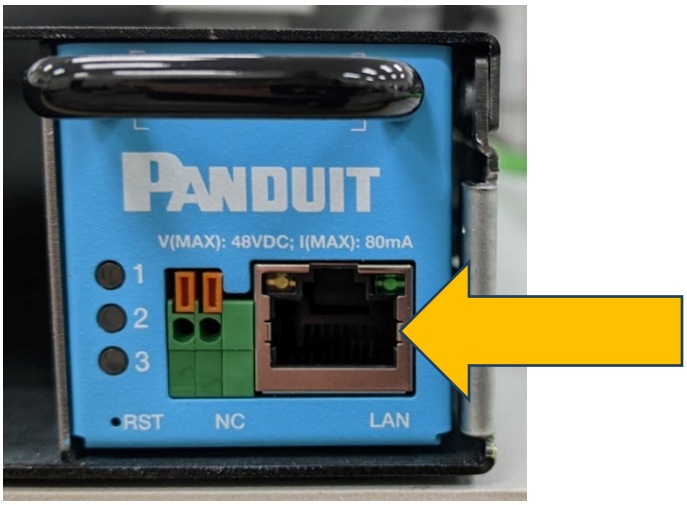
NMC Controller

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.

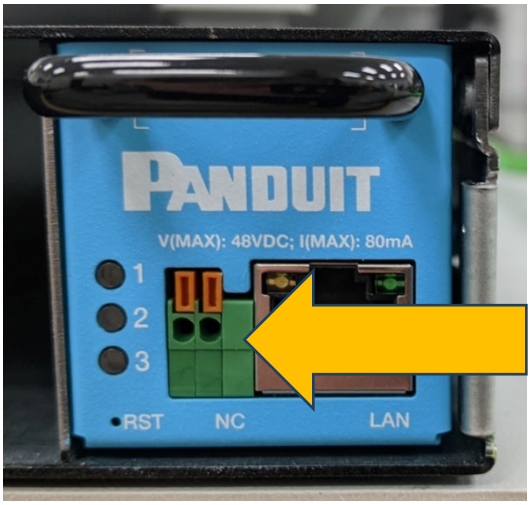
1. Connect an Ethernet cable to the Network port on the NMC.
2. Connect the other end of the cable to the Network port on the switch (or another valid LAN device). A separate VLAN for this solution is recommended.



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 “panduit-fmps-nmc-<macaddress>.local”. For example, “panduit-fmps-nmc-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 FMPS123 system is operating without issue. The contact will **open** when the system is faulted. These contacts are rated for 48/56VDC 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.

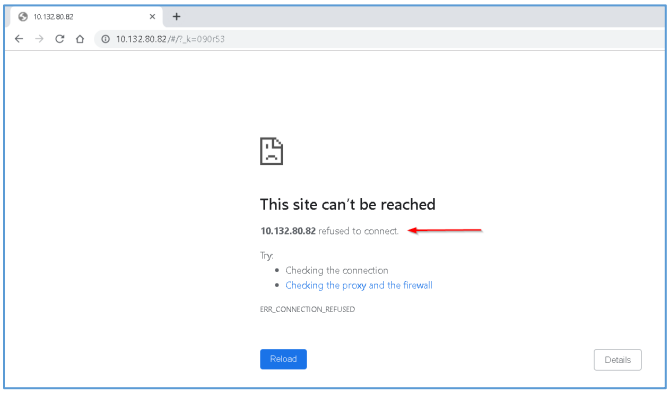
Web Connection

Supported Web Browsers

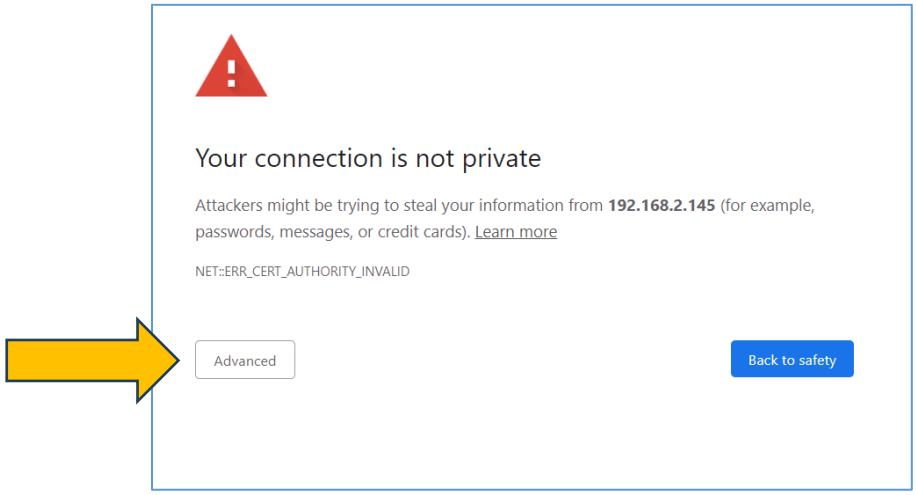
The supported Web browsers are Google Chrome (mobile and desktop), Mozilla Firefox, Microsoft Edge, and Apple Safari (mobile and desktop).

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 you are using the “https://” protocol 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 to factory reset the NMC.

Changing Your Password

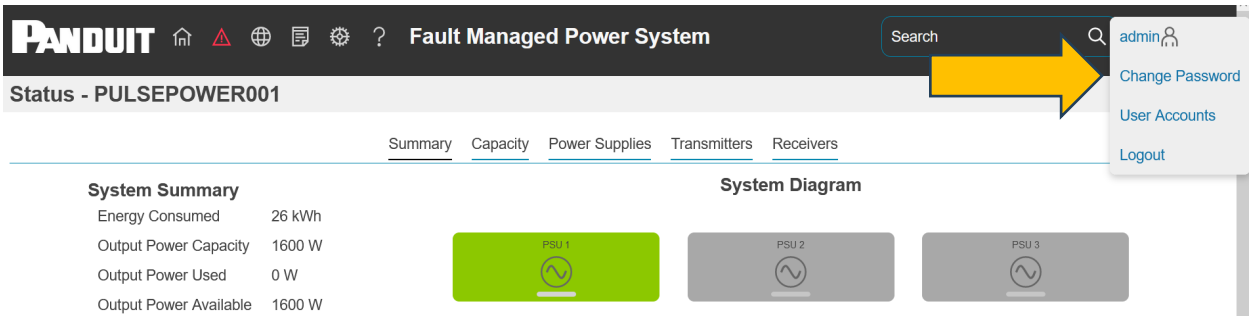
At initial login, you are required to change the default password.

1. Enter the username, current password, and new password twice to confirm. The 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**.

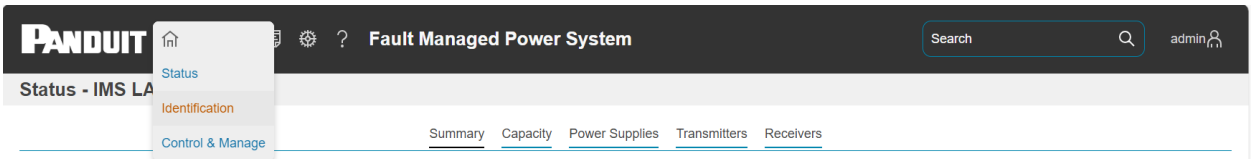


2. The **Change Password** window opens. See this section beginning for details on how to change the password.

Introduction to the Web GUI

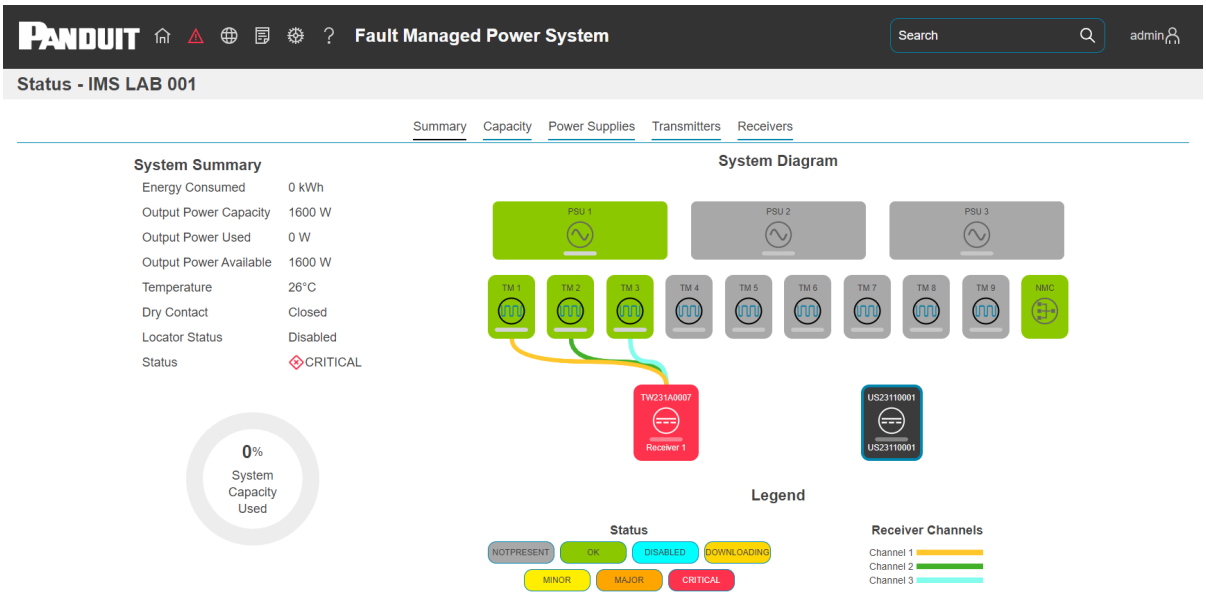
Home

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.

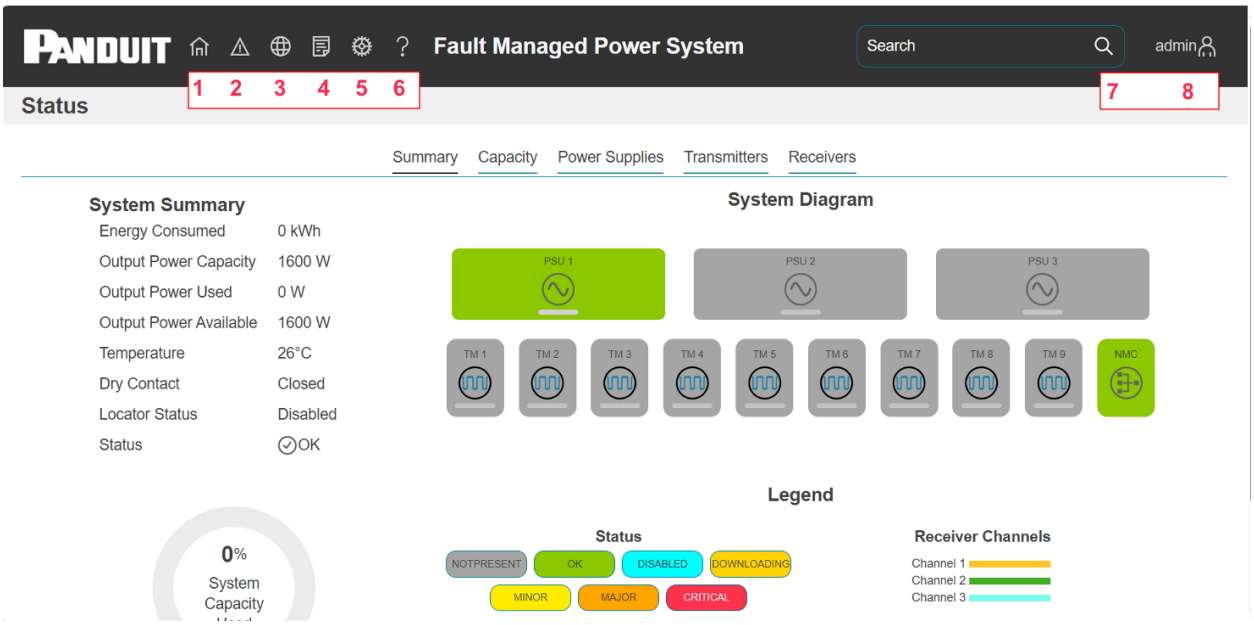


At the top of the screen for the Summary tab, the left pane provides a quick-glance summary of the overall system health, power statistics, and available capacity. Each box represents a module in your system. Consult the color legend on the center-bottom of this screen for information on the colors.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

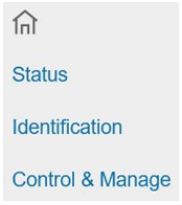


Number	Icon	Description
1		The home icon provides the user with access to an overview of the FMPS via the Status page, an Identification Details page, and Control & Manage functions page.
2		The Alarm icon provides details of the active alarms.
3		This icon lets you select a Language. Available languages: 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 setup the Network Settings, System Management, SNMP Manager, Email Setup, Trap Receiver, User Accounts and Thresholds.

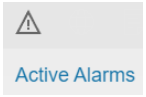
Number	Icon	Description
6		Information about the FMPS can be found using this icon. You can also click user guide and license for additional information about the system.
7		The search icon allows you to input key words and search for the related results.
8		This icon shows who is logged in (user or admin). Account passwords can be changed, and user accounts managed through this page.

Menu Dropdowns

Overview

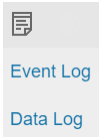


Alarms

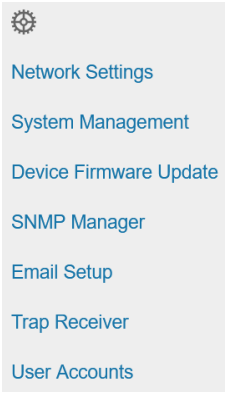


Language

Logs

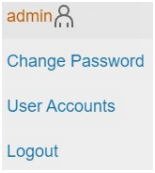


Setting



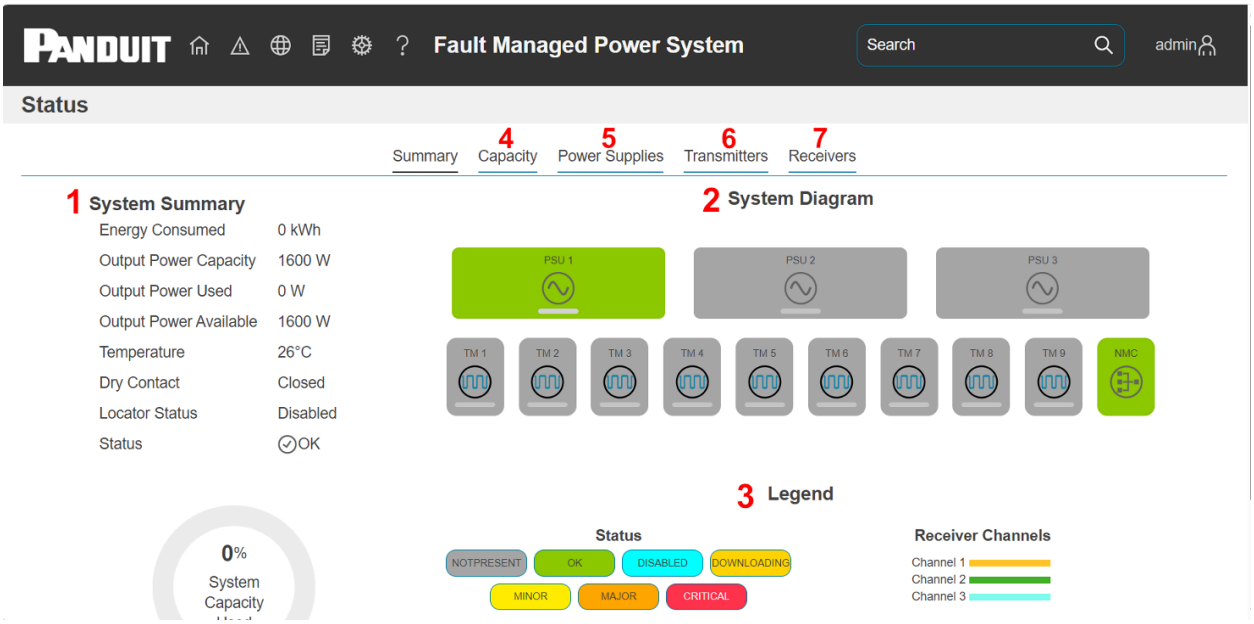
Help

User



Introduction to the Dashboard

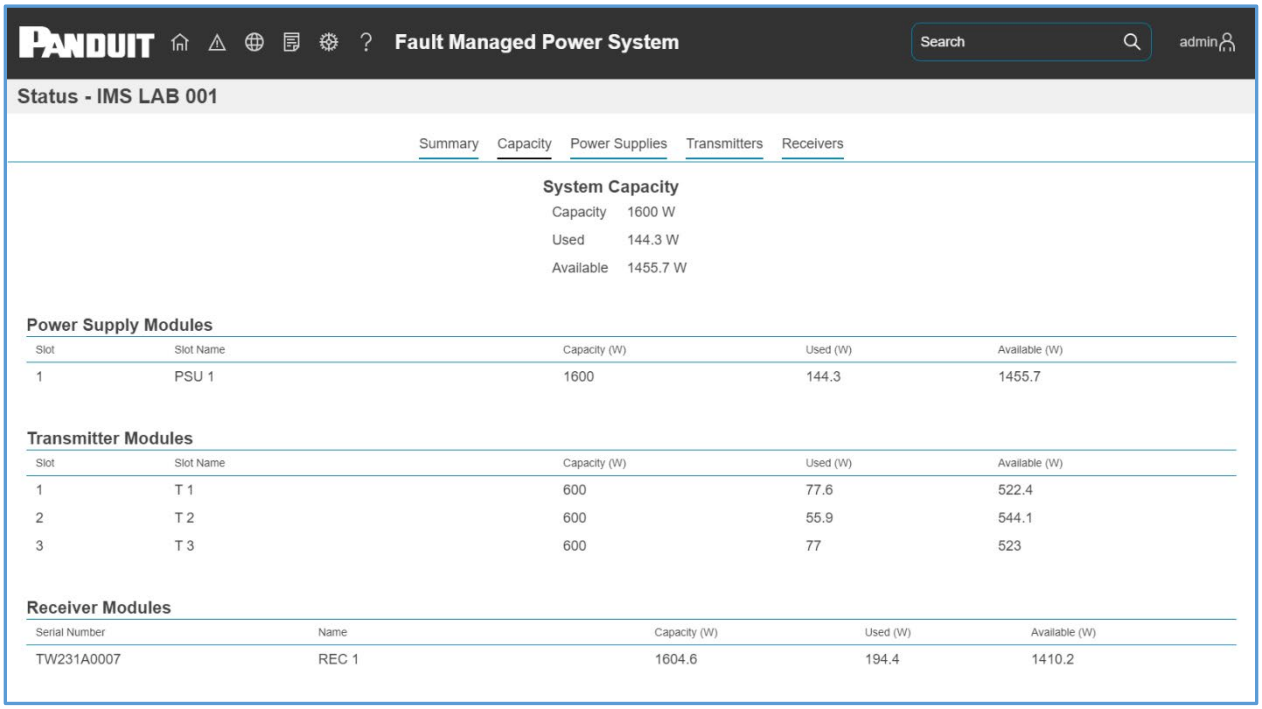
Power Summary Page



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.

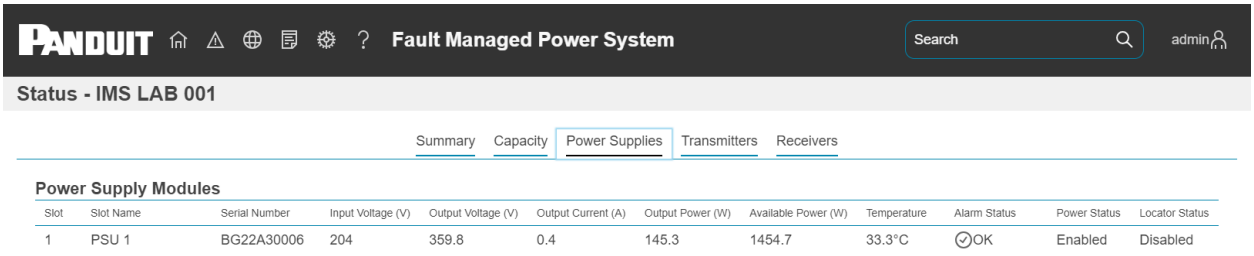
5	Clicking on the Power Supplies tab brings up a detailed view of the power supplies.
6	Clicking the Transmitter tab brings up a detailed view of the Transmitters of the system and how they are performing.
7	Clicking the Receivers tab brings up a detailed view of the Receivers of the system and how they are performing.

FMPS Capacity Page



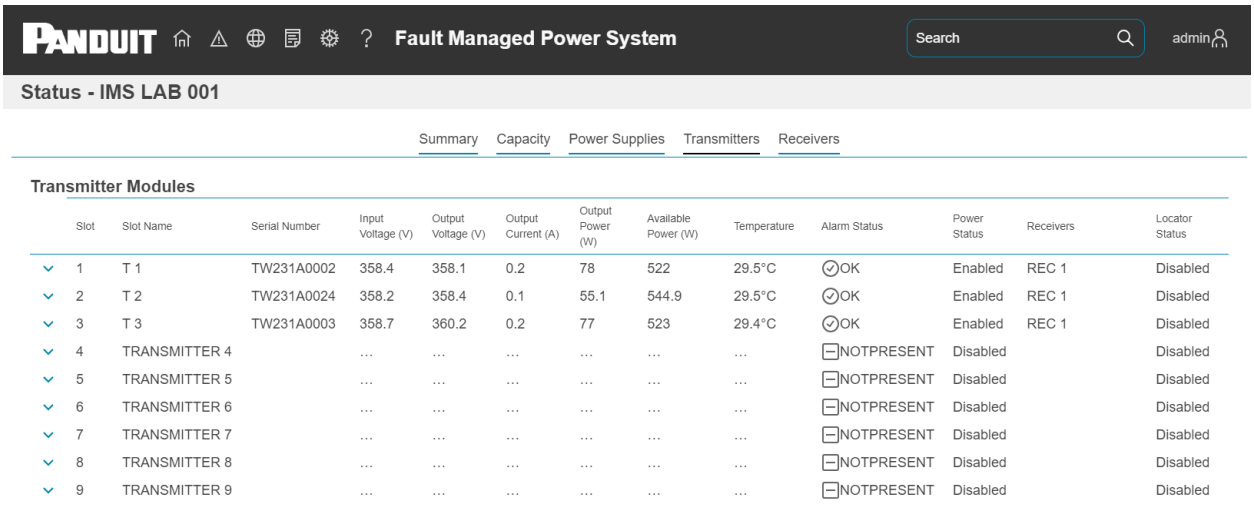
This page shows the system power capacity (total available), how much of this capacity is being used, and available power for edge devices (in watts). It also provides power details on each part of the system which includes the Power Supplies, Transmitters, and Receivers.

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.

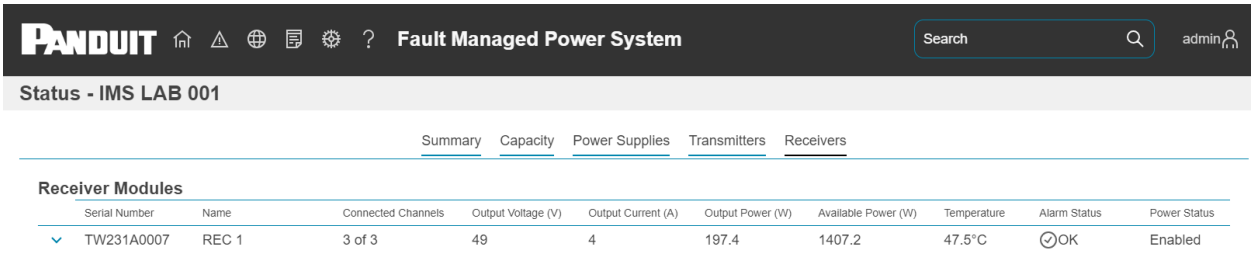
Transmitter Page



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 bottom LED on the Transmitter.

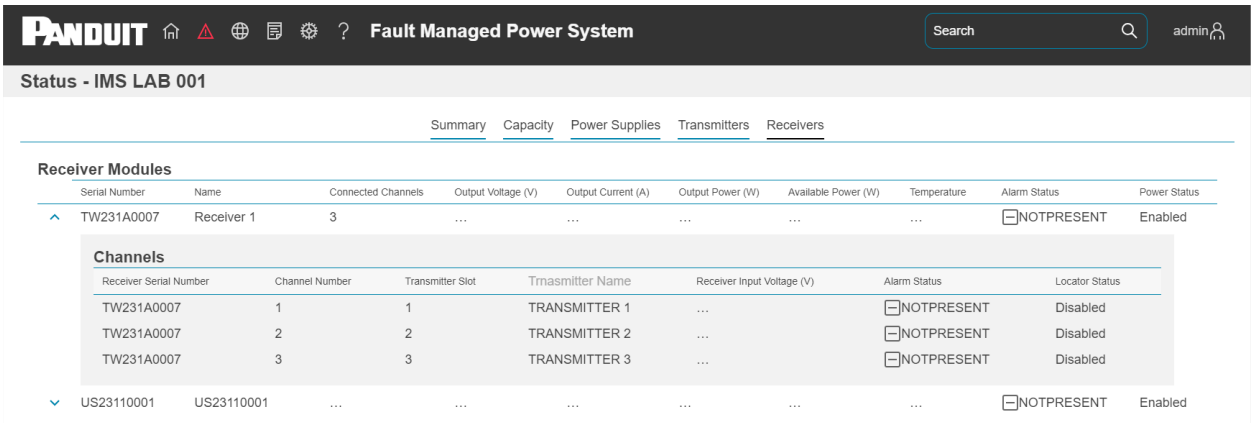
Receiver Page



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, and power status.

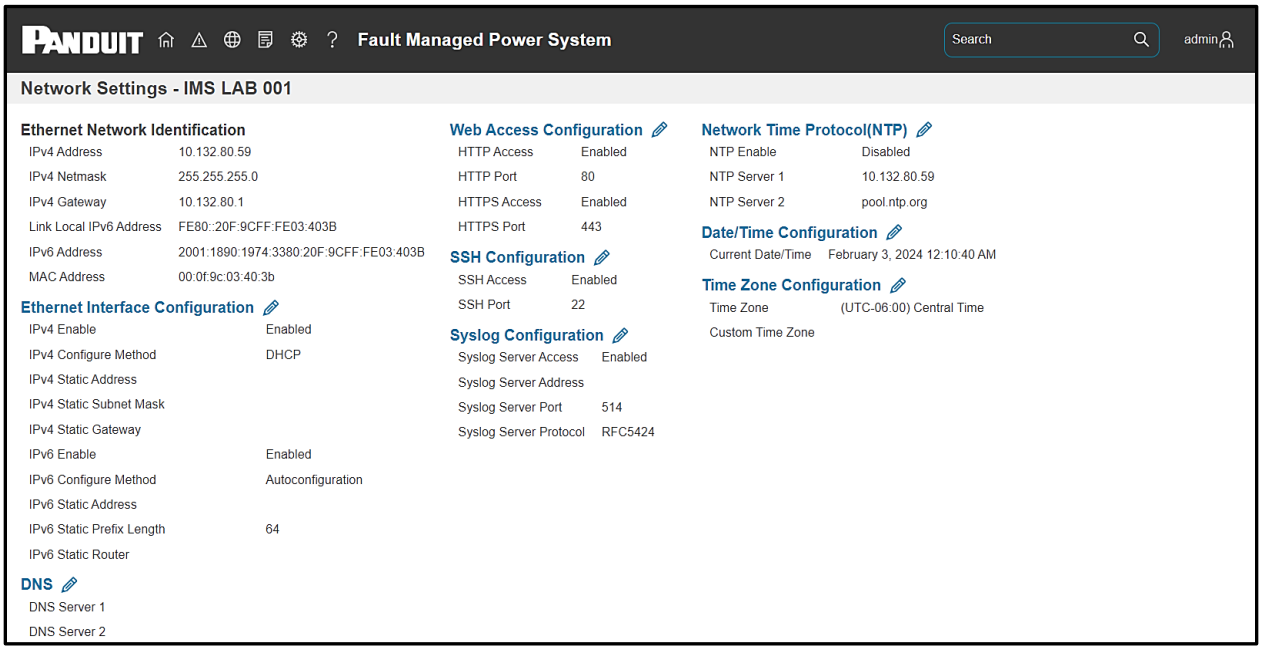
Alarm status options are OK (no alarms) and NOTPRESENT. The power status will normally show as enabled but can be disabled via the control page for maintenance work. A disabled Receiver will not deliver output power to the load.

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

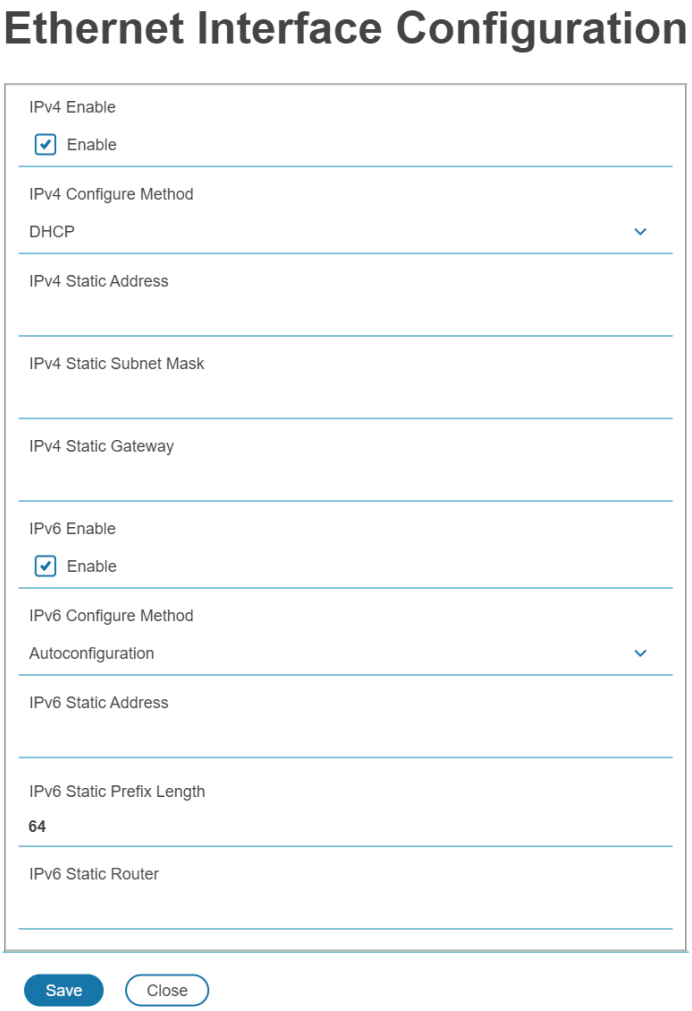


Network Settings

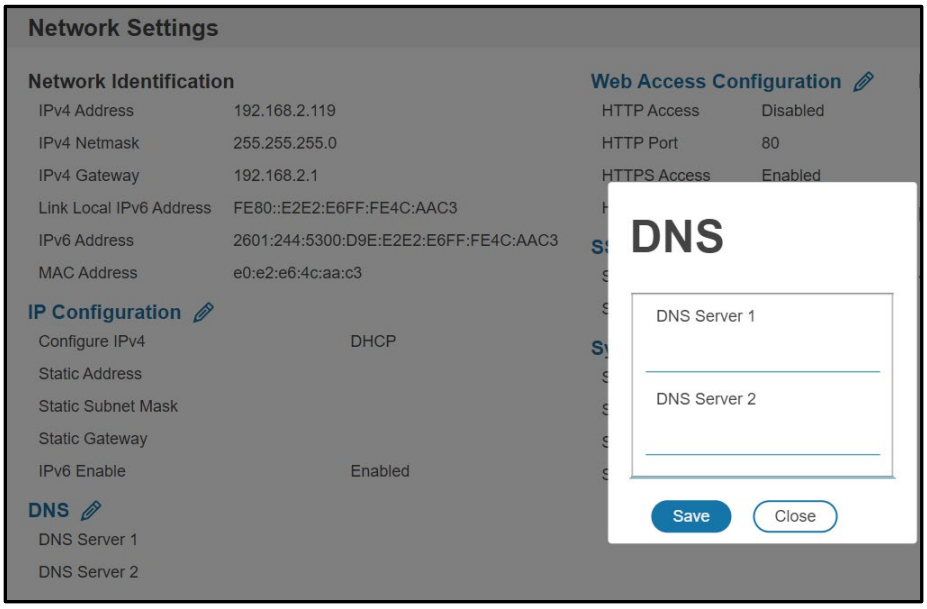
The Network Settings allow management of IP Configuration, DNS, Web Access, SSH Configuration, Syslog Configuration, Network Time Protocol (NTP), Date/Time Configuration, and Time Zone Configuration.



Ethernet Interface Configuration:

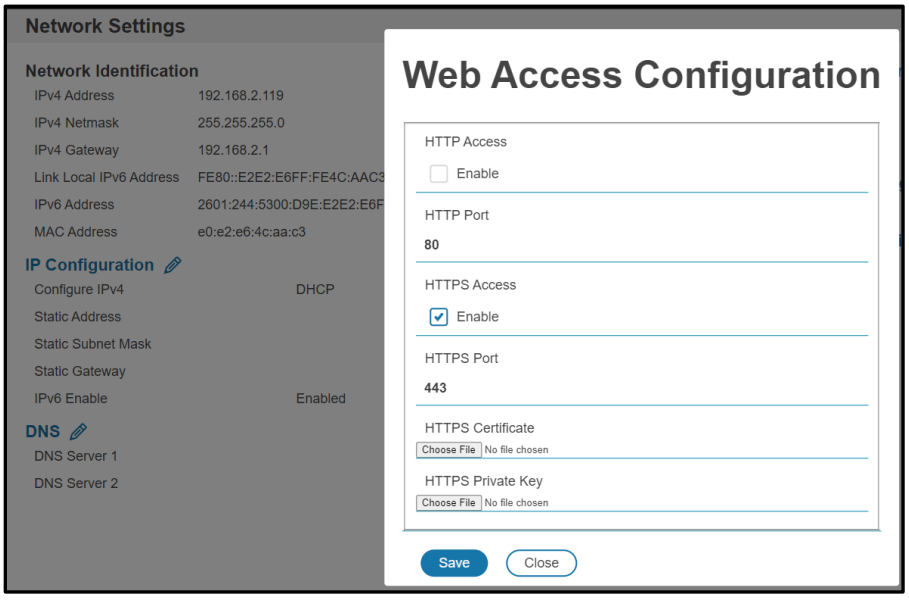


DNS configuration:

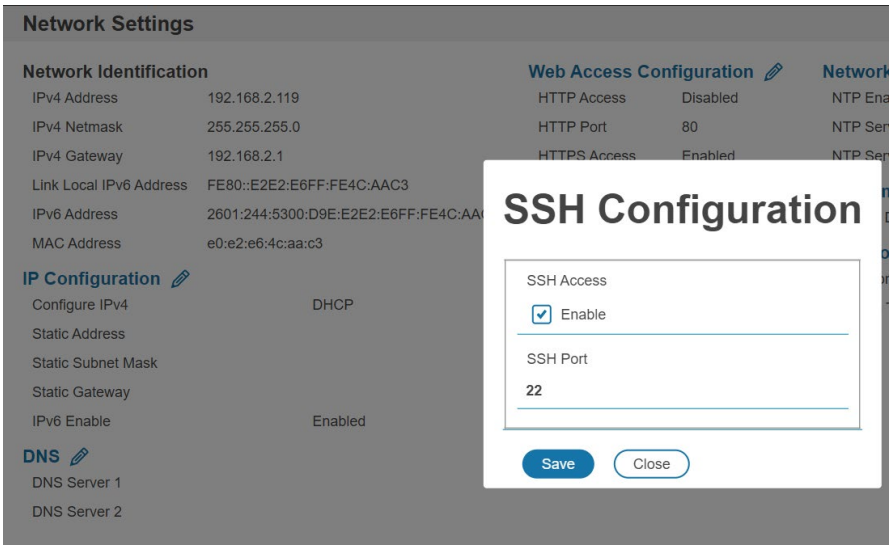


Web Access Configuration

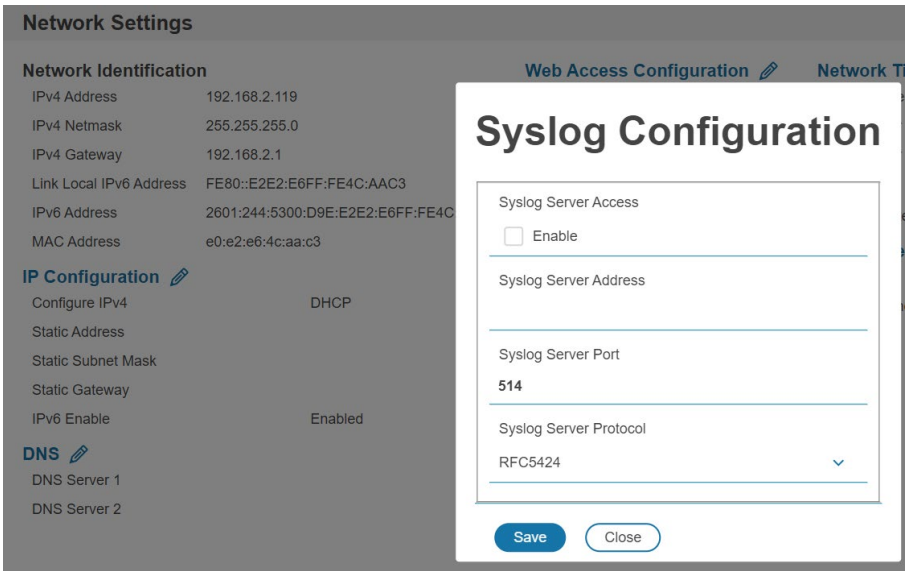
Web Access Configuration is used to set HTTP and HTTPS. Also, this section will be used to upload HTTPS Certificates.



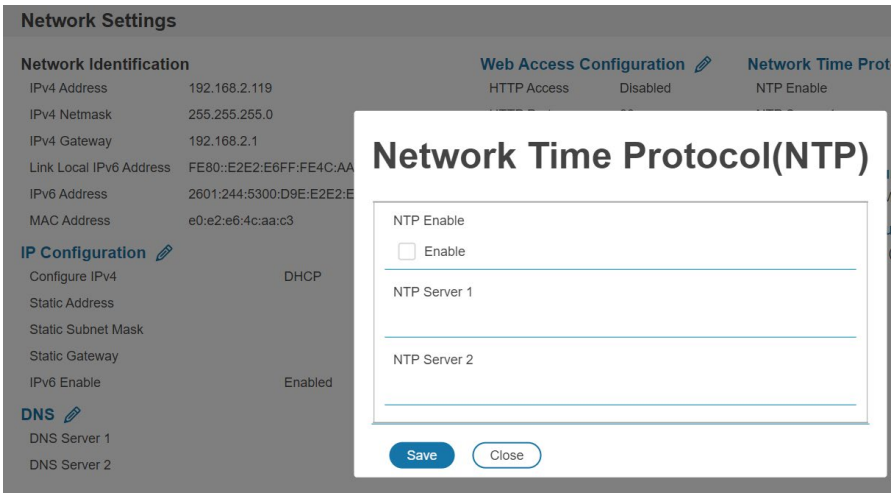
SSH Configuration:



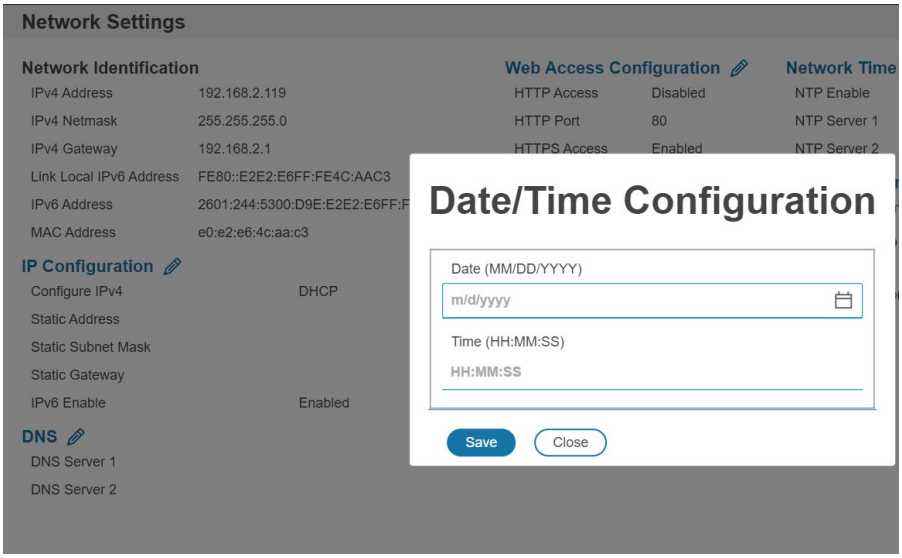
Syslog Configuration:



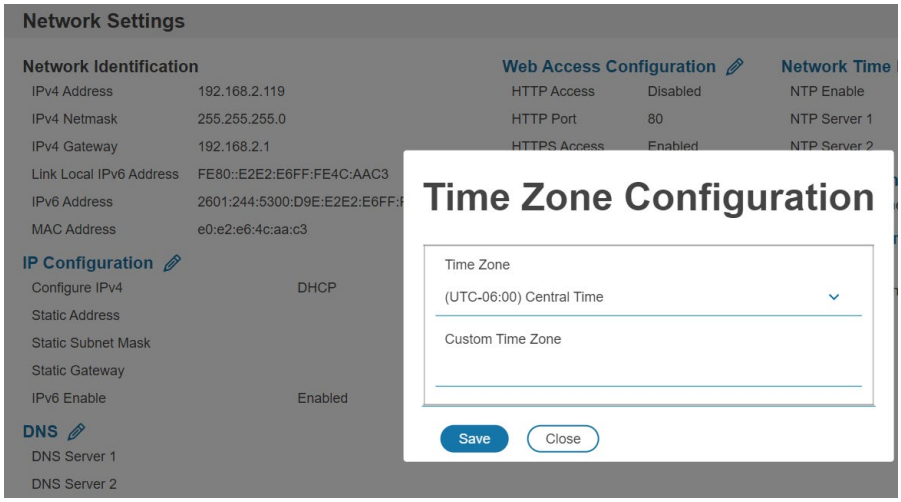
Network Time Protocol (NTP)



Date/Time Configuration:



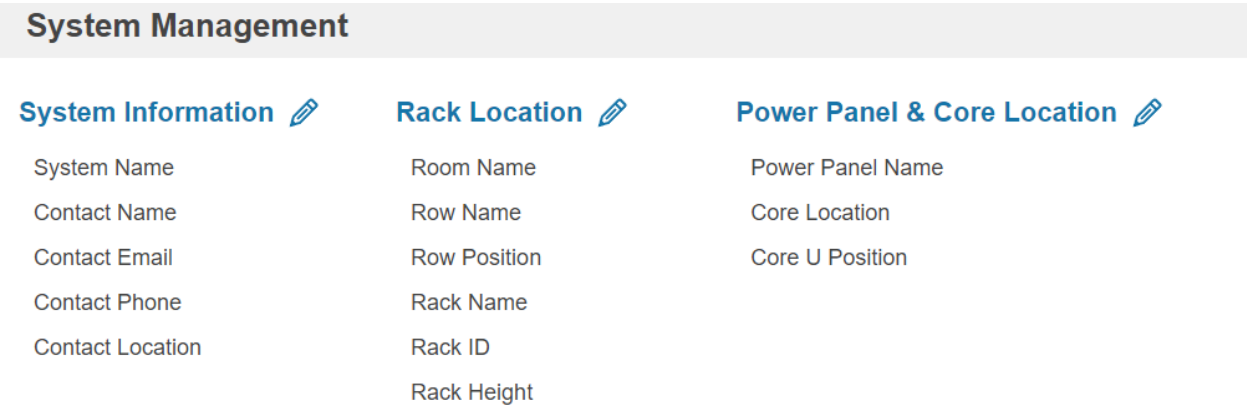
Time Zone Configuration:



System Management Information

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

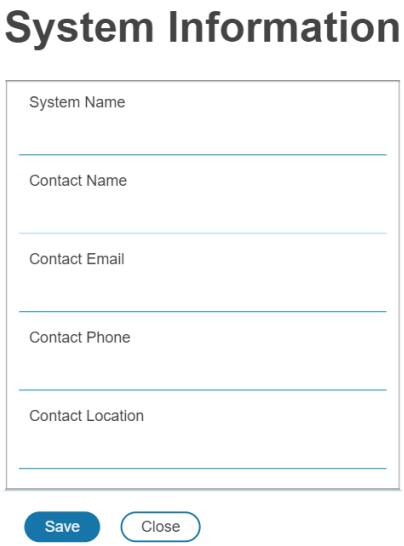
To configure the system management information, select **System Management** under the **gear** icon.



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.**

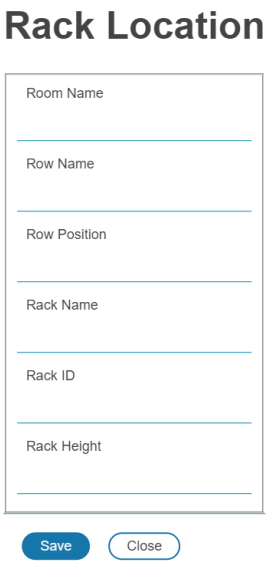


2. Enter the **System Name**
3. Enter the name of the person who should be contacted if there is a problem with the system into the **Contact Name** section.
4. Enter the email of the contact person into the **Contact Email**.
5. Enter the phone number of the contact person into **Contact Phone**.
6.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

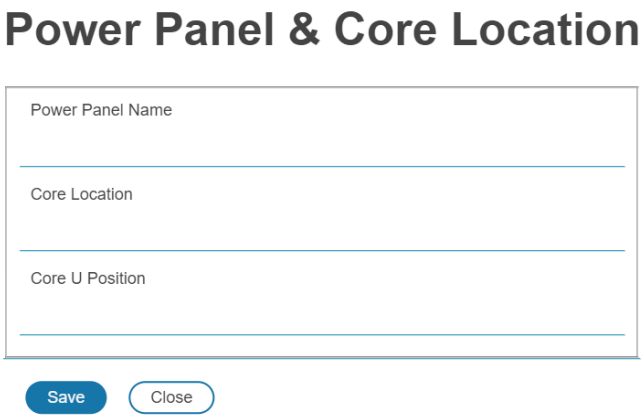


2. Enter the room location of the rack or cabinet that contains the NMC system into **Room Name.**
3. Enter the **Row Name** where the NMC is located.
4. Enter the position of the row where the NMC is positioned in **Row Position**.
5. Enter the ID of the rack/cabinet where the NMC is located into **Rack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



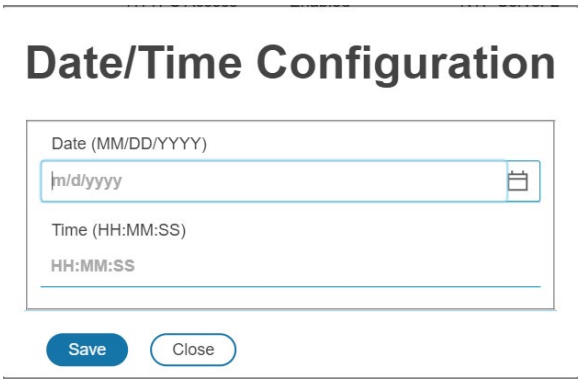
2. Enter the name of the NMC in the **Power Panel Name**.
3. Select **Front** or **Back** for the **Core Location.** The **Core Location** is the side of the rack/cabinet where the NMCs are installed. For vertical NMCs, they are typically installed in the back.
4. Enter the rack unit (RU) location into the **Core U Position**. Vertical NMCs are usually installed in the 0 RU space.
5. Press **Save**.

Setting Time and Date on the NMC

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

Manually Setting Time and Date

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



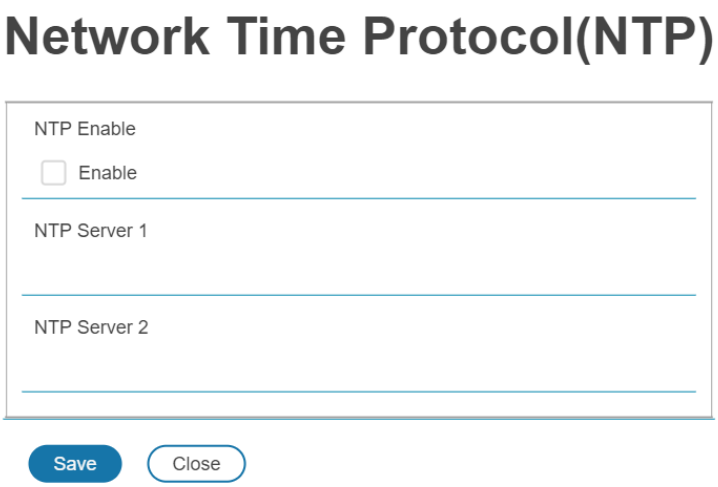
2. Enter the date using the MM/DD/YYYY format or use the calendar icon to select a date.

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 **Network Settings** and select **Network Time Protocol** (NTP).



2. Click **Enable** to enable NTP.

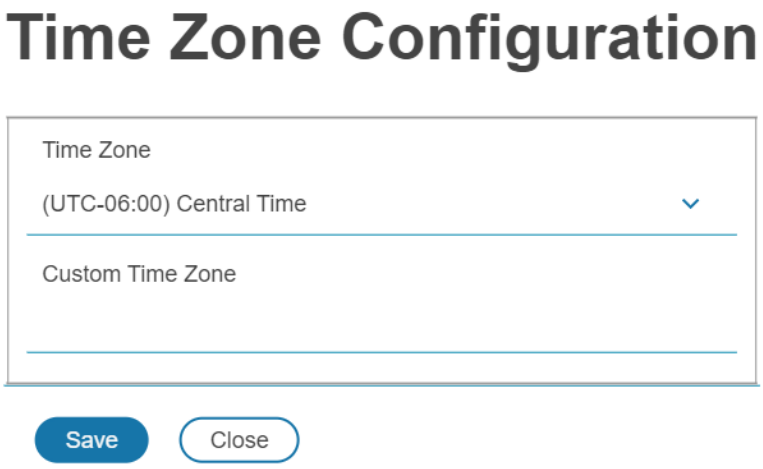
3. Enter the hostname or IP address of the primary NTP server in the **Primary NTP Server** field.

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 **Network Settings** and select **Time Zone Configuration**.

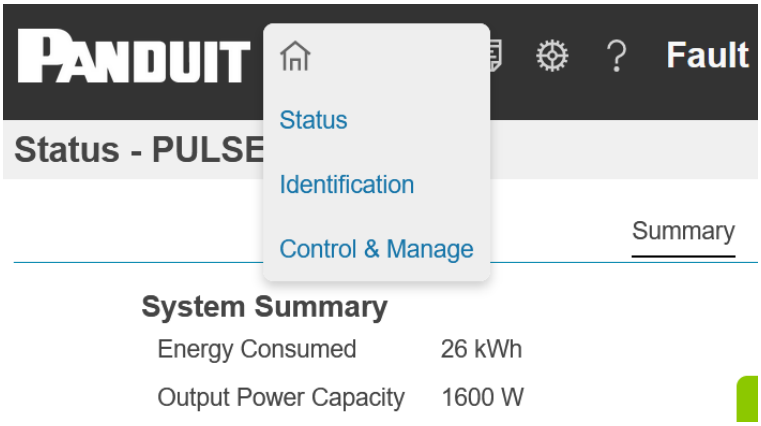


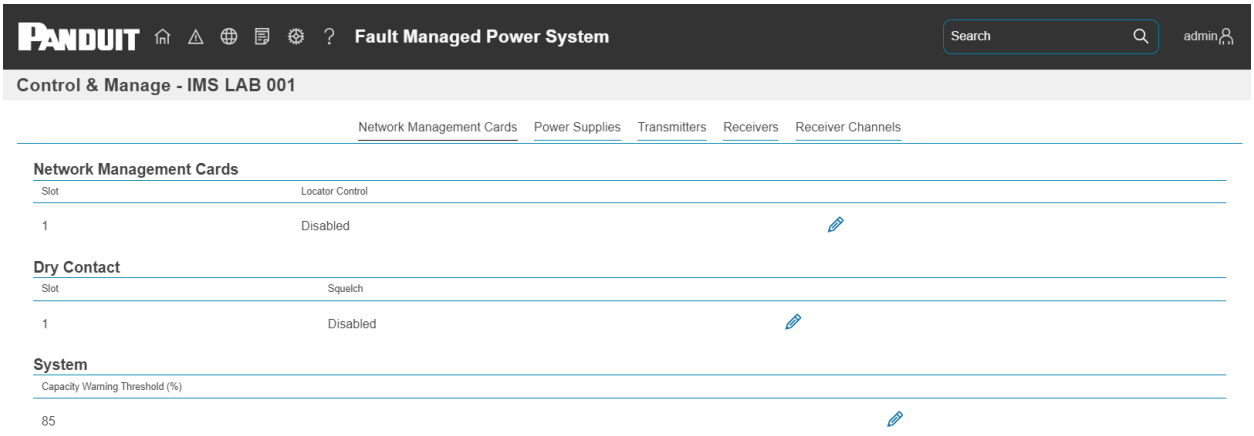
2. Select a predefined time zone from the pull-down menu.
3. If the desired time zone is not in pull down menu, enter the POSIX time zone in the **Custom Time Zone**:
   - The POSIX format is local_timezone,date/time,date/time.
   - For more information on the POSIX time zone formats see Appendix F: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





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

*Network Management Cards

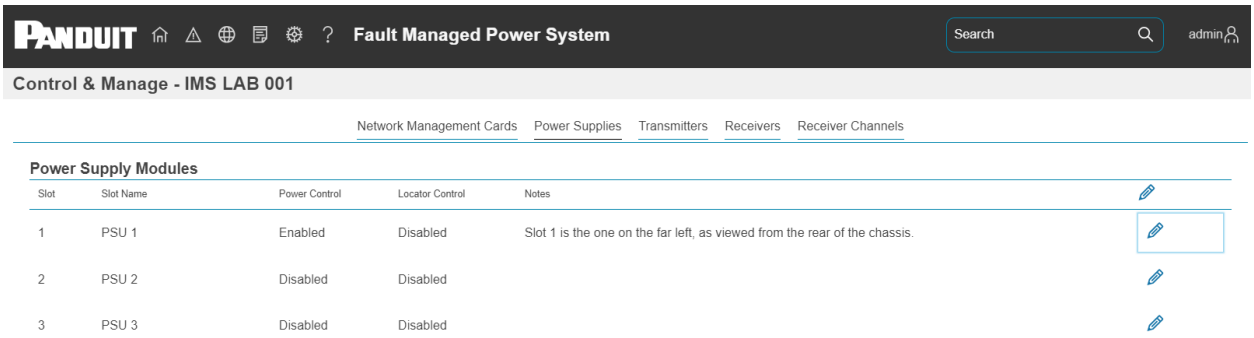
*Power Supplies

*Transmitters

*Receivers

*Receiver Channels

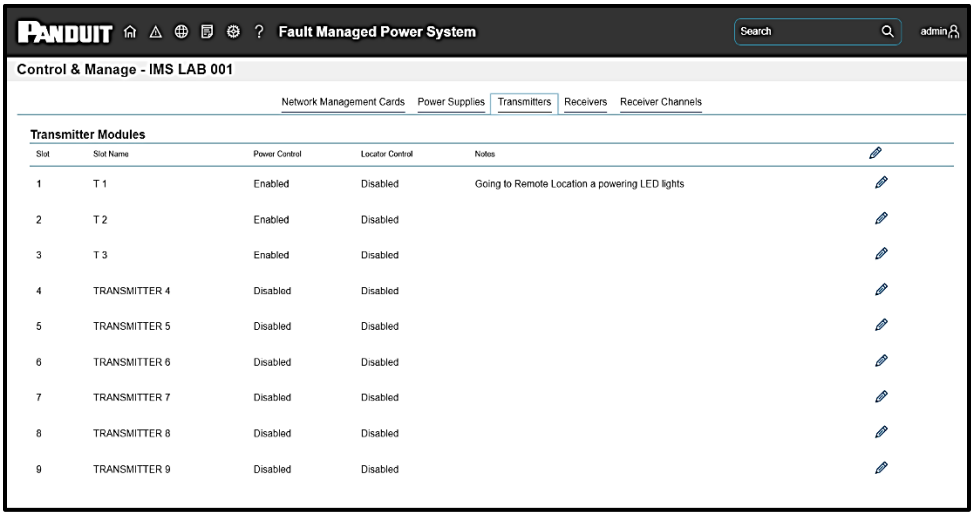
The “**Network Management Card” tab** allows you to activate the locator function on the NMC (flashing the bottom LED on NMC module), allow or ignore the Dry Contacts, and set the System Capacity Warning Threshold (%). Click the pencil icon to modify settings and select Save or Close when done.



The **"Power Supplies" tab** allows you 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.

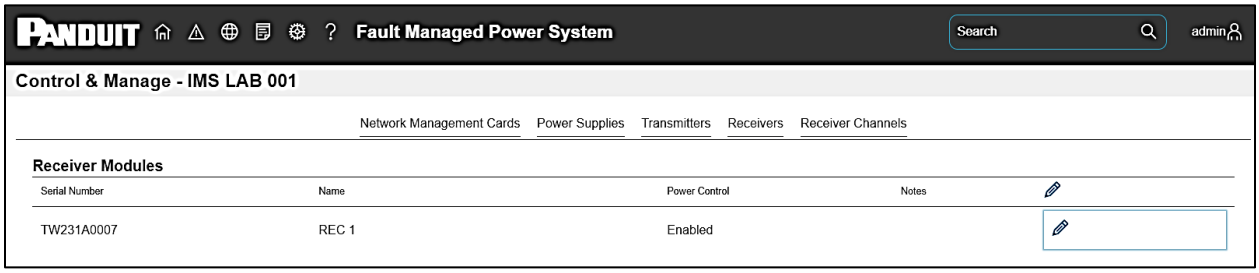
The locator control feature will blink the rear left LED on the Supply, making this Supply stand out from others installed. Select the pencil icon to edit the setting(s) then click on Save or Close when completed.



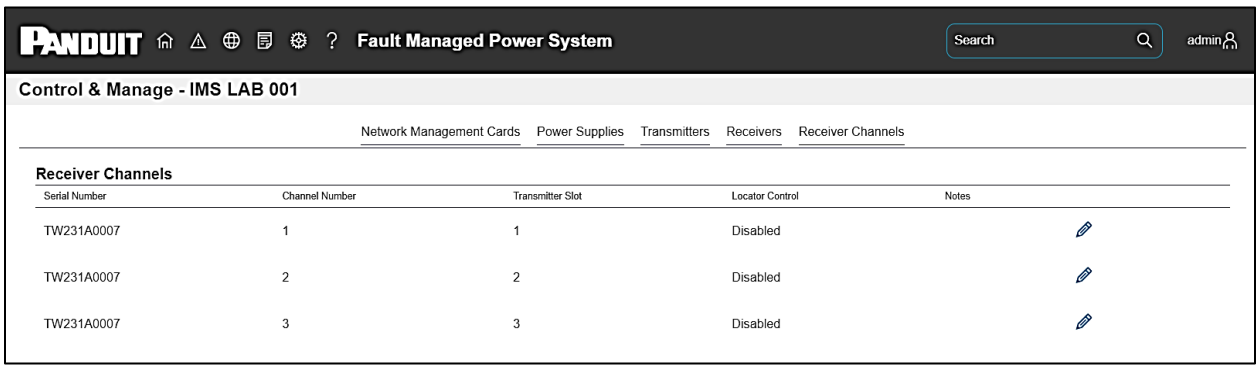
The **"Transmitters" tab** allows the user to customize the Transmitters name, enable/disable the Transmitter, activate the locator control feature, and provide a detailed note about the Transmitter. It is a best practice to disable a Transmitter before performing work on the cabling system connected to it.

The locator control function can be used to flash the bottom LED on the Transmitter 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.



The **“Receivers” tab** of the Control & Manage page allows the user to modify the name of the Receiver, enable or disable output power, and record a custom note regarding this Receiver. Best practice is to record the device(s) being powered by the Receiver and the typical load of these device(s).



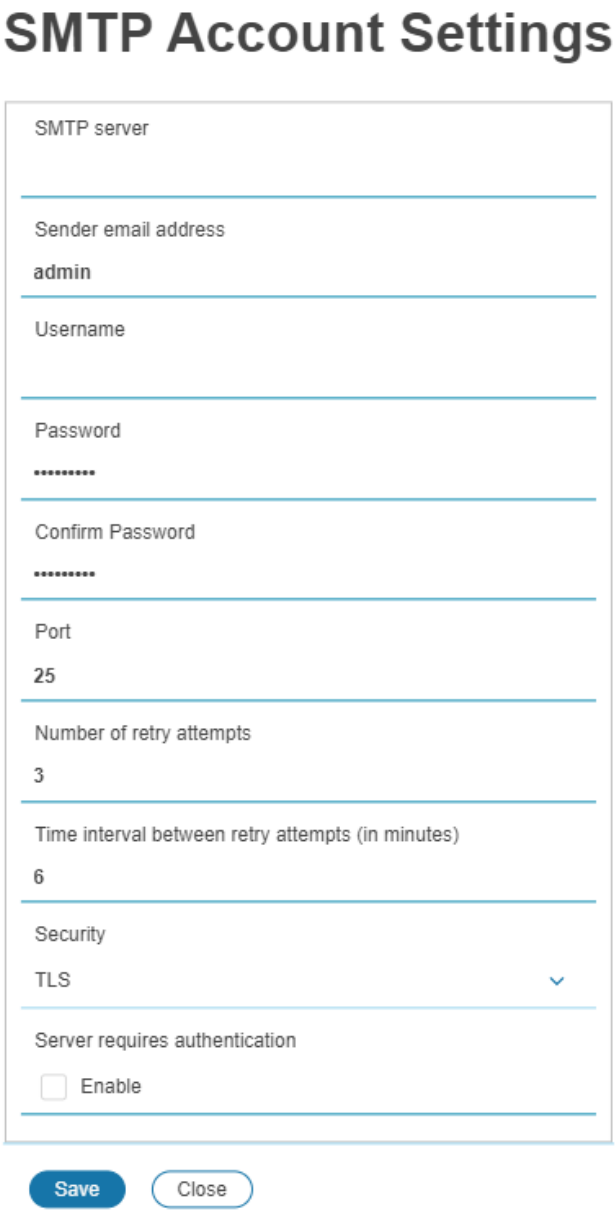
The **“Receiver Channels” tab** of the Control & Manage page allows the user to activate the Locator control feature for each channel and record a custom note about each channel.

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 Setup**.

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



- Set the **SMTP server**. This is the address of the SMTP relay server that is going to accept the messages.
- Set the **Sender email address.** This is the email address from which the email is sent. You could use a unique email address on each FMPS or the same email address across all FMPSs.
- Configure the **Port** number. The port number is the communication

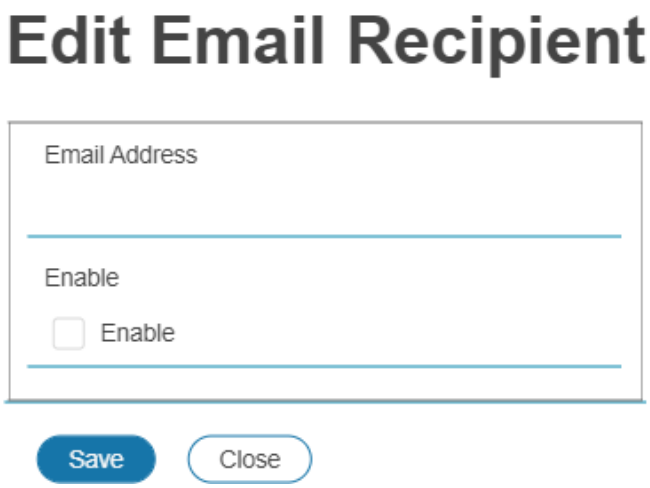
endpoint on the server. The default is 25. Other common SMTP ports are 587 and 465.

- 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.

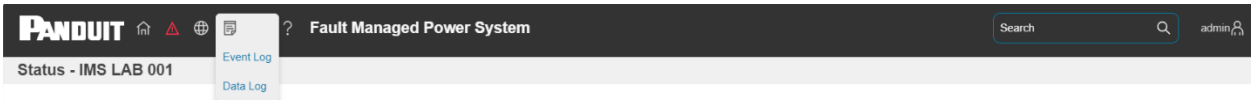


2. Enter the desired email address and press **Enable**.
3. Press **Save**.

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

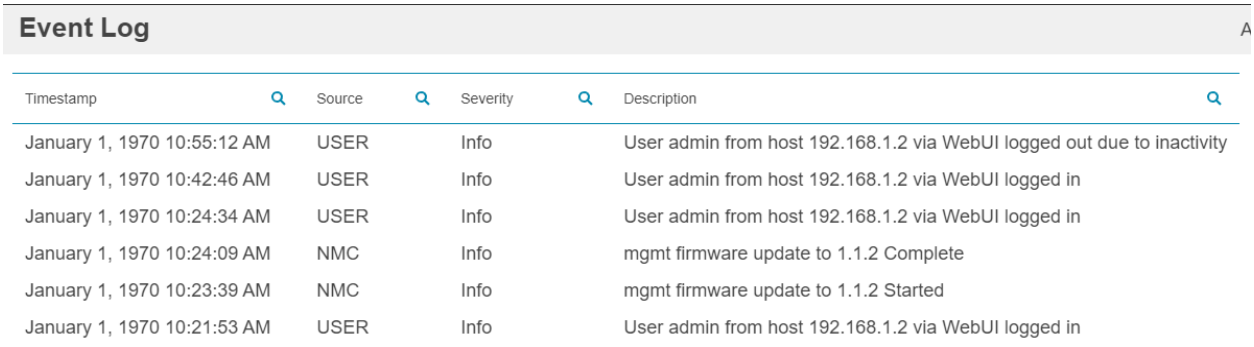
Logs

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.

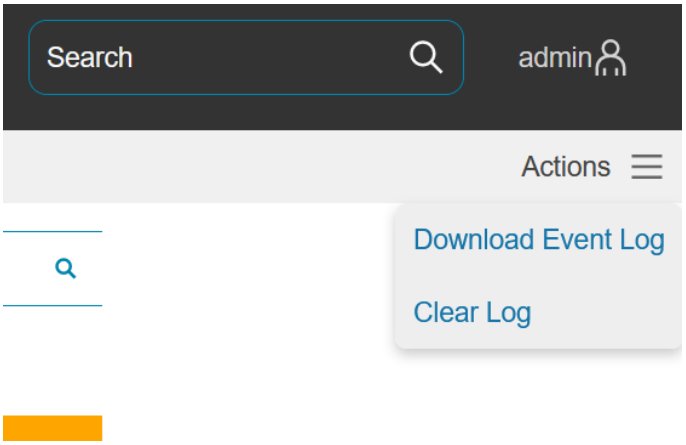


Event Log

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



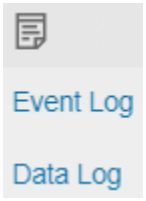
Event log can be downloaded or cleared from the Actions menu.



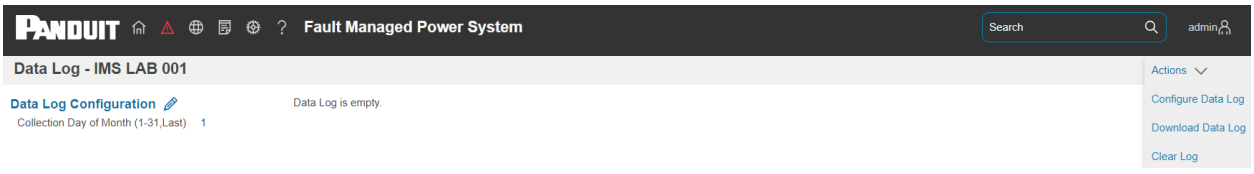
Data Log

The period visible in the data log at any one time depends on the time between data log entries. The time range of each record can be configured from 1 to 1440 minutes. (As an example, if a data log is in an interval of 60 minutes, the entire data log contains 1000 records with up to 41.67 days of data.) Once the data log reaches the maximum of 1000 records, the oldest entries are overwritten by the newer entries.

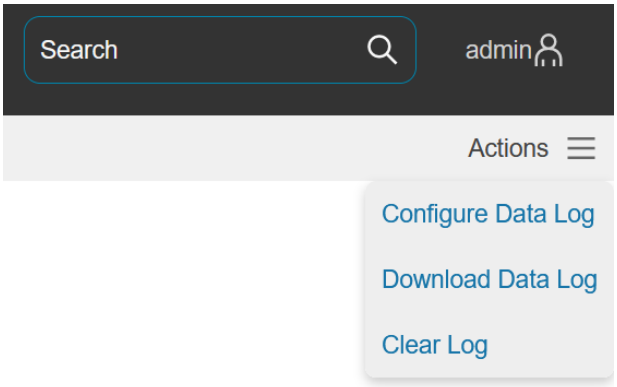
1. Go to **Logs** and select **Data Log**.



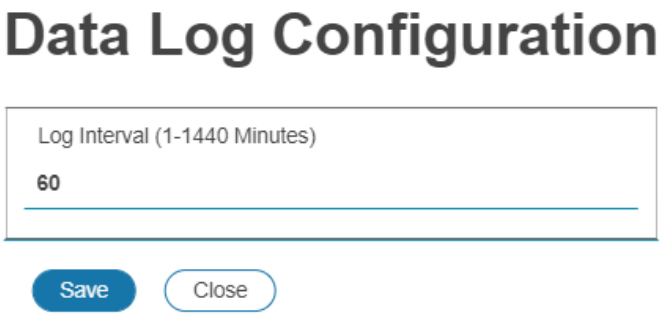
Features are accessed from the Actions dropdown menu and include: Configure Data Log, Download Data Log, and Clear Log.



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



3. **Enable** must be selected and enter an interval number in the **Log Interval** field. (Valid range is from 1 to 1440 minutes. The default time is 60 minutes.)



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

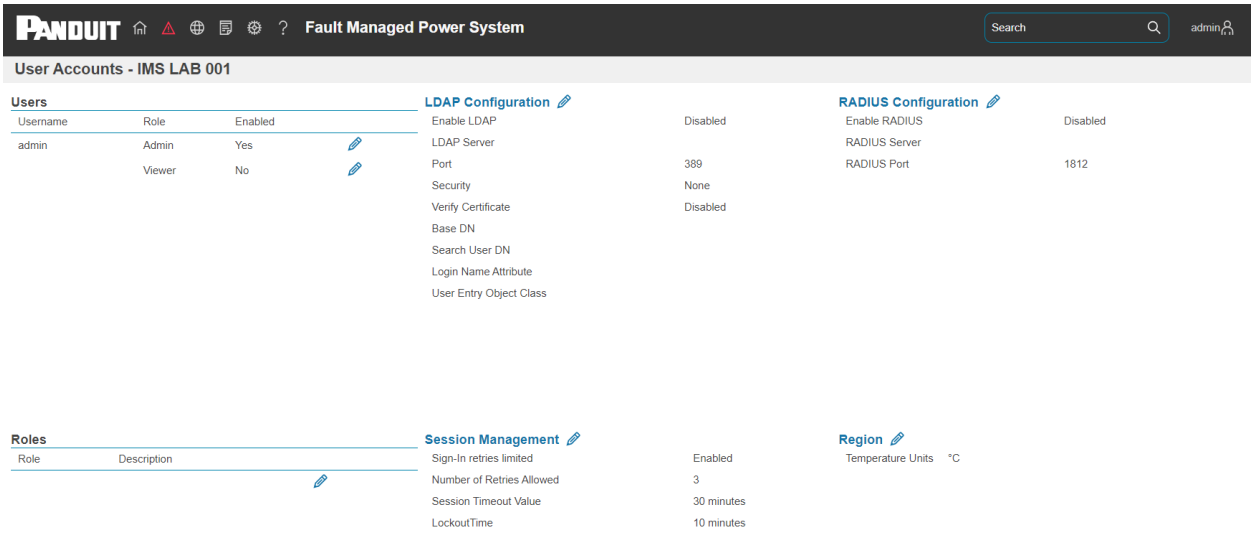
The FMPS comes with an **Admin, Controller,** and **Viewer** profile. The **Admin** role is typically the system administrator and has the Administrator Privileges with full operating permissions. The **Viewer** role is a Read Only profile. All other users must

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.**

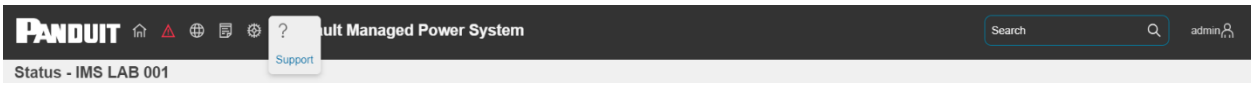
Change Password

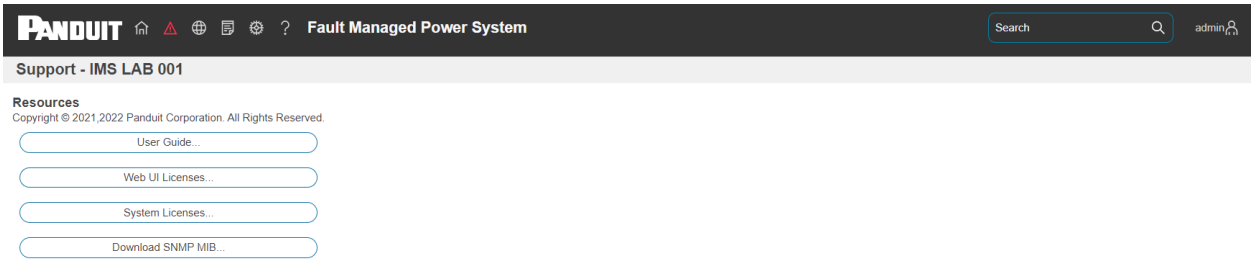
The Change Password feature can be used to modify the password used to access the system's user interface. At the Change Password screen, enter the required information, then click on Log In.

Help

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

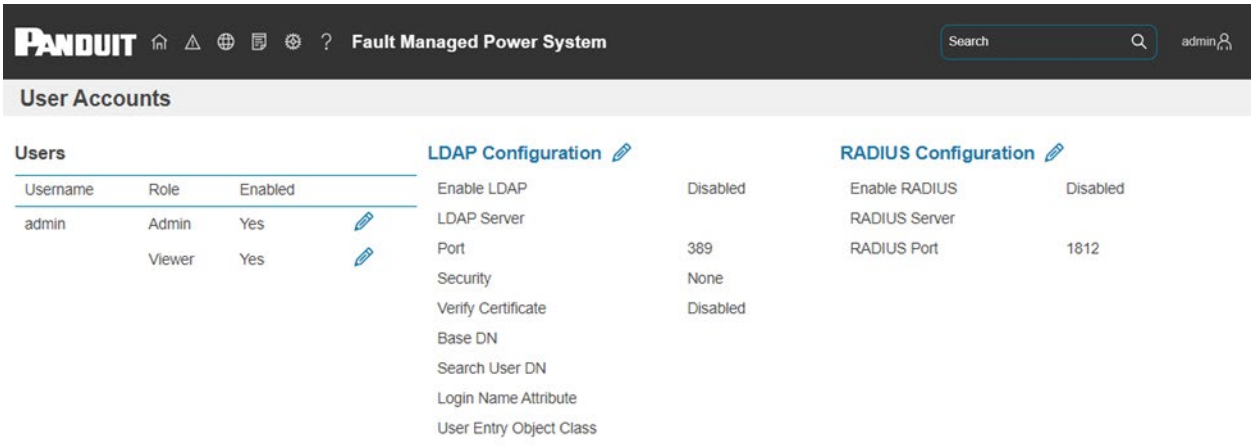
- User Guide
- Web UI Licenses
- System Licenses
- Download SNMP MIB



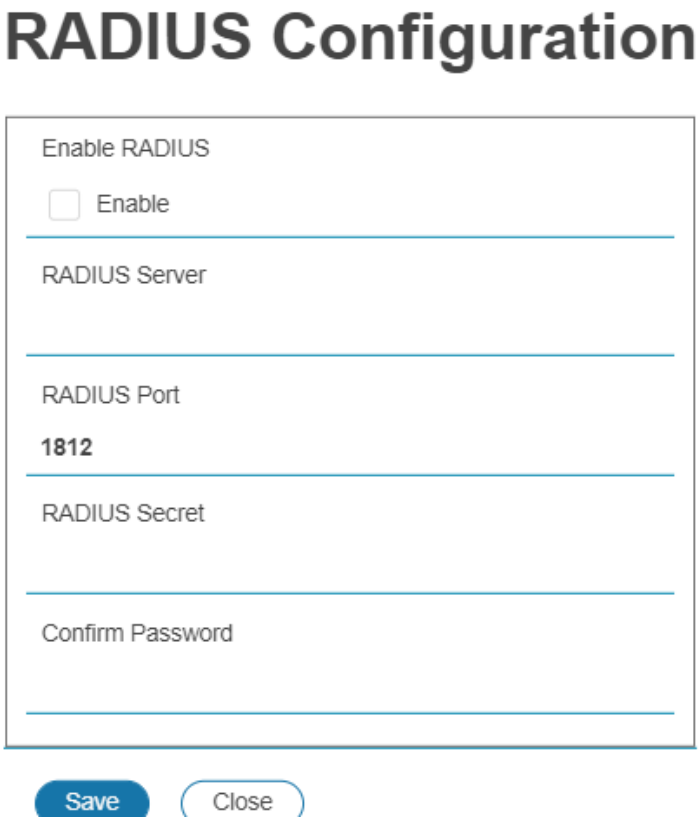


Setting Up the System for RADIUS Authentication

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 your Radius authentication is complete.

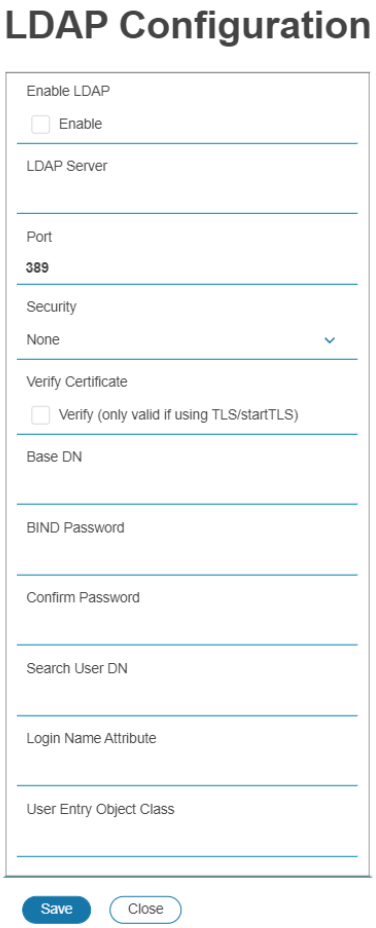
   Note: By default, a RADIUS user will have the “viewer” Role if one is not specified. The administrator of the RADIUS server may configure a Panduit vendor (19536) dictionary, with a “User-Role” integer attribute set to User (1) or Admin (2) or Control(3). For complete details, see Appendix E: RADIUS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

Configuring the system with LDAP Server Settings

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

1. Go to User Accounts (under 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.

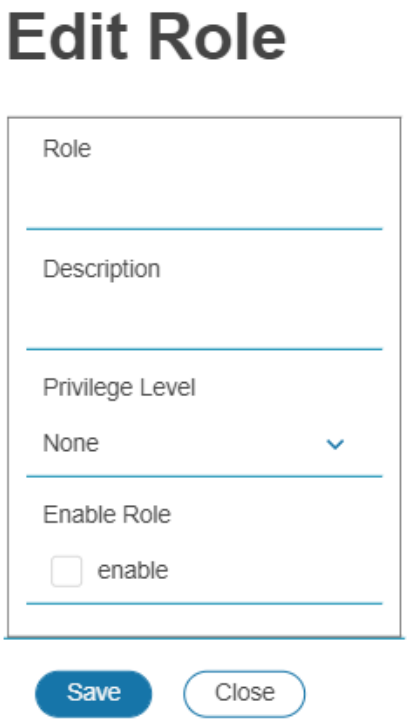


Once LDAP is configured, the FMPS must understand for which group authentication occurs. A role must be created on the FMPS to reference a group within the Active Directory (AD).

1. Within the Active Directory, create a group for the users that you 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).



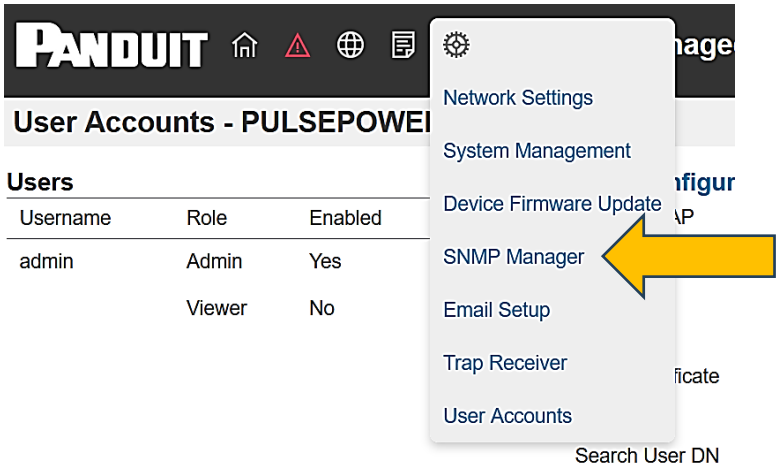
4. LDAP authentication is ready to use.

Section 3 – Simple Network Management Protocol (SNMP)

SNMP Management Configuration

Setup SNMP

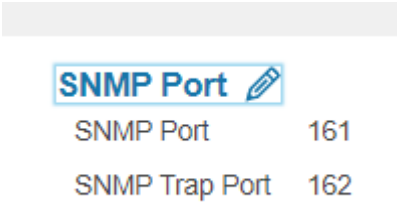
1. Access the Web interface and login.
2. Under SNMP Managers, select SNMP General (or type SNMP in the search). The SNMP General page displays.



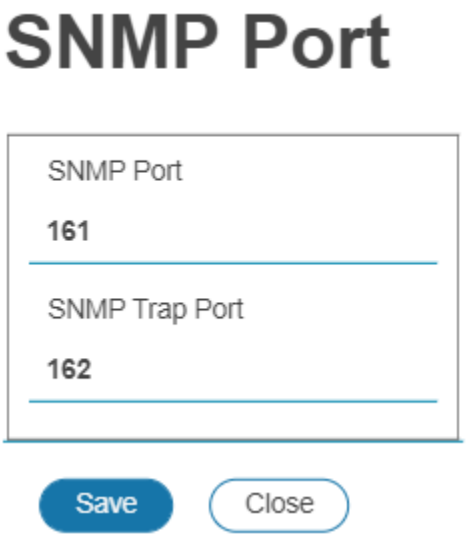
3. The SNMP General includes SNMP Access and Version.

Setup SNMP Port

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

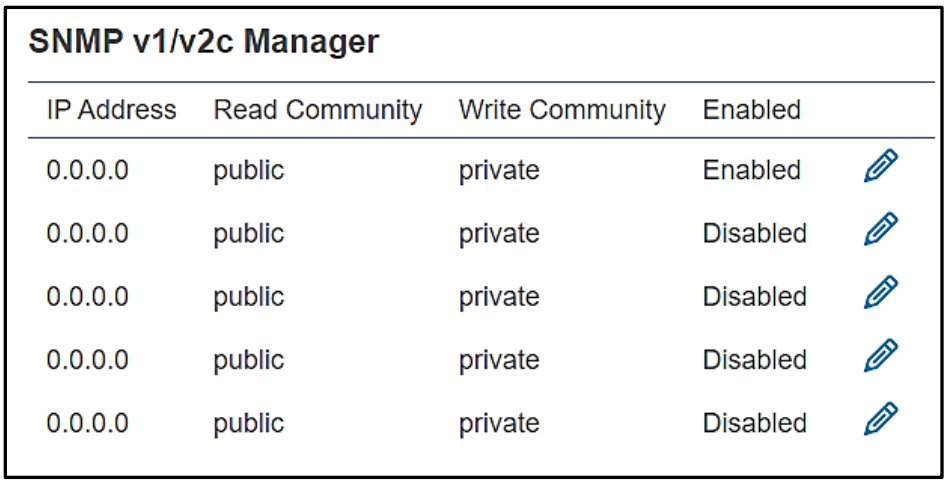


3. Set up SNMP Port and SNMP Trap Port.

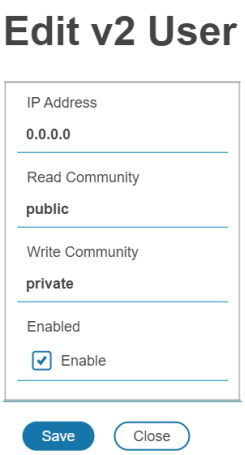


Configuring Users for SNMP V1/V2c

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 SNMMP object.
   - Write Community: the write-only community string to allow an SNMP V1/V2c manager to write an SNMMP object.
6. Click **Enable** and **Save**.

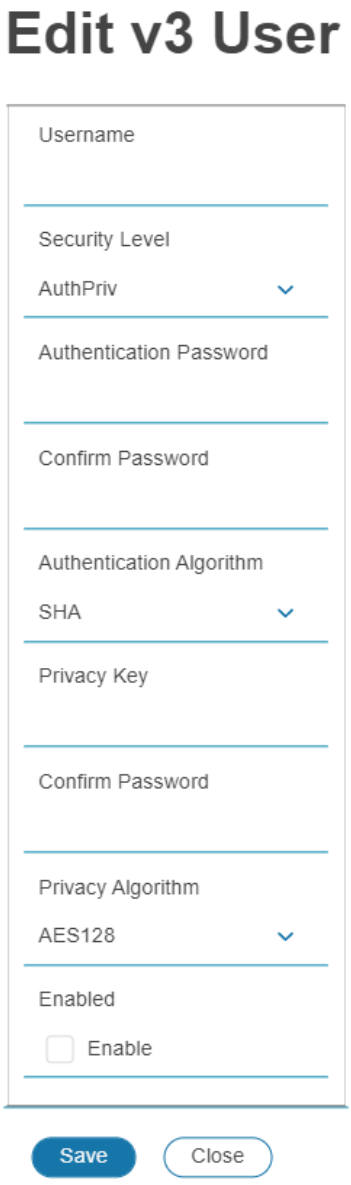
Configuring Users for SNMP v3

1. Access the Web interface and log in.
2. Under Settings, select **SNMP 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.

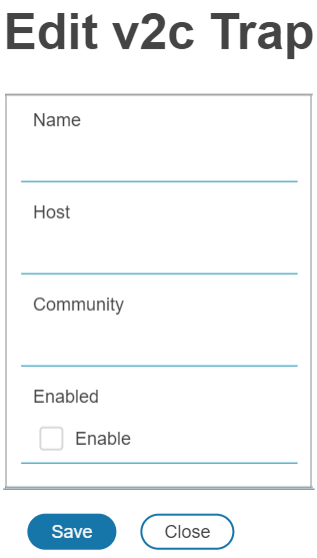
7. Enter a new unique **Authentication Password** to be used for authentication. Repeat the authentication password below it in **Confirm Password**.
8. Select the desired authentication algorithm.
   - MD5
   - SHA
9. Enter a new unique Privacy Key to be used with the privacy algorithm. Repeat the privacy 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

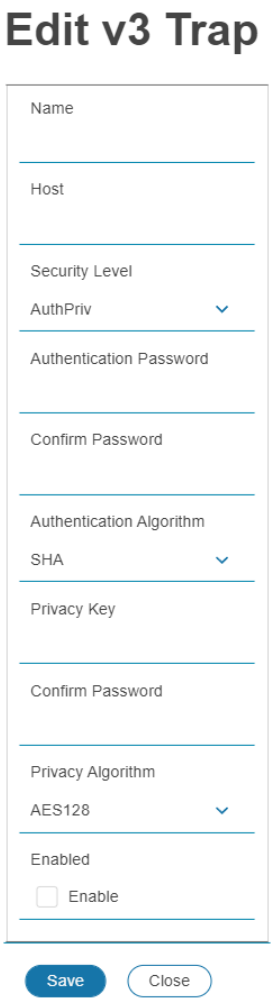
1. Go to **Settings > Trap Receiver**.
2. Click the pencil next to SNMPV2c Trap Receiver you want to update.



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

Configuring SNMP v3 Trap Settings

1. Go to **Settings** > **Trap Receiver.**
2. Click the pencil next to SNMPV3 Trap Server you want to update.



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)

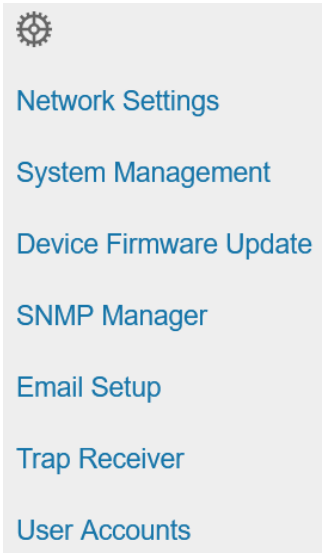
The LED will change colors depending on the NMC State.

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)

Configuring Temperature Scale

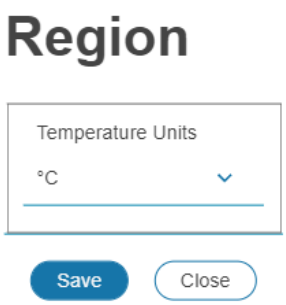
To configure the temperature scale (Celsius or Fahrenheit) of the temperature sensors:

1. Go to **User Accounts.**



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

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.

Secure Disposal Features

- The product provides a “default settings” feature that can be activated using a button press on the product, from the web user interface, from the SSH command line interface, or the USB serial interface.
- The default settings feature erases the encryption keys for the non-volatile storage used for configuration data and reinitializes the non-volatile storage area to default settings.
- The default settings feature erases the flash memory that stores the Event Log and Data Log.
- The reset to defaults feature erases the flash memory that is used to temporarily store firmware update uploads.
- The reset to defaults feature causes the SSH RSA 2048-bit private host key to be regenerated.

Non-volatile Storage

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

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

Network Transport Security

- The product generates a random SSH RSA 2048-bit private host key the first time the product starts up.
- The product has a randomly generated RSA 2048-bit private key configured by the factory. This key is used to generate a HTTPS certificate the first time the product starts up.
- The user may upload a custom HTTPS certificate and private key.
    - The HTTPS certificate should use a SHA-256 signature.
    - The private key should be RSA 2048-bit or prime256v1 (SECP256R1).
    - Other private key types may work, but performance may be negatively impacted if greater private key sizes are used: RSA 3072-bit, RSA 4096-bit; ECC curves: SECP192R1, SECP224R1, SECP256R1, SECP384R1, SECP521R1, SECP192K1, SECP224K1, SECP256K1, BP256R1, BP384R1, BP512R1, CURVE25519.
- The product uses TLS 1.2 to communicate with HTTPS web browser clients.
- Secure communication cipher negotiation with HTTPS clients uses these Cipher Suites:
    - Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
    - Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
    - Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
    - Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)

  - Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)
  - Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)
  - Cipher Suite: TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x009e)
  - Cipher Suite: TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x009f)
- The product uses TLS 1.2 to communicate with LDAPS servers.
- The product uses TLS 1.2 to communicate with SMTP+STARTTLS and SMTPS servers.
- Secure communication cipher negotiation with SMTP servers and LDAP servers uses these Cipher Suites:
  - Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)
  - Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)
  - Cipher Suite: TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xccaa)
  - Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
  - Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
  - Cipher Suite: TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x009f)
  - Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)
  - Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
  - Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x006b)
  - Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
  - Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
  - Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
  - Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
  - Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
  - Cipher Suite: TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x009e)
  - Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)
  - Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)

  - Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x0067)
  - Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
  - Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
  - Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
  - Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
  - Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
  - Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
  - Cipher Suite: TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 (0xc032)
  - Cipher Suite: TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 (0xc02a)
  - Cipher Suite: TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f)
  - Cipher Suite: TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02e)
  - Cipher Suite: TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026)
  - Cipher Suite: TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005)
  - Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
  - Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)
  - Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
  - Cipher Suite: TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 (0xc031)
  - Cipher Suite: TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 (0xc029)
  - Cipher Suite: TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e)
  - Cipher Suite: TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02d)
  - Cipher Suite: TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (0xc025)
  - Cipher Suite: TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004)
- The product provides a SSH server with these algorithms to communicate with SSH clients:
  - Key exchange algorithms:
    - curve25519-sha256, curve25519-sha256@libssh.org, 62ijnda-hellman-group-exchange-sha256 (2048-bit), 62ijnda-hellman-group16-sha512, 62ijnda-hellman-group18-sha512, 62ijnda-hellman-group14-sha256
    - For compatibility: ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521
  - Host key algorithms:
    - rsa-sha2-512 (3072-bit), rsa-sha2-256 (3072-bit), ssh-ed25519
    - For compatibility: ssh-rsa (3072-bit), ecdsa-sha2-nistp256

    - Encryption algorithms:
        - chacha20-poly1305@openssh.com, aes128-ctr, aes192-ctr, aes256-ctr, aes128-gcm@openssh.com, aes256-gcm@openssh.com
    - MAC algorithms:
        - mailto:umac-128-etm@openssh.com, hmac-sha2-256-etm@openssh.com, hmac-sha2-512-etm@openssh.com
        - For compatibility: umac-64-etm@openssh.com, hmac-sha1-etm@openssh.com, umac-64@openssh.com, umac-128@openssh.com, hmac-sha2-256, hmac-sha2-512, hmac-sha1
- The product connects to user configured SSH servers using these algorithms:
    - Key exchange algorithms:
        - ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521, 63ijnda-hellman-group-exchange-sha256, 63ijnda-hellman-group16-sha512, 63ijnda-hellman-group18-sha512, 63ijnda-hellman-group14-sha256, 63ijnda-hellman-group14-sha1, 63ijnda-hellman-group1-sha1, 63ijnda-hellman-group-exchange-sha1
    - Host key algorithms:
        - ecdsa-sha2-nistp256
    - Encryption algorithms:
        - aes128-ctr, aes192-ctr, aes256-ctr, aes256-cbc, 63ijndael-cbc@lysator.liu.se, aes192-cbc, aes128-cbc, blowfish-cbc, arcfour128, arcfour, 3des-cbc
    - MAC algorithms:
        - hmac-sha2-256, hmac-sha2-512, hmac-sha1, hmac-sha1-96, hmac-md5, hmac-md5-96, hmac-ripemd160, hmac-ripemd160@openssh.com

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.

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 describing 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

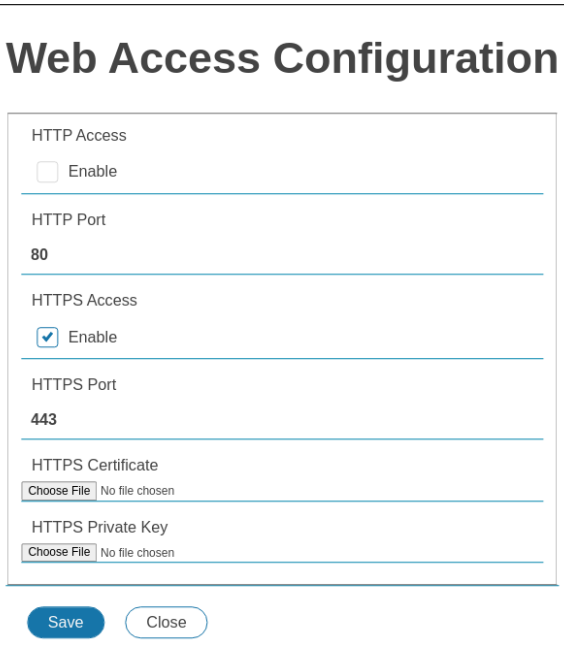
- The product includes a real-time clock and a battery that maintains time for a short amount of time when no power is applied. When combined with NTP, accurate timestamps on logs are provided.

Secure deployment

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

Upload Certificate

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



Use SNMPv3c

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

Disabling unused interfaces

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

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

Review Session management

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

Warranty and Regulatory Information

Warranty Information

(https://www.panduit.com)

Regulatory Information

Safety and regulatory compliance

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

Panduit Support and Other Resources

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

Accessing Panduit Support

North America

Customer Service

- Price & Availability
- Expedites

800-777-3300 or cs@panduit.com

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

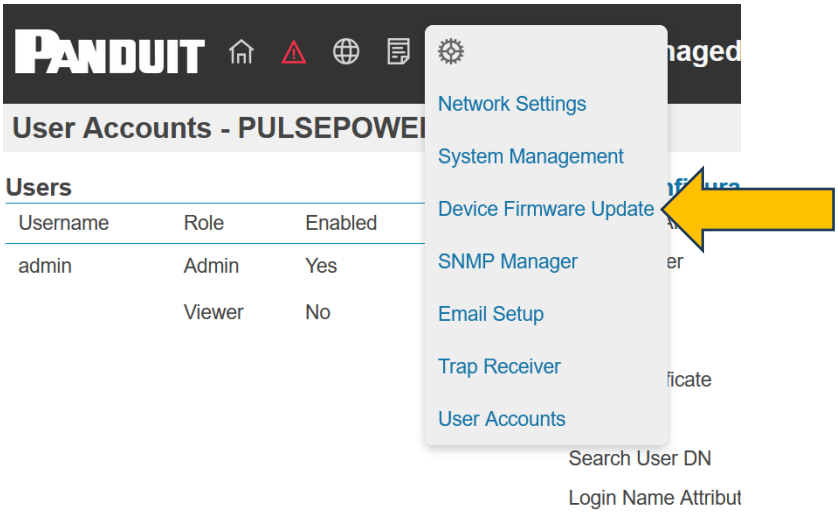
W

Watts

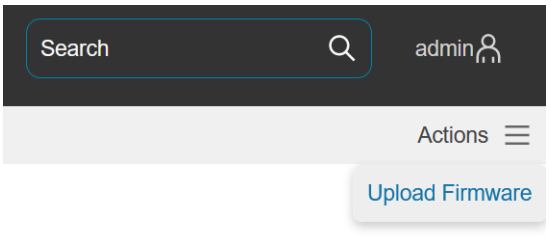
Appendix A: Firmware Update Procedure

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

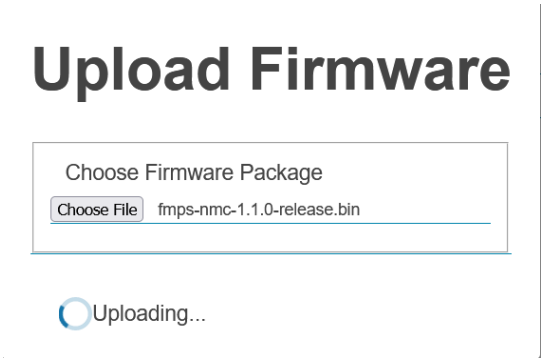
1. Download the firmware file from the Panduit web page.
2. Unzip the downloaded file.
3. Open the User interface in a web browser by entering the NMC IP address.
4. Login with Administration credentials.
5. Go to **Settings > Device Update Firmware**.



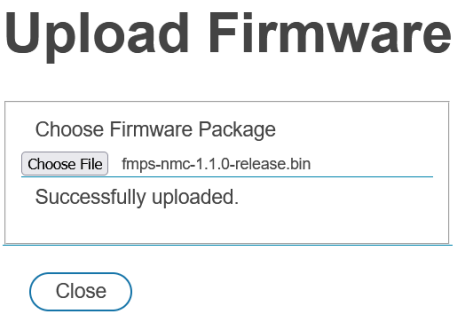
6. In the upper right, transfer the new Firmware onto the NMC using the Update Firmware command from the dropdown.



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.

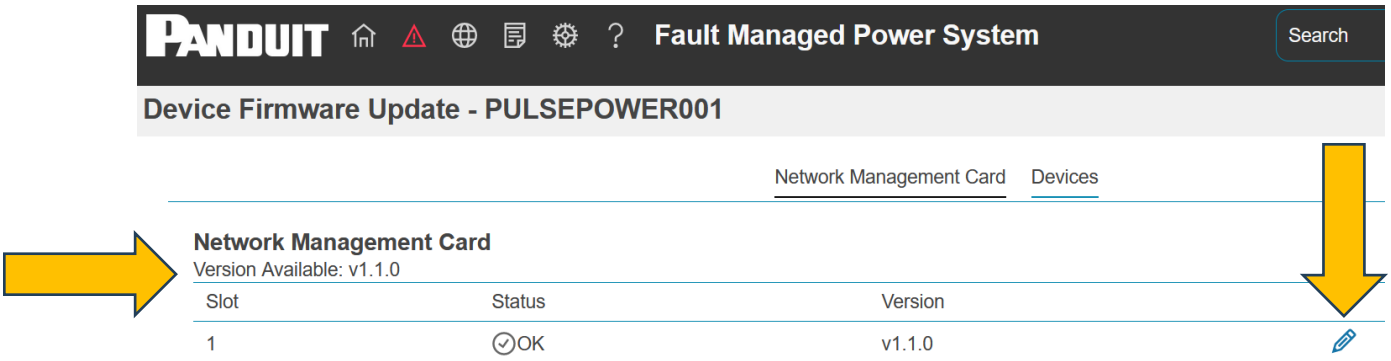


8. The screen will then change to “Successfully Uploaded”. The dialog box can be closed.

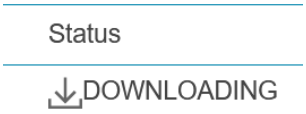


NOTE: The firmware has not been installed to any device yet. The Version Available will be displayed below the device name and will match the file name uploaded.

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

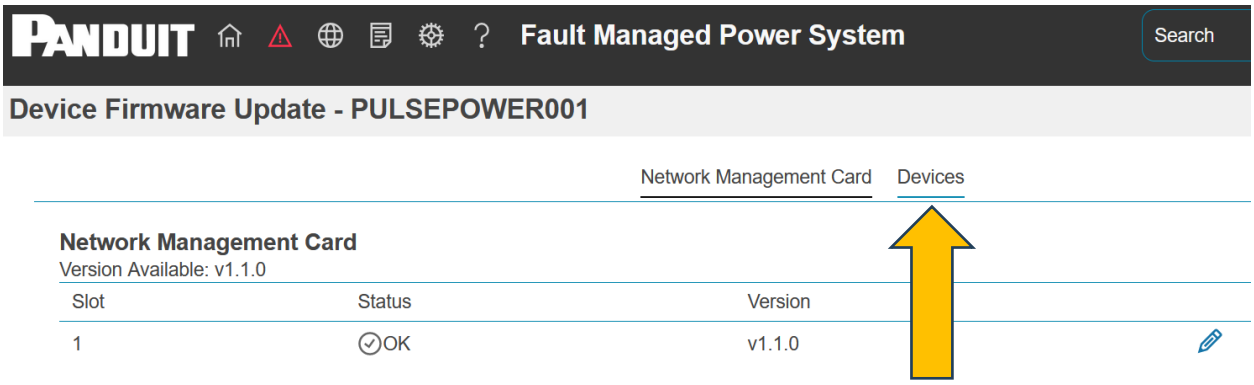


When the dialog box opens, click on Upload.

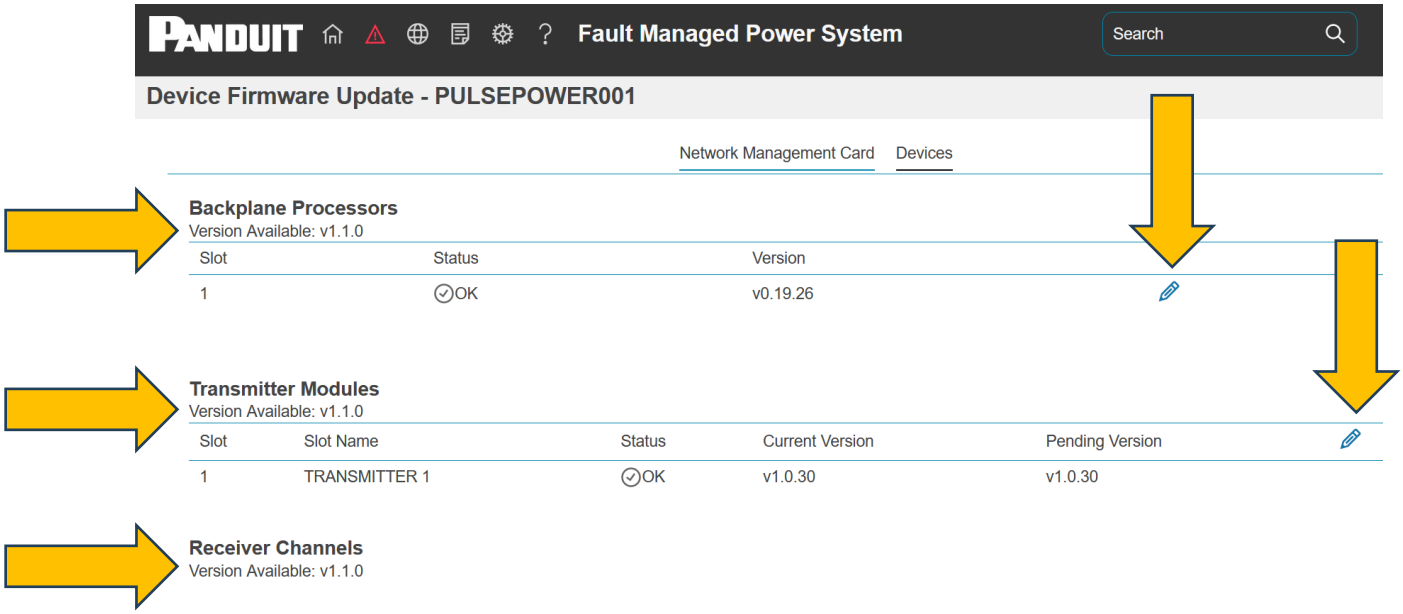


The Firmware is now being installed onto the NMC. After the file is installed, the NMC will **automatically reboot**.

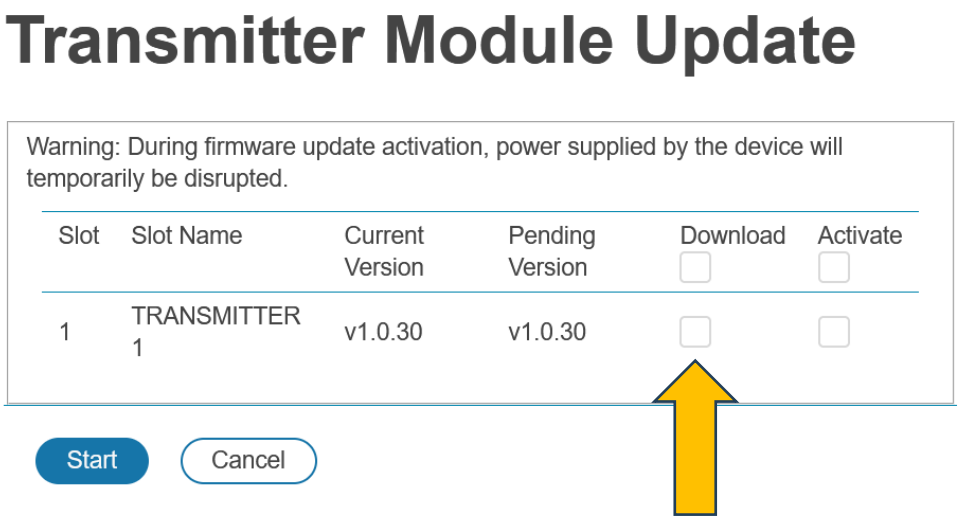
To update the Transmitter and/or Receiver, click on Devices from the main page.



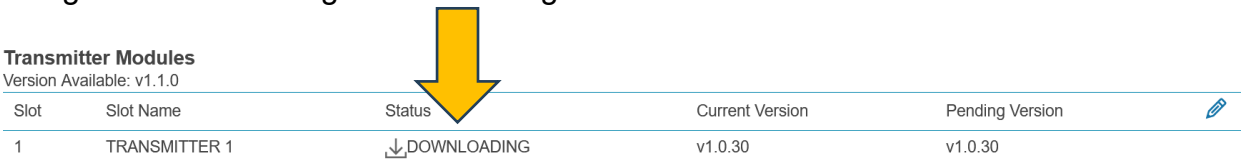
Select the device to be updated using the pencil icon.



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



Select the Download 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 "Downloading". The Pending Version will match the Available Version.



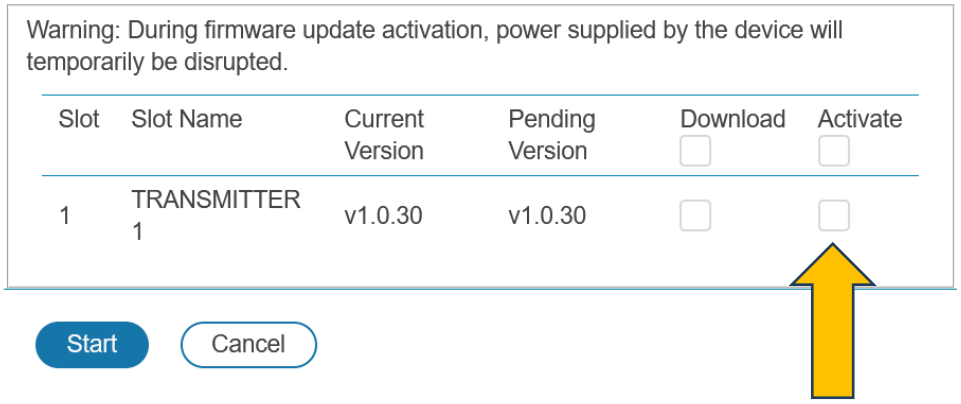
NOTE: The Transmitter and Backplane firmware will take less than a minute to download. **The Receiver may take over an hour to download**.

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.

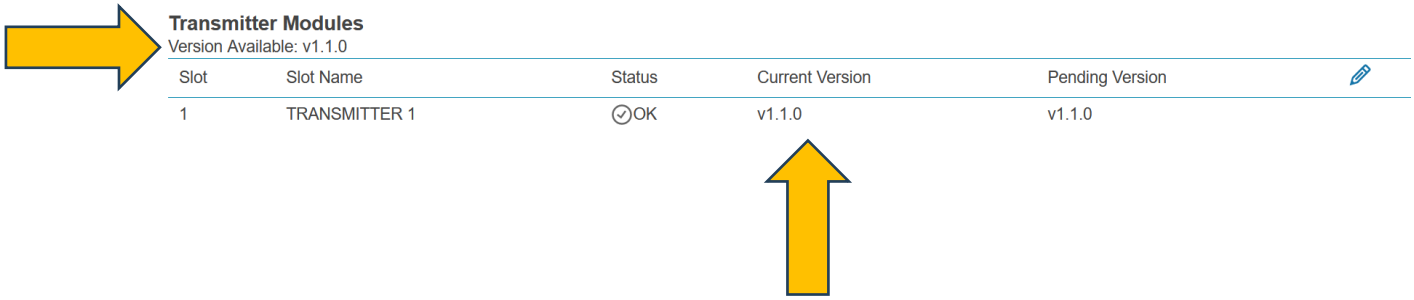
To apply the firmware update (after Downloading completes), reenter the Update screen using the pencil icon and check the Activate button then press Start.

Transmitter Module Update



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

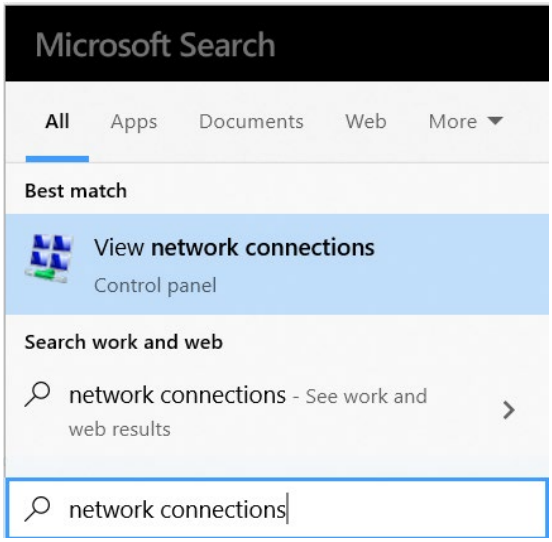
Press and hold the Reset Button for 2 seconds to recover from a NMC controller communication failure. The green LED will flash slowly indicating the controller will reset. This will cause a reset of the NMC controller, all configuration(s) will be retained.

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

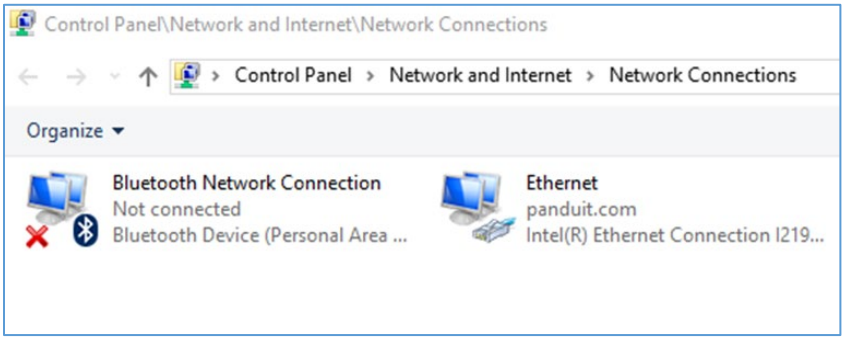
Appendix C: Direct connect to the FMPS via Ethernet without Bonjour

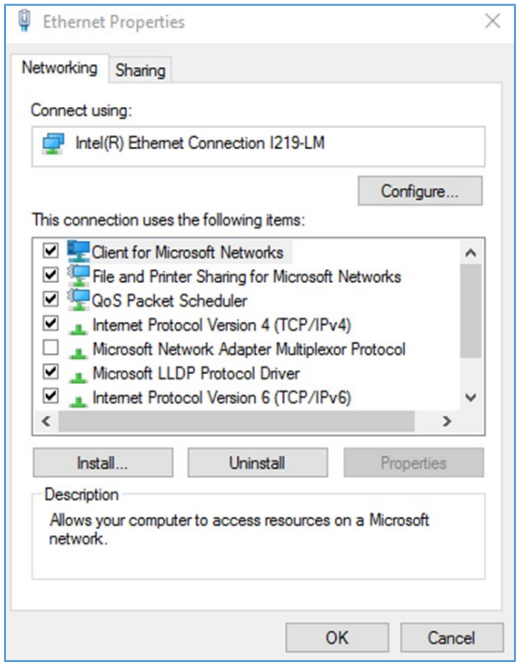
Note: Instructions refer specifically to Windows 10. Please refer to your operating system documentation if you are not using Windows 10.

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** (you may need to scroll down). 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. You may proceed as this error is expected.

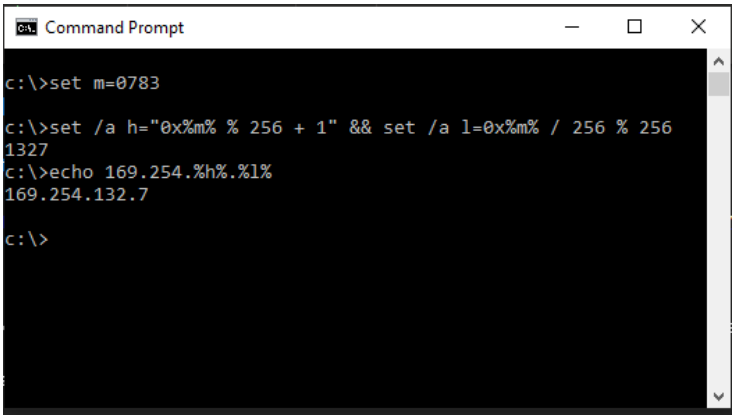
Note: If the browser does not connect, the device may have older firmware. Try again with the following additional steps:

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

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

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

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



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

    example: **https://169.254.132.7/**

5. Use the Enter key to navigate to the web site.
6. A Privacy Error or an error explaining that the certificate (cert) authority is invalid. This message is presented when a device has the initial certificate in-use. You may proceed as this error is expected.

Appendix D: Command Line Interface

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

Logging in using SSH protocol

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

Changing Your Password

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

Enter the username, current password, and new password twice to confirm. The 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

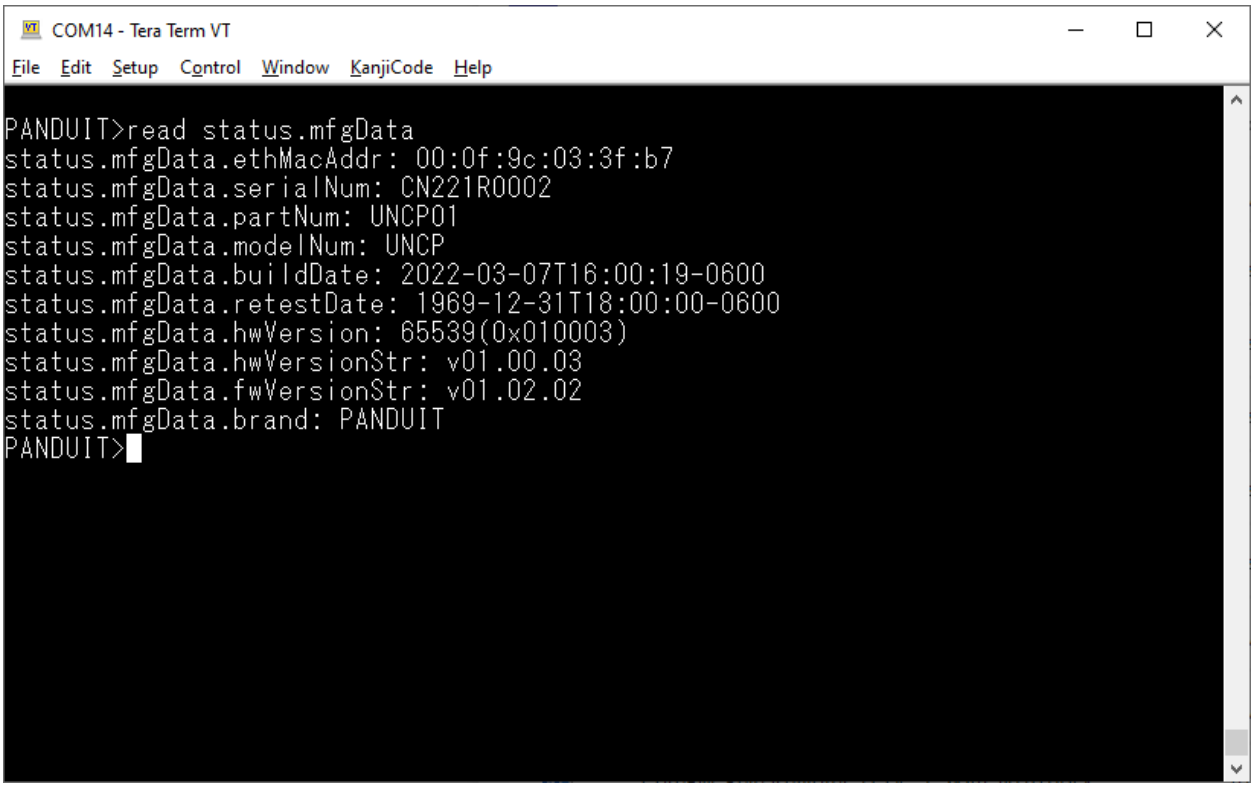
Command list

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.

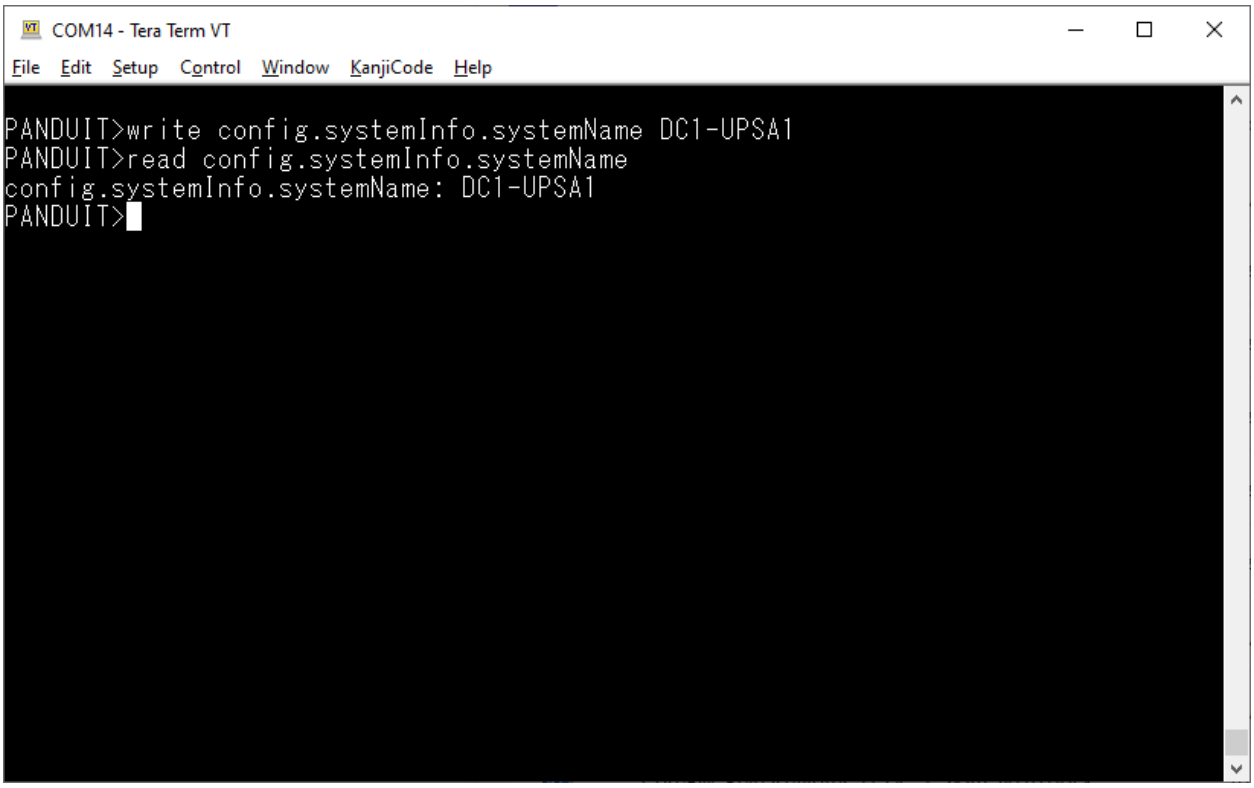
  Example: read status.mfgData



- **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 your security requirements.
3. Create a dictionary at `/usr/share/freeradius/dictionary.Panduit` containing:

```
# -*- text -*-
VENDOR          Panduit         19536
BEGIN-VENDOR    Panduit
ATTRIBUTE       Panduit-User-Role       1       integer
VALUE           Panduit-User-Role       User    1
VALUE           Panduit-User-Role       Admin   2
VALUE           Panduit-User-Role       Control 3
END-VENDOR      Panduit
```

4. Load dictionary.Panduit by appending the following line to `/etc/freeradius/3.0/dictionary`:

```
$INCLUDE /usr/share/freeradius/dictionary.Panduit
```

5. Add authorized users to `/etc/freeradius/3.0/mods-config/files/authorize` with the desired role. (Note: the ‘users’ file location may vary based on unique customizations or different package managers.) When specified, the User-Role MUST be the first attribute of the user. Use passwords that are configured for your security requirements.

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

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

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

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

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

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

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

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

7. Verify the server is able to perform authentication and returns the configured User-Role. Note: You may need to change this example based on any client restrictions that are enforced.

```
Usage: radtest [OPTS] user passwd radius-server[:port] nas-port-number secret


# radtest 'radroleadmin' '34567890' 192.0.2.1 0 'panduit#1' ''
Sending Access-Request of id 212 to 192.0.2.1 port 1812
        User-Name = "radroleadmin"
        User-Password = "34567890"
        NAS-IP-Address = 127.0.1.1
        NAS-Port = 0
        Message-Authenticator = 0x00000000000000000000000000000000
rad_recv: Access-Accept packet from host 192.0.2.1 port 1812, id=212, length=38
        Panduit-User-Role = Admin
        Service-Type = Framed-User
```

Appendix F: POSIX Time Zone Information

The custom time zone format is:

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

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

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

`Offset` is the standard time offset from UTC.

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

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

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

`DSTStart and DSTEnd` are in format:

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

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

Example 1: The US Central 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.)