PANDUIT®
infrastructure for a connected world

SmartZone™ *m*Power

User Manual

*m*Power |Manage-Configure-Update|

Table of Contents

Table of Figures

Section 1 – System Overview

*m*Power Software

Panduit *m*Power is designed to simplify monitoring and management of multiple network-connected Panduit UPSes.

Bulk Configuration allows an administrator to configure a single UPS NMC, download the configuration file and upload the configuration to all devices managed by *m*Power with a few additional clicks.

Bulk Update helps keep your system secure by making firmware updates easy. The administrator can initiate a firmware update on all managed devices by uploading the upgrade package to *m*Power and clicking the **Start Upgrade** button.

Monitoring up to 100 devices is simplified by the *m*Power dashboard, alarm aggregation, and event aggregation. *m*Power will display any abnormal conditions and allow the user to investigate system-wide failures with summarized tables and aggregated logs.

*m*Power is currently available for the 64-bit Windows OS.

Quick Start

1. Install *m*Power

   Details: *Appendix B: Installation*

2. Connect & Login

   Details: *Connecting to mPower*

3. Change Device Authentication (Settings -> mPower Settings)

   Details: *Device Authentication*

4. Add Managed Devices (Home-> Control & Manage)

   Details: *Managed Devices Configuration*

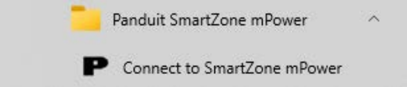
5. View Device status in Dashboard (Home -> Dashboard)

   Details: *Introduction to the Dashboard*

Section 2 – Web Graphical User Interface (GUI) Configuration

Connecting to *m*Power

*m*Power is accessed via a web browser. The installer creates a convenient link in the start menu that will launch *m*Power in the default browser.



Note: https:// must be used when mPower is launched from within the browser.

Web Configuration

Supported Web Browsers

The supported web browsers are Google Chrome (mobile and desktop), Mozilla Firefox, Microsoft Edge, and Apple Safari (mobile and desktop). *m*Power is tested with the most recent version of each browser at time of release.

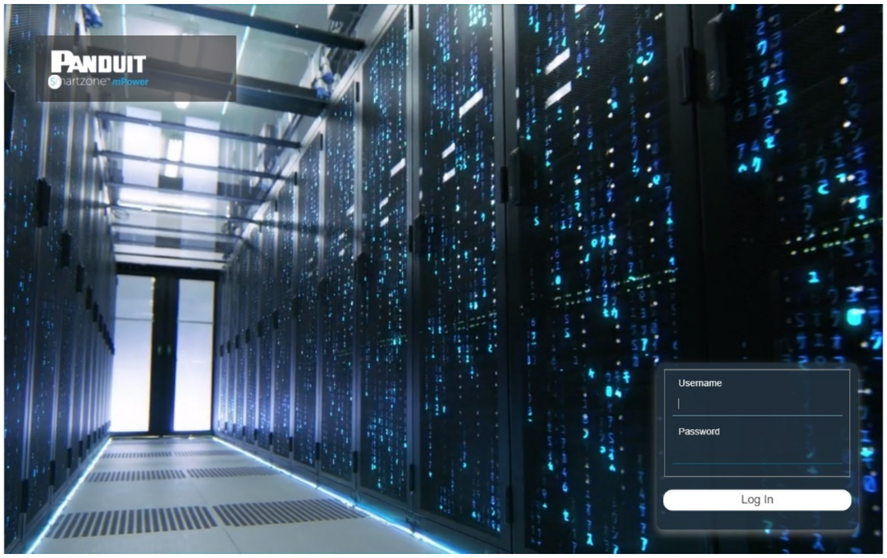


Figure 1: Login Page

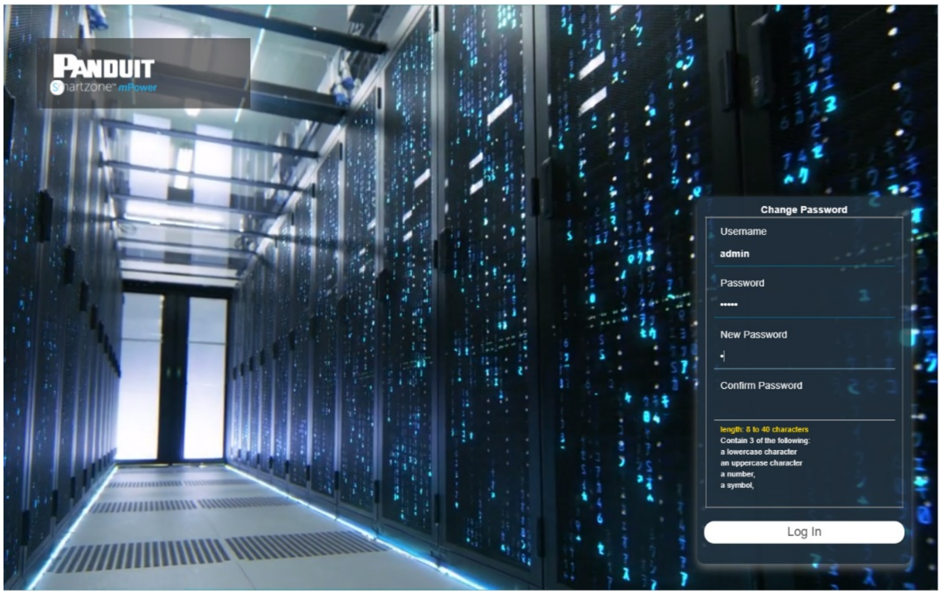
Changing Your Password

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

1. Enter the default username: admin
2. Enter the default password: admin
3. Enter the 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.



Change Password

Username
admin

Password
•••••

New Password
•

Confirm Password

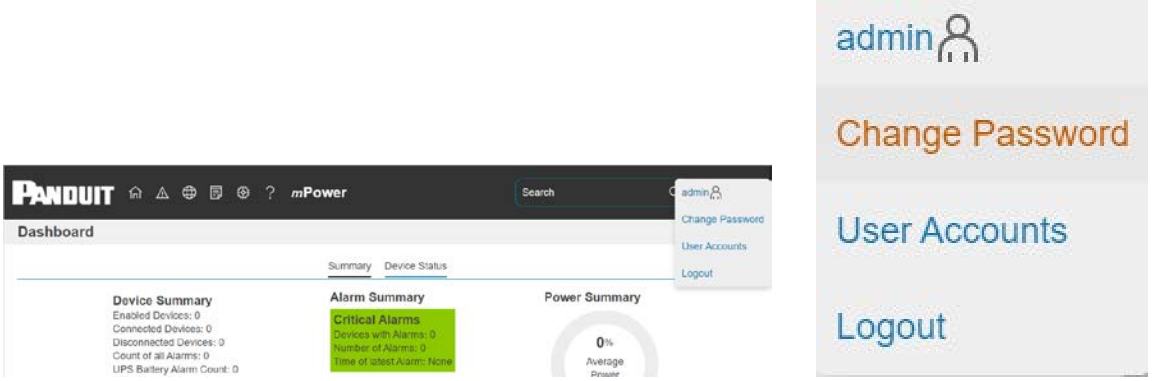
length: 8 to 40 characters
Contain 3 of the following:
a lowercase character
an uppercase character
a number,
a symbol,

Figure 2: Changing Your Password

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

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

1. Click on "admin" or the currently logged in user and select **Change Password**.



Device Summary
Enabled Devices: 0
Connected Devices: 0
Disconnected Devices: 0
Count of all Alarms: 0
UPS Battery Alarm Count: 0

Alarm Summary
Critical Alarms
Devices with Alarms: 0
Number of Alarms: 0
Time of latest Alarm: None

Power Summary
0%
Average Power

Figure 3: After Login

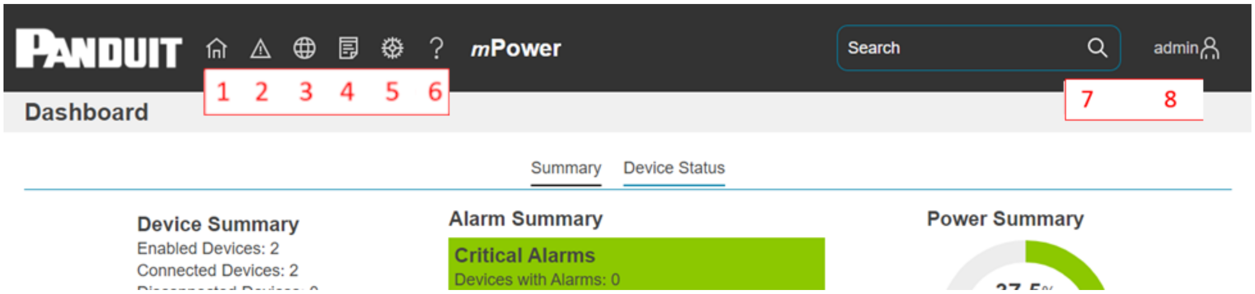
2. The Change Password window opens.

   See Figure 2: Changing Your Password

3. Follow the steps above.

Introduction to the Web GUI

Landing Page/Dashboard



Device Summary
Enabled Devices: 2
Connected Devices: 2

Alarm Summary
Critical Alarms
Devices with Alarms: 0

Power Summary

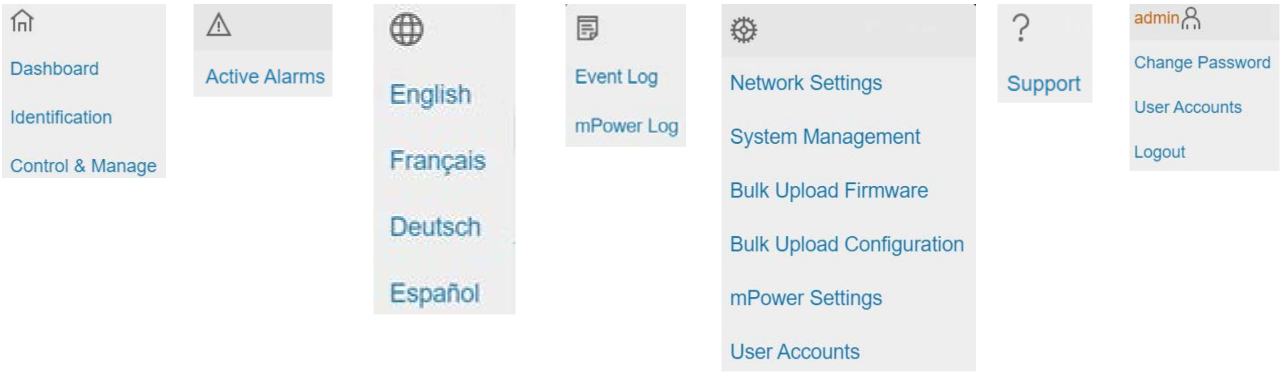
Figure 4: Landing Page/Dashboard

Number	Icon	Description
1	⌂	The home icon provides an overview of the system with access to the Dashboard, Identification, and Control & Manage Pages.
2	⚠	The Alarm icon provides details of the active alarms.
3	🌐	The Globe icon lets you select a Language. There are four languages available to choose from: English, French, German and Spanish.
4	📄	The Page icon provides access to the logs, which can be viewed and downloaded. • The Event Log is an aggregation of all events on the monitored devices • The *m*Power Log shows events in the software itself
5	⚙	The Settings icon allows a user to setup the Network Settings, System Management, Bulk Upload Firmware, Bulk Upload Configuration, *m*Power Settings and User Accounts.
6	?	Information about the *m*Power software can be found using this icon. You also can also click user

Number	Icon	Description
		guide and license to ask for help.
7	🔍	The Search icon allows you to input key words and search for the related results.
8	👤	The User icon shows who is logged in (admin). The menu allows the user to navigate to the Change Password page, go to User Accounts page, or Logout.

Menu Drop-downs

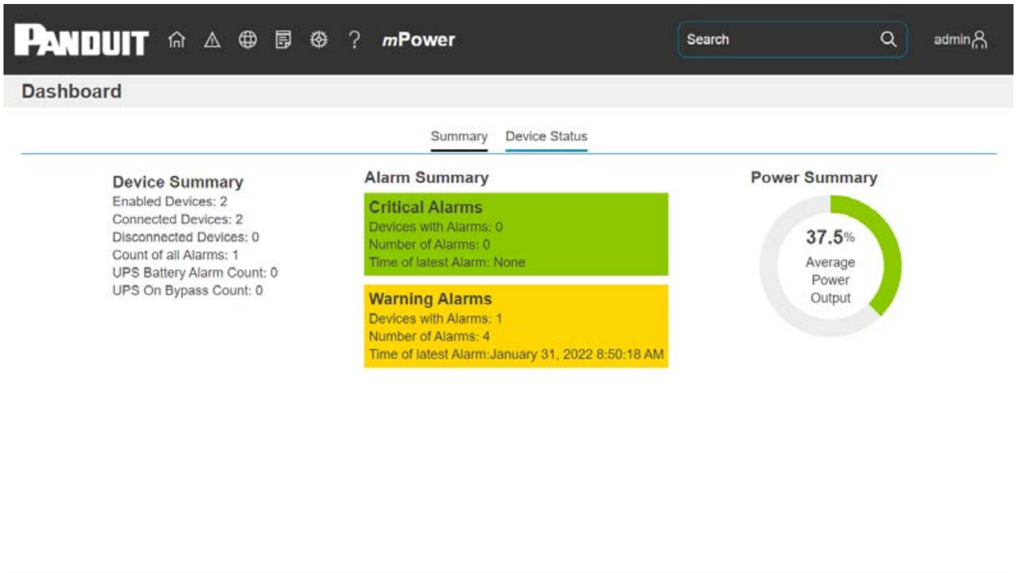
Overview **Alarms** **Language** **Logs** **Setting** **Help** **User**



Introduction to the Dashboard

Summary Page

The summary page provides a high-level view of device status providing the user with a big picture view of health and potential issues.



Device Summary
Enabled Devices: 2
Connected Devices: 2
Disconnected Devices: 0
Count of all Alarms: 1
UPS Battery Alarm Count: 0
UPS On Bypass Count: 0

Alarm Summary

Critical Alarms
Devices with Alarms: 0
Number of Alarms: 0
Time of latest Alarm: None

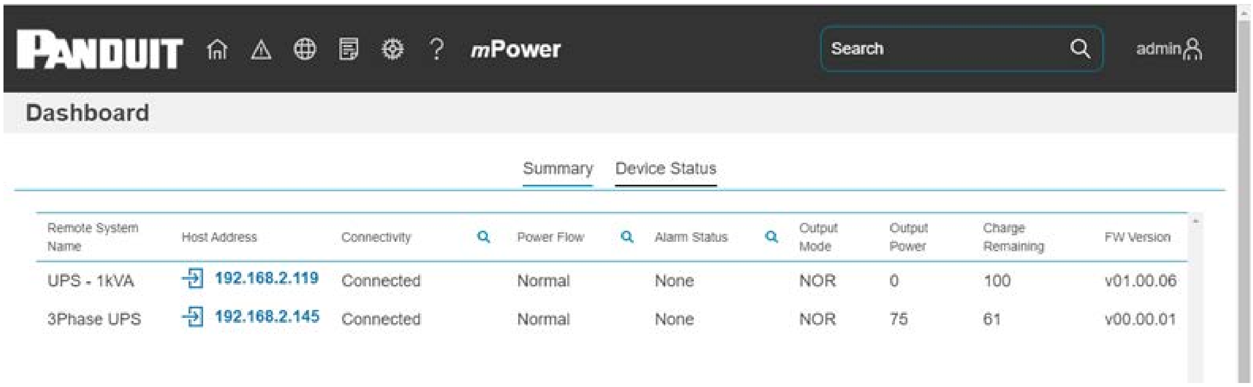
Warning Alarms
Devices with Alarms: 1
Number of Alarms: 4
Time of latest Alarm:January 31, 2022 8:50:18 AM

Power Summary
37.5% Average Power Output

Figure 5: Summary Page

Device Status Page

The device status page provides details on the operation of individual devices. A user can determine which devices have alarms or connectivity issues, evaluate load margins on individual devices and more.



Remote System Name	Host Address	Connectivity	Power Flow	Alarm Status	Output Mode	Output Power	Charge Remaining	FW Version
UPS - 1kVA	192.168.2.119	Connected	Normal	None	NOR	0	100	v01.00.06
3Phase UPS	192.168.2.145	Connected	Normal	None	NOR	75	61	v00.00.01

Figure 6: Device Status Page

Network Settings

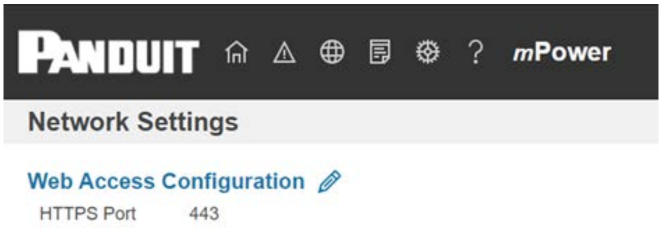
To configure the network settings, click the gear icon (Settings menu) and select Network Settings.

*m*Power Web UI access requires use of the HTTPS protocol, however, the port is configurable and may be changed after installation in network settings.

Note: When the HTTPS Port is changed, wait about 30 seconds, then use the "Connect to SmartZone *m*Power" Program menu item to reconnect to *m*Power.

*m*Power also allows installation of a user create certificate/key pair. CA signed certificates are desirable if *m*Power will be used remotely.

Note: When changing the HTTPS Certificate and Private Key, the change will take effect after both have been changed. If the certificate and key do not match or cannot be used, the system will revert to a certificate/key that was generated when the software was started for the very first time. If only a Certificate or only a Private Key is uploaded, the Certificate and Private Key validation will occur the next time the *m*Power service is started



Network Settings

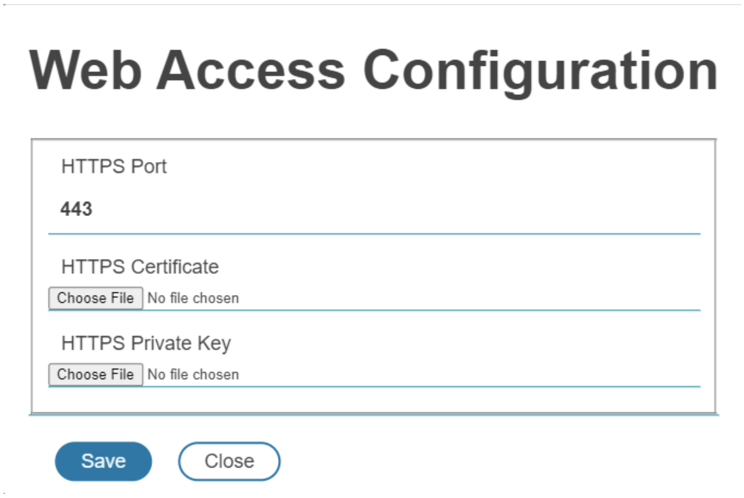
Web Access Configuration

HTTPS Port 443

Figure 7: Network Settings

Web Access Configuration:

1. Select the **pencil** icon next to **Web Access Configuration.**
2. Change the HTTPS Port if needed.
3. Click choose file and select the new HTTPS certificate.
4. Click choose file and select the new HTTPS Private key.



Web Access Configuration

HTTPS Port

443

HTTPS Certificate

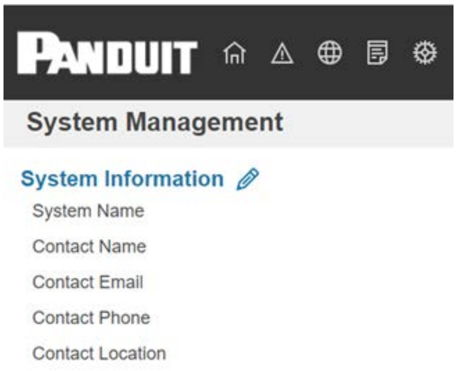
HTTPS Private Key

Figure 8: Web Access Configuration

System Management Information

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

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



System Management

System Information

System Name

Contact Name

Contact Email

Contact Phone

Contact Location

Figure 9: System Management

System Info

The system information includes the name of the system and information of the person to contact in case an issue arises. Follow the steps below to set up the system information:

1. Select the **pencil** icon next to **System Management.**

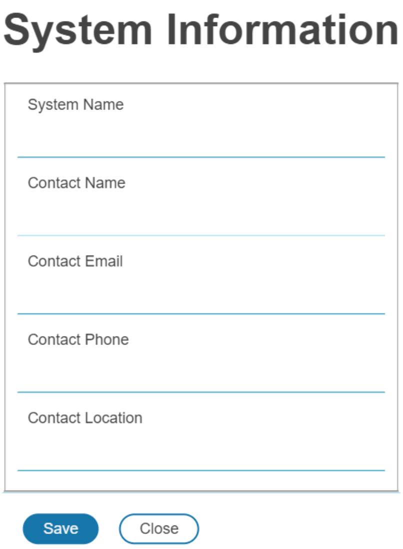


Figure 10: System Information Configuration

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

Restart mPower

Restart *m*Power by selecting **Restart** in the **Actions** menu under **System Management.**

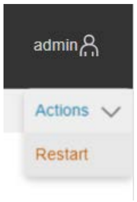


Figure 11: System Management Actions

Control & Manage

The **Control & Manage** section of the Web GUI allows a user to manage connections to all devices monitored by the system.

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

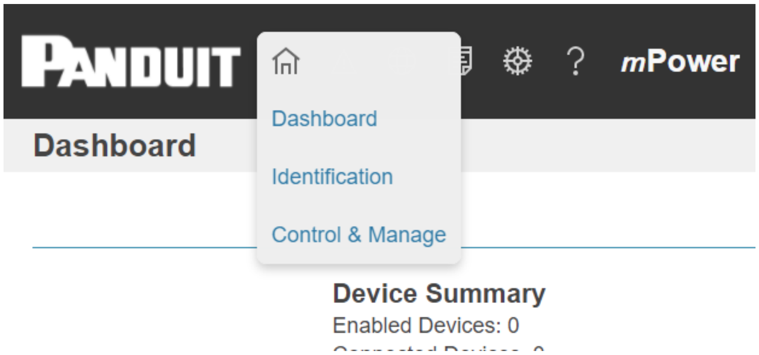


Figure 12: Control & Manage Navigation

Managed Devices Configuration

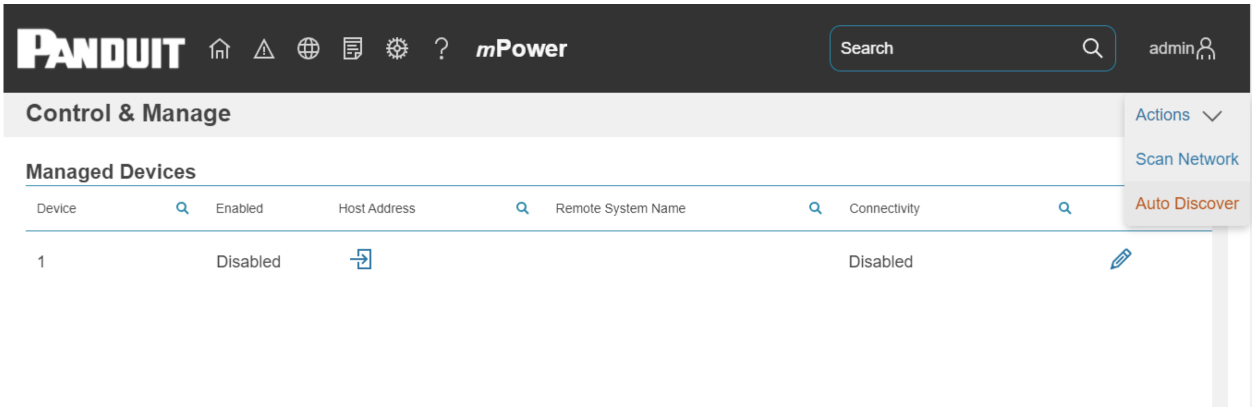
Any device that *m*Power should monitor or bulk update must be configured as a managed device. Three methods of adding devices are provided: Auto Discover, Scan Network, and Manual Device Configuration. Prior to scanning, managed devices must have a user configured that matches the setting in *m*Power Settings → Device Authentication. See *Device Authentication* for details.

Auto Discover

*m*Power provides auto-discovery of any devices on the local network using the Bonjour service. Any UPS devices on the same local network with credentials matching the *m*Power Device Authentication will automatically be added to the managed device list. Status of the auto- discovery process can be reviewed in the *m*Power log. The **Auto Discover** feature generates messages to the Event Log while it is in process, and a message when it has finished.

To Auto Discover devices:

1. Select the Home Icon then **Control & Manage** from the drop-down menu in the Web GUI.
2. Select **Actions → Auto Discover**.



Managed Devices

Device	Enabled	Host Address	Remote System Name	Connectivity
1	Disabled			Disabled

Figure 13: Control & Manage Page

Scan Network

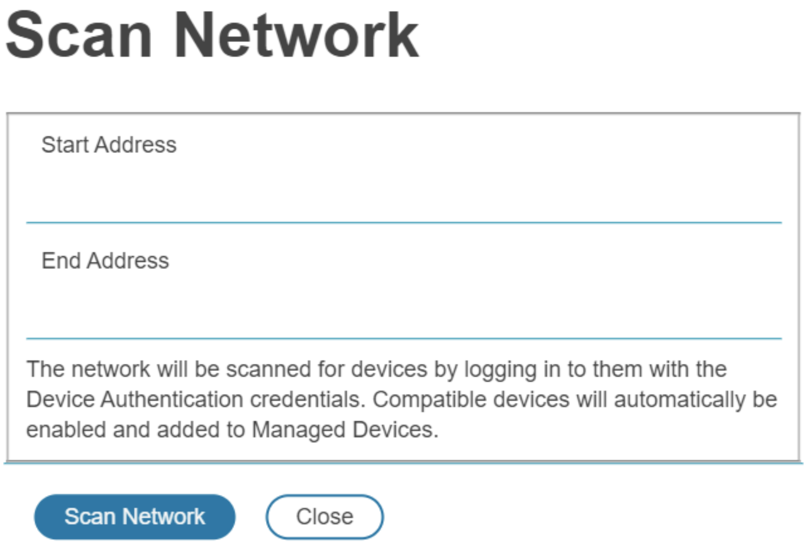
*m*Power provides network scan functionality in case *m*Power is not running on the same local network as the devices it should monitor. The **Scan Network** process will first ping each address in the requested network segment, then attempt to connect to the device. If *m*Power can authenticate, it will add the scanned device to the managed devices list. While **Scan Network** is attempting to connect to the device, some unmanageable devices may temporarily show up as "Added by Scan Network". The Scan Network feature generates messages to the Event Log while it is in process, and a message when it has finished.

Note: Since Scan Network is a brute force detection method it may trigger some network intrusion detection systems.

To scan a network segment:

1. Select the Home Icon then **Control & Manage** from the drop-down menu in the Web GUI.
2. Select **Actions → Scan Network**.
3. Enter the IP address *m*Power should start scanning at under **Start Address**.

4. Enter the IP address *m*Power should stop scanning at under **End Address**.
5. Click **Scan Network**.



Scan Network

Start Address

End Address

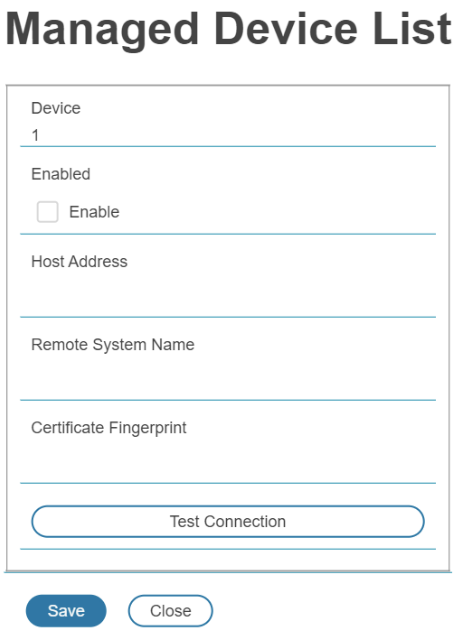
The network will be scanned for devices by logging in to them with the Device Authentication credentials. Compatible devices will automatically be enabled and added to Managed Devices.

Figure 14: Scan Network Page

Manual Device Configuration

Select the Home Icon then **Control & Manage** from the drop-down menu in the Web GUI.

1. For each new device, select the **Edit** pencil next to the last device slot shown. (Only the first empty device slot is shown.)



Managed Device List

Device
1

Enabled
□ Enable

Host Address

Remote System Name

Certificate Fingerprint

Figure 15: Managed Device Edit

2. Check **Enabled**.

3. Enter the new device IP address or hostname.

4. Enter a text description under **Remote System Name**.

5. Click **Save** to add the new device.

Device Removal

To temporarily remove a device:

1. Selecting the pencil icon next to the device
2. Uncheck **Enable**.
3. Click **Save**.

To permanently remove a device (free slot):

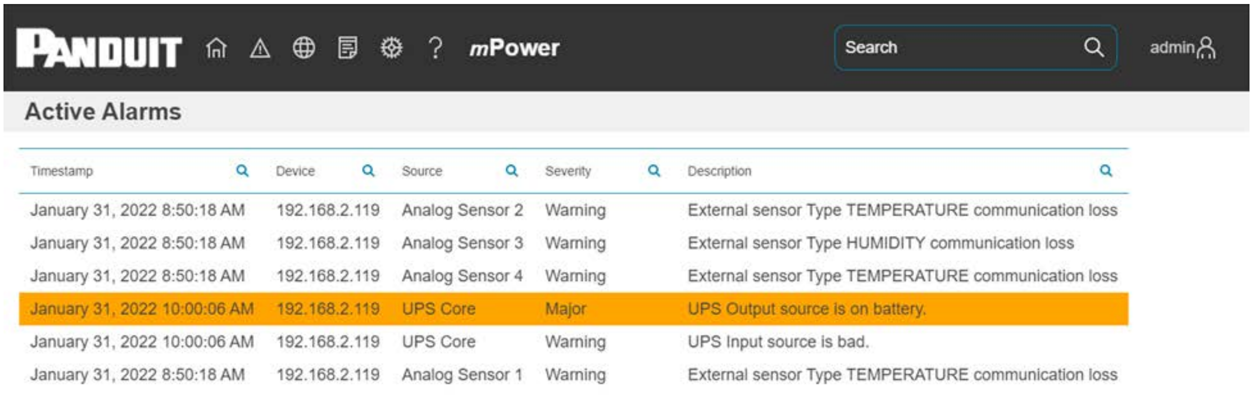
1. Selecting the pencil icon next to the device
2. Uncheck **Enable**.

3. Clear all other fields (leave blank)
4. Click **Save**.

Alarms

Active Alarms

The **Active Alarms** page shows an aggregation of all alarms on all devices managed. The alarms may be filtered by time, device, source, or severity to simplify analysis.



Active Alarms

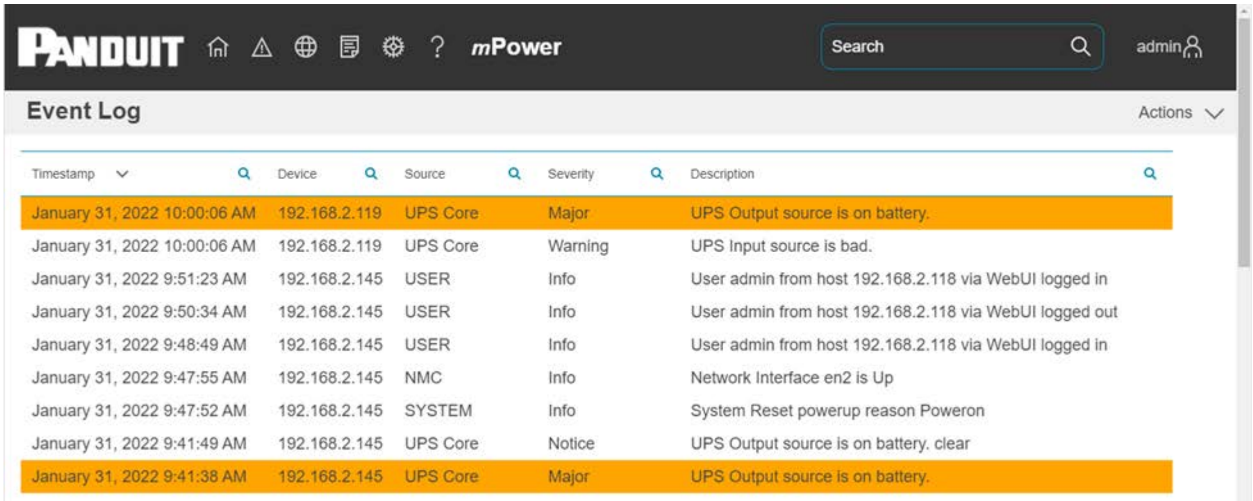
Timestamp	Device	Source	Severity	Description
January 31, 2022 8:50:18 AM	192.168.2.119	Analog Sensor 2	Warning	External sensor Type TEMPERATURE communication loss
January 31, 2022 8:50:18 AM	192.168.2.119	Analog Sensor 3	Warning	External sensor Type HUMIDITY communication loss
January 31, 2022 8:50:18 AM	192.168.2.119	Analog Sensor 4	Warning	External sensor Type TEMPERATURE communication loss
January 31, 2022 10:00:06 AM	192.168.2.119	UPS Core	Major	UPS Output source is on battery.
January 31, 2022 10:00:06 AM	192.168.2.119	UPS Core	Warning	UPS Input source is bad.
January 31, 2022 8:50:18 AM	192.168.2.119	Analog Sensor 1	Warning	External sensor Type TEMPERATURE communication loss

Figure 16: Active Alarms Page

Logs

Event Log

The **Event Log** page shows an aggregation of all events logged on all devices managed. The events may be filtered by time, device, source, or severity to allow analysis of specific events.



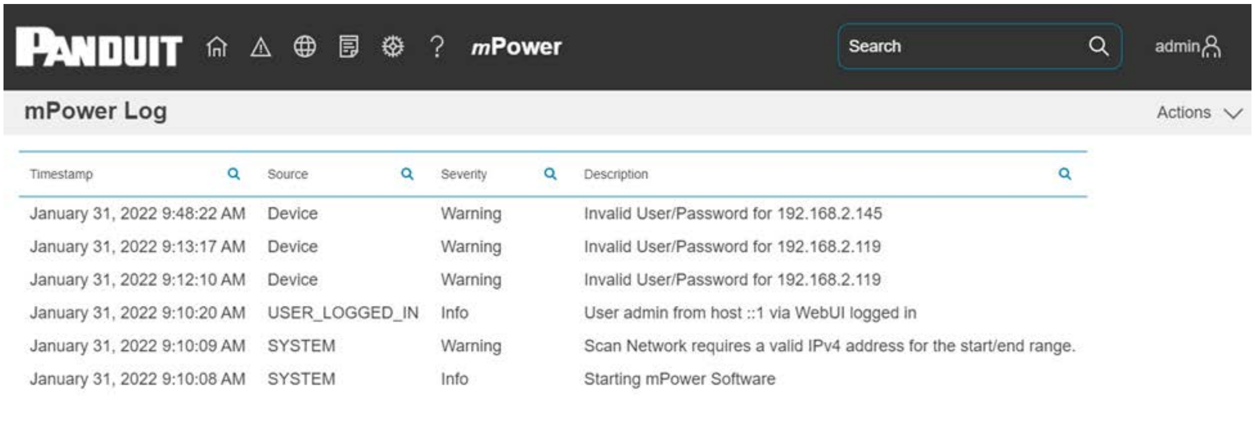
Timestamp	Device	Source	Severity	Description
January 31, 2022 10:00:06 AM	192.168.2.119	UPS Core	Major	UPS Output source is on battery.
January 31, 2022 10:00:06 AM	192.168.2.119	UPS Core	Warning	UPS Input source is bad.
January 31, 2022 9:51:23 AM	192.168.2.145	USER	Info	User admin from host 192.168.2.118 via WebUI logged in
January 31, 2022 9:50:34 AM	192.168.2.145	USER	Info	User admin from host 192.168.2.118 via WebUI logged out
January 31, 2022 9:48:49 AM	192.168.2.145	USER	Info	User admin from host 192.168.2.118 via WebUI logged in
January 31, 2022 9:47:55 AM	192.168.2.145	NMC	Info	Network Interface en2 is Up
January 31, 2022 9:47:52 AM	192.168.2.145	SYSTEM	Info	System Reset powerup reason Poweron
January 31, 2022 9:41:49 AM	192.168.2.145	UPS Core	Notice	UPS Output source is on battery. clear
January 31, 2022 9:41:38 AM	192.168.2.145	UPS Core	Major	UPS Output source is on battery.

Figure 17: Event Log Page

The Event Log Actions dropdown menu includes an option to download the event log in csv format.

*m*Power Log

The *m*Power log shows *m*Power specific events, such as device connection errors, bulk operation events, and security events. The events may be filtered by time, source, or severity to allow analysis of specific events.



Timestamp	Source	Severity	Description
January 31, 2022 9:48:22 AM	Device	Warning	Invalid User/Password for 192.168.2.145
January 31, 2022 9:13:17 AM	Device	Warning	Invalid User/Password for 192.168.2.119
January 31, 2022 9:12:10 AM	Device	Warning	Invalid User/Password for 192.168.2.119
January 31, 2022 9:10:20 AM	USER_LOGGED_IN	Info	User admin from host ::1 via WebUI logged in
January 31, 2022 9:10:09 AM	SYSTEM	Warning	Scan Network requires a valid IPv4 address for the start/end range.
January 31, 2022 9:10:08 AM	SYSTEM	Info	Starting mPower Software

Figure 18: *m*Power Log Page

The *m*Power Log Actions dropdown menu includes options to download the *m*Power log in csv format and clear the log.

Bulk Upload Firmware

1. Select **Bulk Upload Firmware** under the **gear** icon.

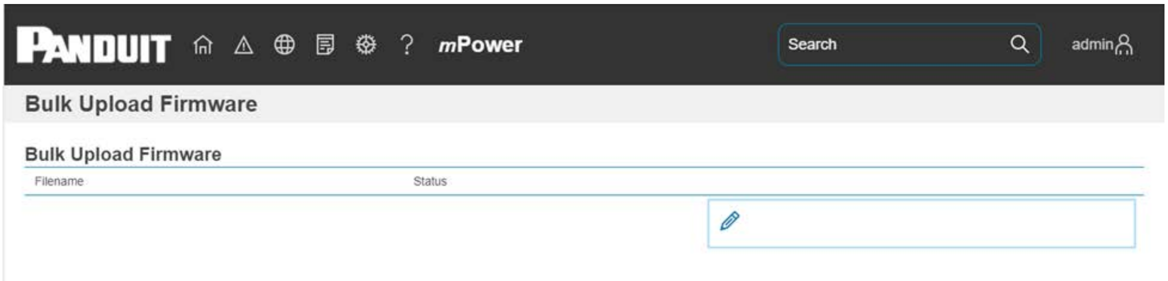


Figure 19: Bulk Upload Firmware

2. Select the **pencil** icon under Bulk Upload Firmware.

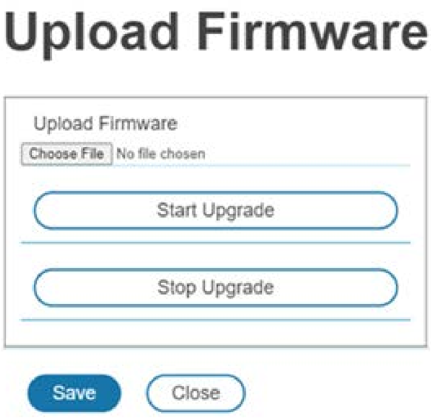
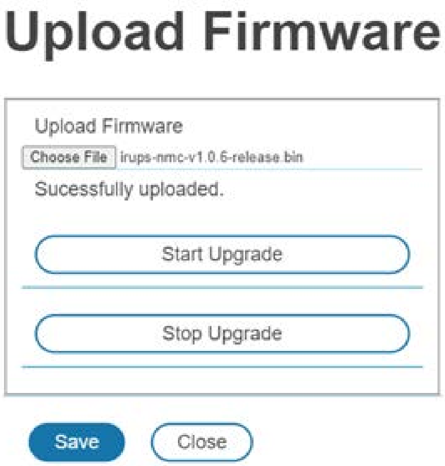


Figure 20: Update Firmware Popup

3. Click **Choose File** and select the new firmware file.

4. When “Successfully Uploaded” is shown, the upgrade file is now stored in *m*Power.



Upload Firmware

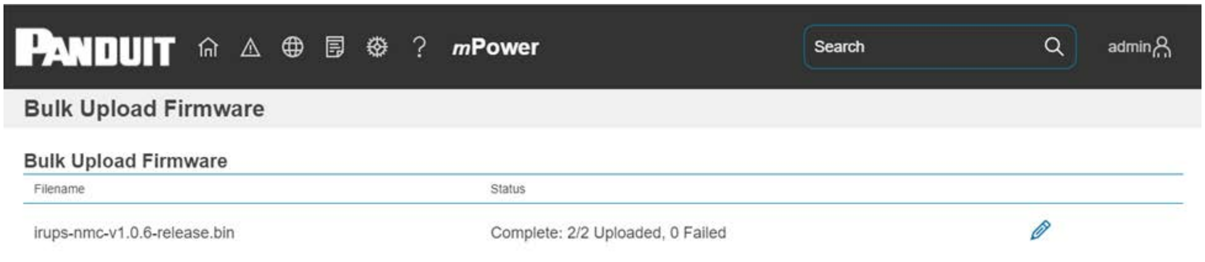
Upload Firmware

Choose File irups-nmc-v1.0.6-release.bin

Sucessfully uploaded.

Figure 21: Ready to upgrade

5. Click **Start Upgrade** to initiate upgrade of all devices managed by *m*Power
6. Monitor the Bulk Upload Firmware Status until uploads to all devices are complete.



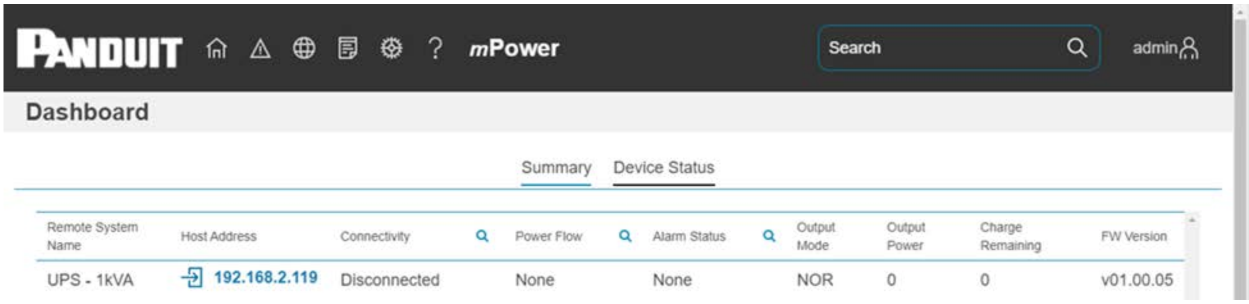
Bulk Upload Firmware

Bulk Upload Firmware

Filename	Status
irups-nmc-v1.0.6-release.bin	Complete: 2/2 Uploaded, 0 Failed

Figure 22: Bulk Upload Firmware Status

7. If any failures are shown, review the *m*Power log under **Logs**
8. Select **Dashboard** under the **home** icon and click the **Device Status** tab
9. Monitor the Device status tab during the reconnection phase. Devices may momentarily show Disconnected during this phase.

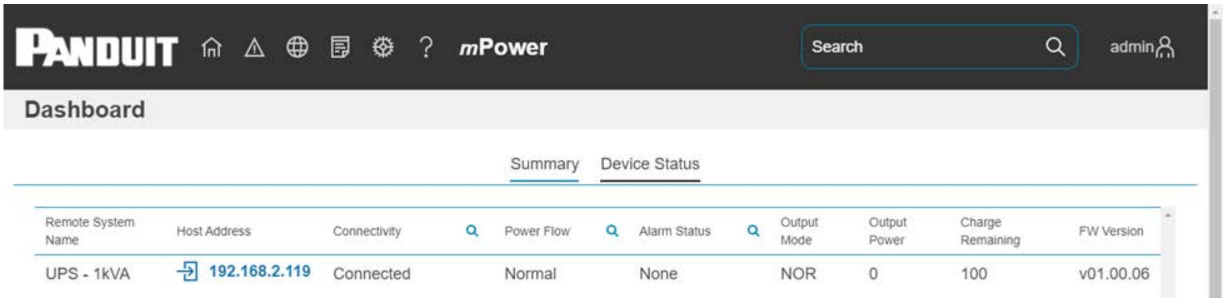


Dashboard

Remote System Name	Host Address	Connectivity	Power Flow	Alarm Status	Output Mode	Output Power	Charge Remaining	FW Version
UPS - 1kVA	192.168.2.119	Disconnected	None	None	NOR	0	0	v01.00.05

Figure 23: Firmware Update In Process

10. When all devices have reconnected, review the FW Version column to ensure all devices were properly upgraded. The reconnection phase will complete in under five minutes.



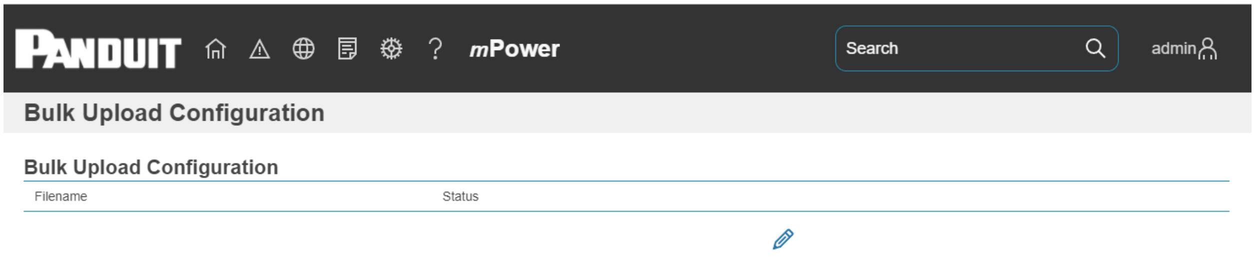
Dashboard

Remote System Name	Host Address	Connectivity	Power Flow	Alarm Status	Output Mode	Output Power	Charge Remaining	FW Version
UPS - 1kVA	192.168.2.119	Connected	Normal	None	NOR	0	100	v01.00.06

Figure 24: Firmware Update Complete

Bulk Upload Configuration

1. Download the config file from a configured device.
    a. Login to a configured device (not *m*Power).
    b. Select **System Management** under the **gear** icon.
    c. Select **Download Configuration**.
2. In *m*Power, select **Bulk Upload Configuration** under the **gear** icon.



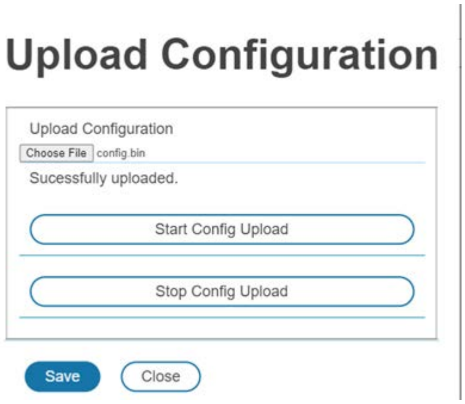
Bulk Upload Configuration

Bulk Upload Configuration

Filename	Status

Figure 25: Bulk Upload Configuration Page

3. Select the **pencil** icon under Bulk Upload Configuration.
4. Click **Choose File** and select a file downloaded from a configured device.
5. When “Successfully Uploaded” is shown, the configuration file is now stored in *m*Power.



Upload Configuration

Upload Configuration

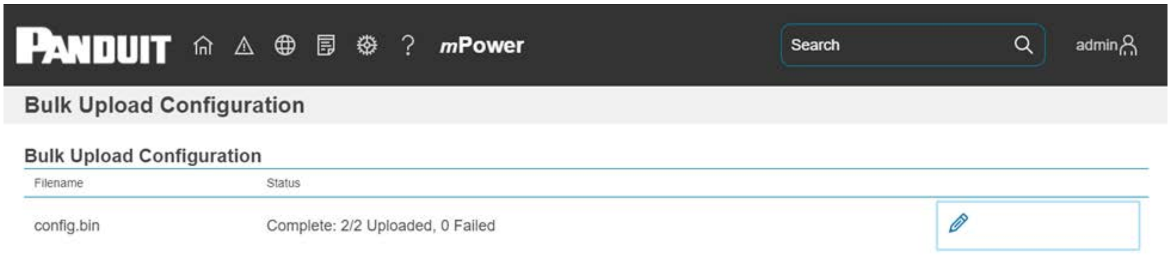
Choose File config.bin

Sucessfully uploaded.

Figure 26: Update Configuration Popup

6. Click **Start Config Upload** and click **OK** in the popup to confirm.

7. Monitor the Bulk Upload Status until uploads to all devices are complete



Bulk Upload Configuration

Bulk Upload Configuration

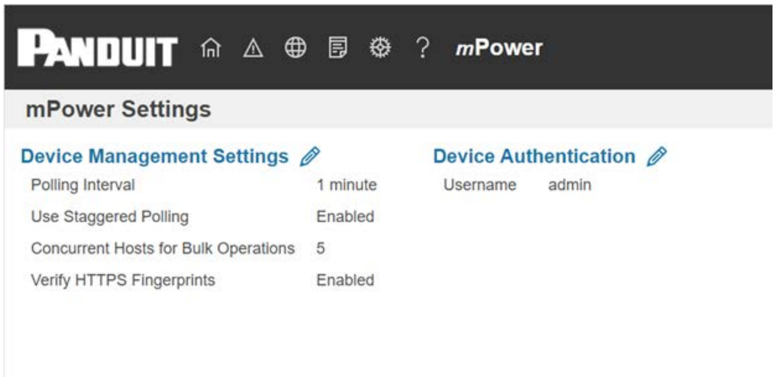
Filename	Status
config.bin	Complete: 2/2 Uploaded, 0 Failed

Figure 27: Update Configuration Complete

8. If any failures are shown, review the *m*Power log under **Logs**.

*m*Power Settings

Select ***m*Power Settings** under the **gear** icon.



mPower Settings

Device Management Settings

Polling Interval	1 minute
Use Staggered Polling	Enabled
Concurrent Hosts for Bulk Operations	5
Verify HTTPS Fingerprints	Enabled

Device Authentication

Username	admin

Figure 28: *m*Power Settings

Device Management Settings Configuration

The default values for Device Management Settings are appropriate for most scenarios. Review the descriptions below if the host network has restrictions that require modifying any of the following.

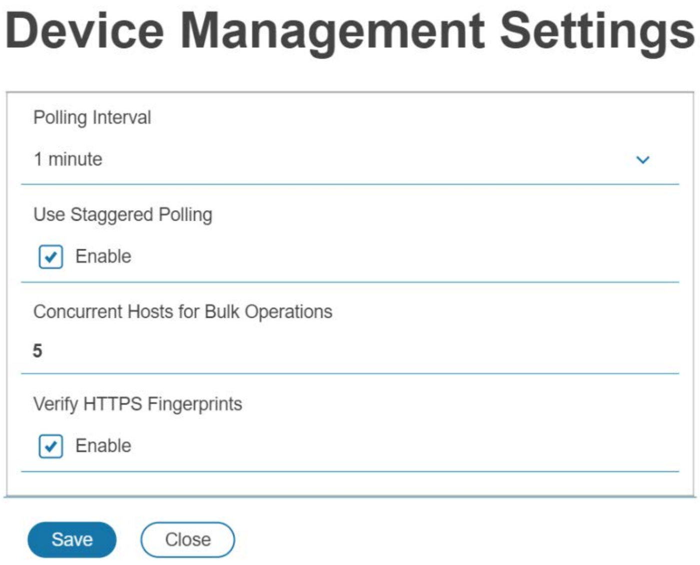
Polling interval: the interval at which *m*Power polls all managed devices.

Staggered Polling: *m*Power completes each device poll before starting the next. If many devices are managed, this may cause the polling interval to be greater than configured.

Concurrent Hosts for Bulk Operations: The number of devices *m*Power will upload firmware or configuration at a time.

Verify HTTPS Fingerprints: When enabled, *m*Power will verify that the device certificate has not changed since configured. If a certificate is changed on the device, the user must delete the existing fingerprint for the device under **Control & Manage** → **Managed Device**. If left blank, when the device is re-enabled, *m*Power will poll the device and store a fingerprint of the new certificate.

1. Select the **pencil** icon next to Device Management.
2. Edit Device Management settings if needed.
3. Click **Save**.



Device Management Settings

Polling Interval
1 minute

Use Staggered Polling
☑ Enable

Concurrent Hosts for Bulk Operations
5

Verify HTTPS Fingerprints
☑ Enable

Figure 29: Device Management Settings

Device Authentication

The username and password must match the credentials created in the managed device to ensure a successful authentication.

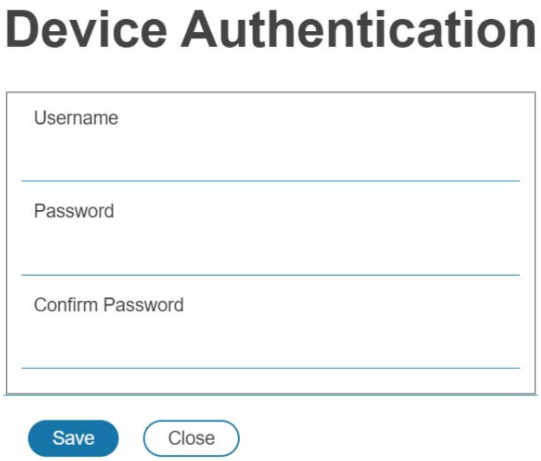


Figure 30: Device Authentication

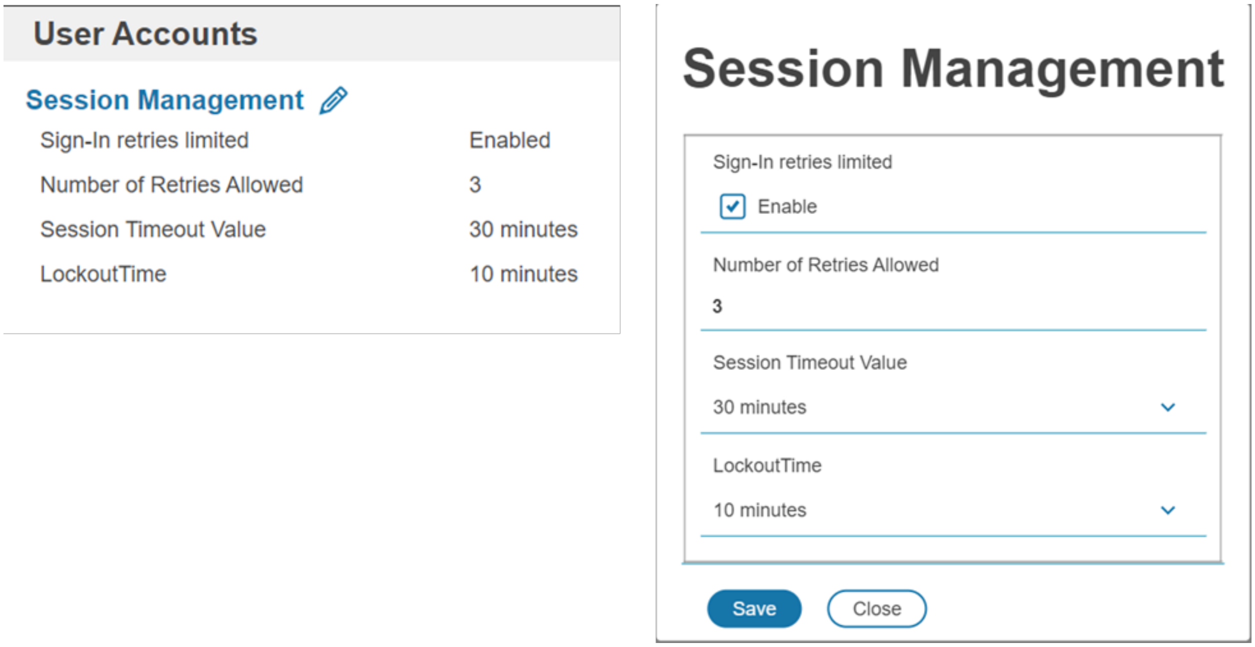
1. Select the **pencil** icon next to **Device Authentication.**
2. Type the device username in the Username box.
3. Type the device password in the Password box.
4. Type the device password in the Confirm Password box.
5. Click **Save**.

User Accounts

Currently, *m*Power is limited to a single user and provides only session management settings under user accounts.

Session Management

Session management provides security settings for the *m*Power user session. Default settings should be acceptable for most installations.



User Accounts

Session Management

Sign-In retries limited	Enabled
Number of Retries Allowed	3
Session Timeout Value	30 minutes
LockoutTime	10 minutes

Session Management

Sign-In retries limited

☑ Enable

Number of Retries Allowed

3

Session Timeout Value

30 minutes

LockoutTime

10 minutes

Figure 31: Session Management

Section 3 – Security

Security is typically top of mind for IT managers when implementing any networked device. The below section is not meant to be comprehensive but rather informative to the areas of security with regards to Panduit SmartZone *m*Power and associated accessories.

*m*Power software stores user-entered data. All data entered by the user is stored in non-volatile storage on the system running the software.

Non-volatile Storage

- File system permissions are used to protect all configuration data.

Authentication Data

- Usernames are stored in plain text 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.)
- The product only communicates with user configured remote servers/devices.

Network Transport Security

- The product uses TLS 1.2 or TLS 1.3 to communicate with user configured remote servers/devices.
- The product uses TLS 1.2 or TLS 1.3 to communicate with HTTPS web browser clients.
- The product stores and checks a fingerprint (hash) of the certificate presented by the configured managed remote server/device to verify remote host authenticity.

Network Configuration Data

- Network Configuration, including Static IP addresses and addresses obtained by DHCP are exposed on "Identification" page and on a Network Configuration page, to aid in network management of the product.
- The product leverages the host operating system's Network Configuration Settings or System Preferences.

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

External Authorization Mechanisms

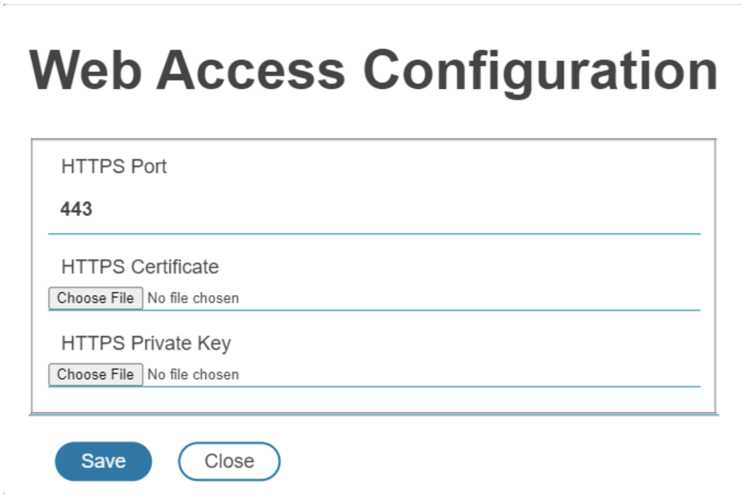
- The *m*Power product manages configuration of managed devices. To access these devices, the IP address or hostname of managed UPSes are stored in non-volatile storage.
- The *m*Power software also collects Event Logs from the managed devices. These event logs contain IP addresses of authentication events from the remote systems.
- The *m*Power software collects and verifies a host fingerprint of managed devices to establish authenticity of the managed device.

Secure Deployment

To maintain the highest level of security, Panduit recommends that the user configure *m*Power with the following settings.

Upload Certificate

Certificates ensure that in a secure connection, the user is connecting to a legitimate service. It is recommended that the X.509 SSL certificate is uploaded to *m*Power and that the certificate has a key strength of 2048 RSA or greater. This area can be accessed from **Settings** → **Network settings**



Web Access Configuration

HTTPS Port
443

HTTPS Certificate
Choose File No file chosen

HTTPS Private Key
Choose File No file chosen

Figure 32: Web Access Configuration Page

Review Session management and password policies

*m*Power gives the customer the flexibility to change session management settings. It is recommended to review the session management settings under **User Accounts**.

Appendix A: Acronyms and Abbreviations

A

Amps/Amperes

AC

Alternating Current

AES

Advanced Encryption Standard

Gb

Gigabyte

GUI

Graphical User Interface

IP

Internet Protocol

kVA

Kilo-Volt-Ampere

kW

Kilowatts

kWH

Kilowatt Hour

LAN

Local Area Network

NMC

Network Management Card

SHA

Secure Hash Algorithms

SSL

Secure Sockets Layer

TCP/IP

Transmission Control Protocol/Internet Protocol

TLS

Transport Layer Security

UPS

Uninterruptible Power Supply

V

Volts

W

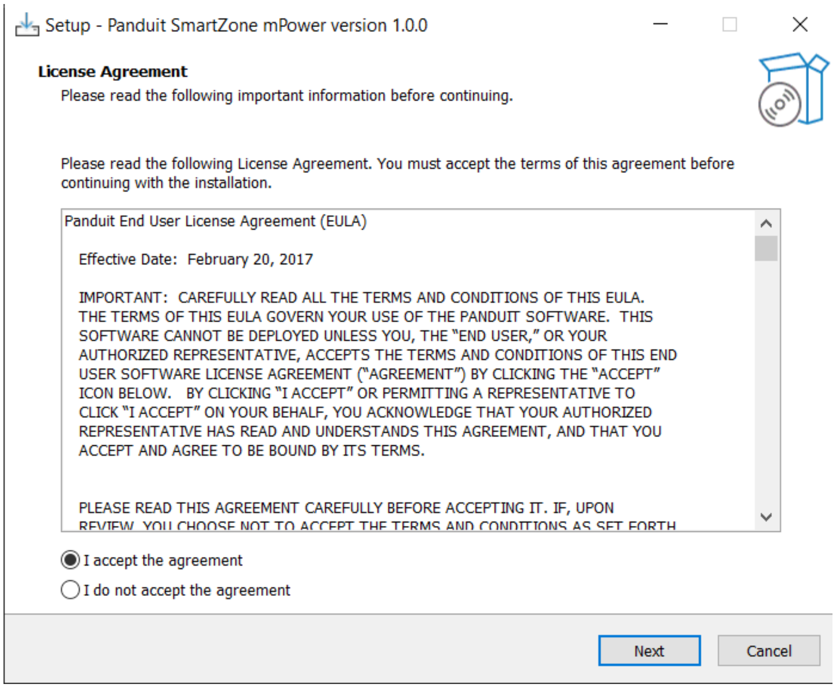
Watts

Appendix B: Installation

Installing *m*Power

1. Double click / Run the installer.

2. Review the license agreement and accept if the terms are acceptable. Click **Next**.



Setup - Panduit SmartZone mPower version 1.0.0

License Agreement

Please read the following important information before continuing.

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

Panduit End User License Agreement (EULA)

Effective Date: February 20, 2017

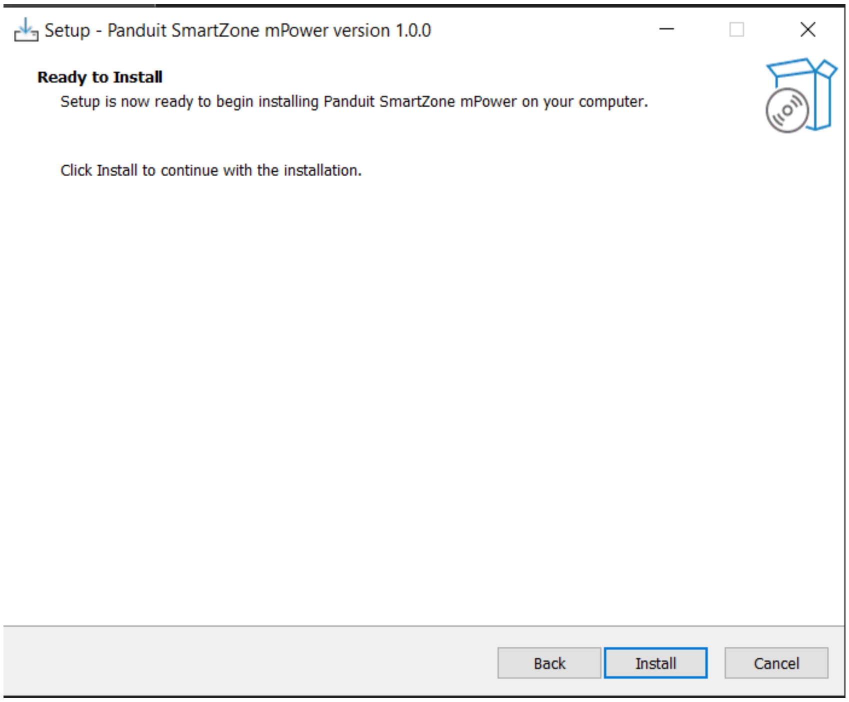
IMPORTANT: CAREFULLY READ ALL THE TERMS AND CONDITIONS OF THIS EULA. THE TERMS OF THIS EULA GOVERN YOUR USE OF THE PANDUIT SOFTWARE. THIS SOFTWARE CANNOT BE DEPLOYED UNLESS YOU, THE "END USER," OR YOUR AUTHORIZED REPRESENTATIVE, ACCEPTS THE TERMS AND CONDITIONS OF THIS END USER SOFTWARE LICENSE AGREEMENT ("AGREEMENT") BY CLICKING THE "ACCEPT" ICON BELOW.   BY CLICKING "I ACCEPT" OR PERMITTING A REPRESENTATIVE TO CLICK "I ACCEPT" ON YOUR BEHALF, YOU ACKNOWLEDGE THAT YOUR AUTHORIZED REPRESENTATIVE HAS READ AND UNDERSTANDS THIS AGREEMENT, AND THAT YOU ACCEPT AND AGREE TO BE BOUND BY ITS TERMS.

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE ACCEPTING IT. IF, UPON REVIEW, YOU CHOOSE NOT TO ACCEPT THE TERMS AND CONDITIONS AS SET FORTH

● I accept the agreement

○ I do not accept the agreement

3. Click **Install** to continue.



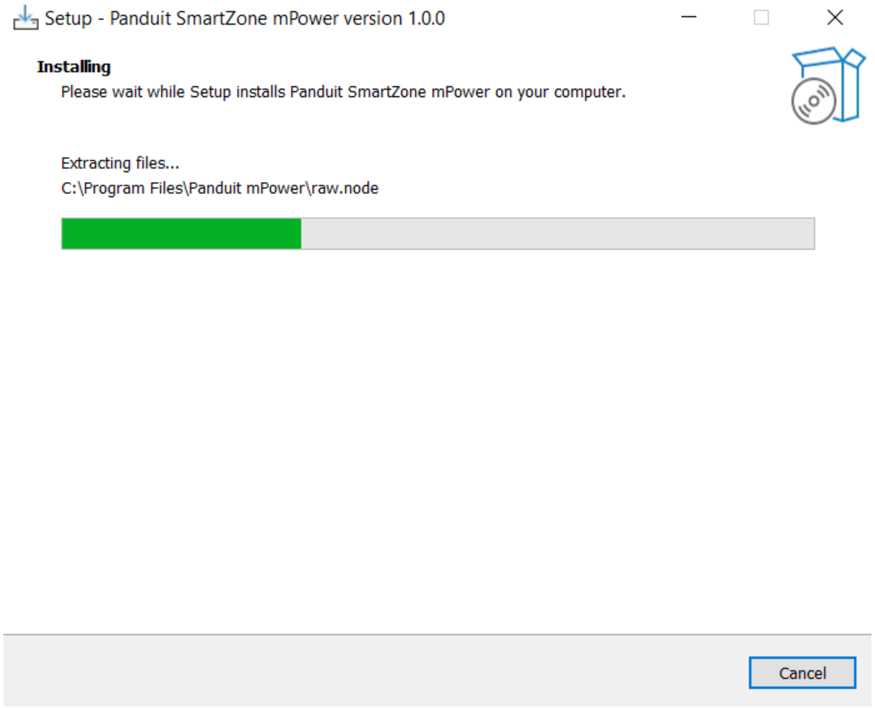
Setup - Panduit SmartZone mPower version 1.0.0

Ready to Install

Setup is now ready to begin installing Panduit SmartZone mPower on your computer.

Click Install to continue with the installation.

4. Wait while files are copied to the computer.



Setup - Panduit SmartZone mPower version 1.0.0

Installing

Please wait while Setup installs Panduit SmartZone mPower on your computer.

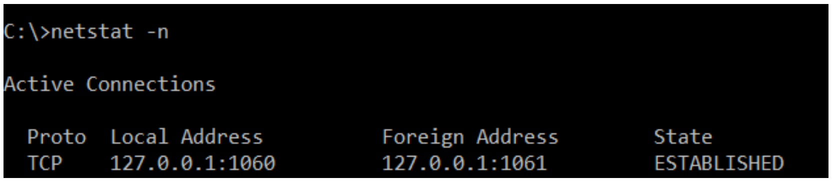
Extracting files...
C:\Program Files\Panduit mPower\raw.node

5. Enter the TCP port that *m*Power should use. The default is “443’, which is the

standard HTTPS port. If the computer is already running another HTTPS server, choose another port that is not in use.

Optional: Discover open ports.

- Open a command prompt and run:
  netstat -n
- Ports in use are shown after the colon in the “Local Address” column.



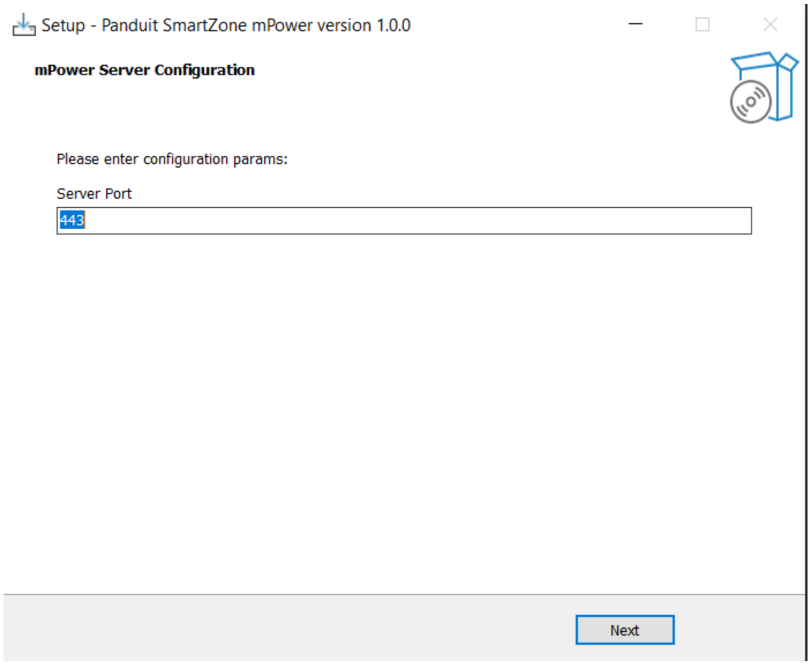
```
C:\>netstat -n

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:1060         127.0.0.1:1061         ESTABLISHED
```

In the example above, the port in use is “1060”.

- Choose 443 or any port 1024-49151 that is not in use.



Setup - Panduit SmartZone mPower version 1.0.0

mPower Server Configuration

Please enter configuration params:

Server Port: 443

6. Select any post installation options desired:

   a. Install Bonjour.

      Bonjour is required to use the auto-discovery feature built into *m*Power.

      Auto-discovery will fail if it is not installed.

b. Install Firewall Rule.

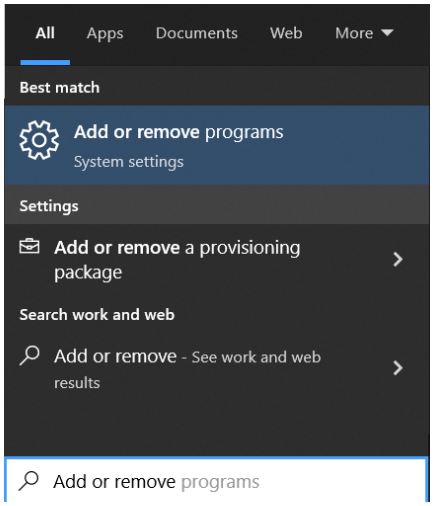
   Check this option if *m*Power should be accessible remotely. It will install a rule in the Windows firewall that allows remote devices to access *m*Power.

c. Start SmartZone *m*Power Service.

   Leave this option checked to start the *m*Power service immediately.

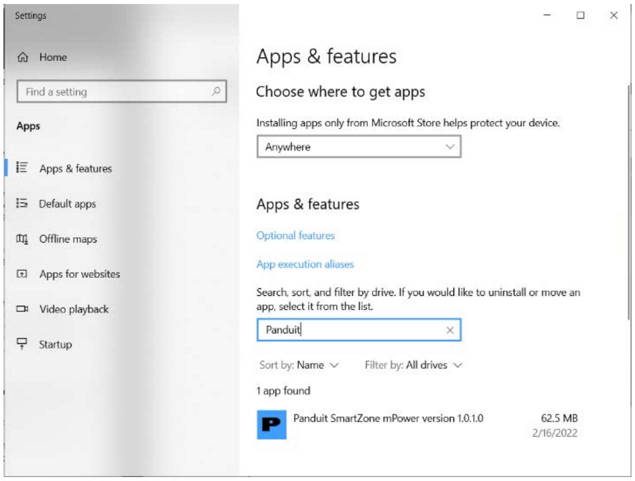
Appendix C: Uninstalling *m*Power

1. Launch the Windows **Add or remove programs** application.



Add or remove programs

2. Search for Panduit Applications.



Installing apps only from Microsoft Store helps protect your device.

Anywhere

Search, sort, and filter by drive. If you would like to uninstall or move an app, select it from the list.

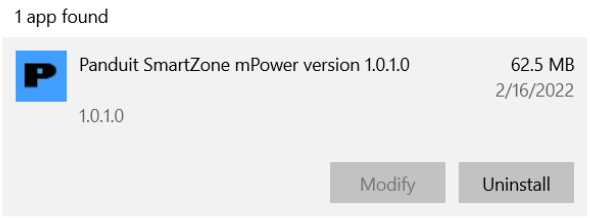
Panduit

Sort by: Name   Filter by: All drives

1 app found

Panduit SmartZone mPower version 1.0.1.0   62.5 MB   2/16/2022

3. Click on Panduit SmartZone *m*Power, then click uninstall.



4. Click **Uninstall** & allow “Setup/Uninstall” to make changes.

5. Click **Yes** to confirm *m*Power should be removed.

6. Click **OK** to acknowledge the uninstall is complete.

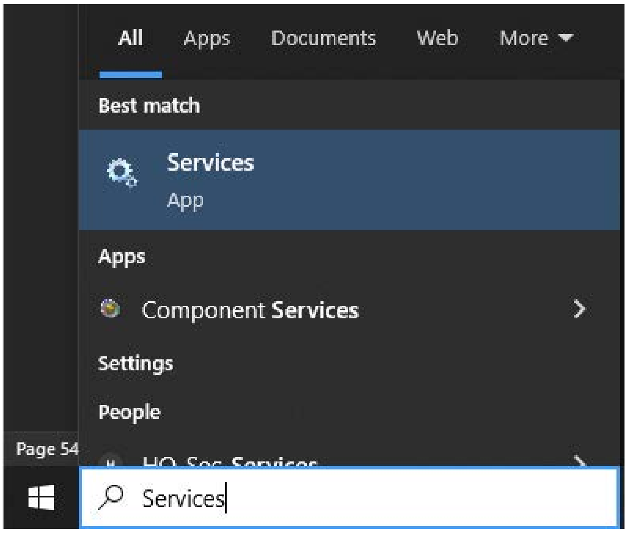
7. Optionally, to remove all configuration files:
    a. Open the Windows **File Explorer** application.
    b. Navigate to C:\ProgramData.
    c. Delete the Panduit *m*Power directory.

Appendix D: Password Recovery

The *m*Power password may be manually reset by stopping the *m*Power service, manually deleting the password file, and restarting the password service.

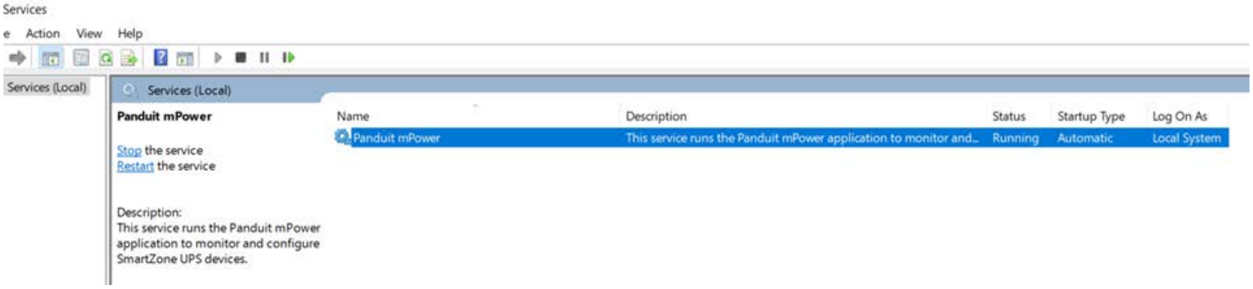
Note: Instructions refer specifically to Windows 10. Please refer to your operating system documentation if you are not using Windows 10.

1. Type **services** into Windows Search and select **Services**.



Services

2. Click the **Services** application. Find the Panduit *m*Power Service.



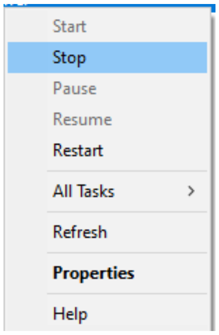
Panduit mPower

Stop the service
Restart the service

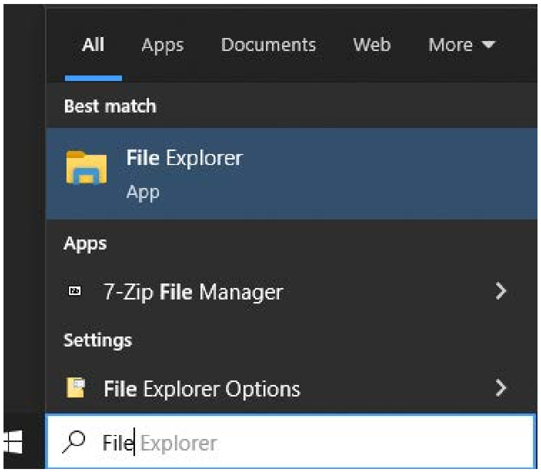
Description:
This service runs the Panduit mPower application to monitor and configure SmartZone UPS devices.

Name	Description	Status	Startup Type	Log On As
Panduit mPower	This service runs the Panduit mPower application to monitor and...	Running	Automatic	Local System

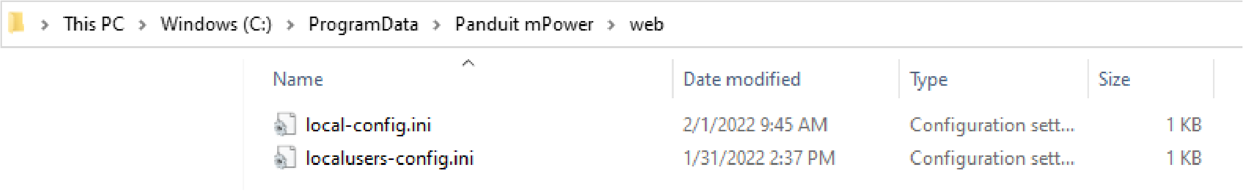
3. Right click on the **Panduit *m*Power Service** and select **Stop**.



4. Open **File Explorer**.



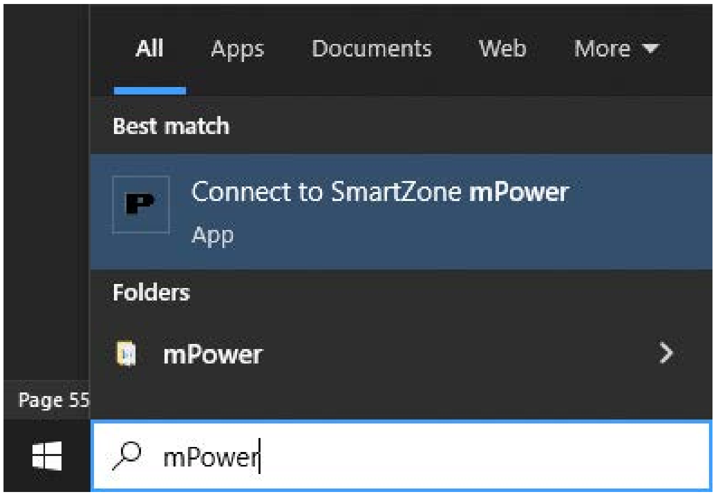
5. Navigate to c:\ProgramData\Panduit *m*Power\web.



This PC > Windows (C:) > ProgramData > Panduit mPower > web

Name	Date modified	Type	Size
local-config.ini	2/1/2022 9:45 AM	Configuration sett...	1 KB
localusers-config.ini	1/31/2022 2:37 PM	Configuration sett...	1 KB

6. Right click on localusers-config.ini and select **Delete**.
7. Navigate back to the services application.
8. Right clock on Panduit *m*Power and select **Start**.
9. Open *m*Power using the search bar.

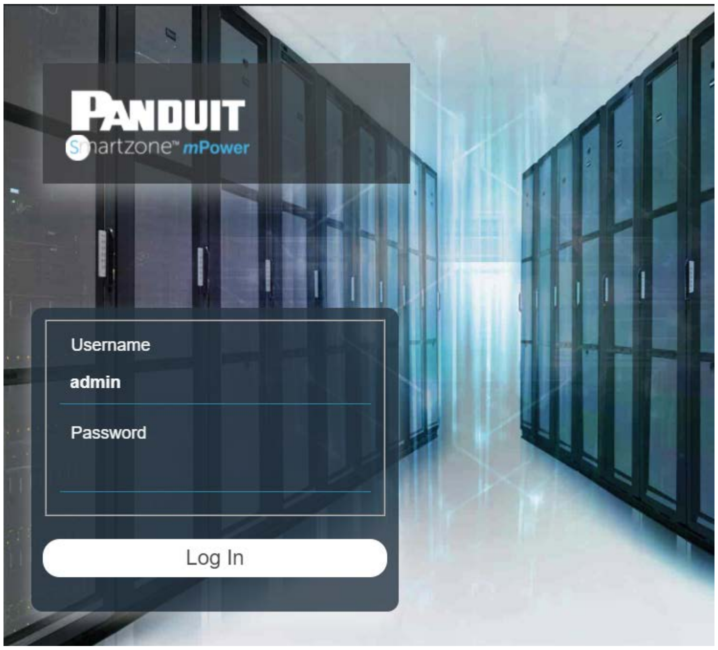


mPower

10. Login using the default credentials:

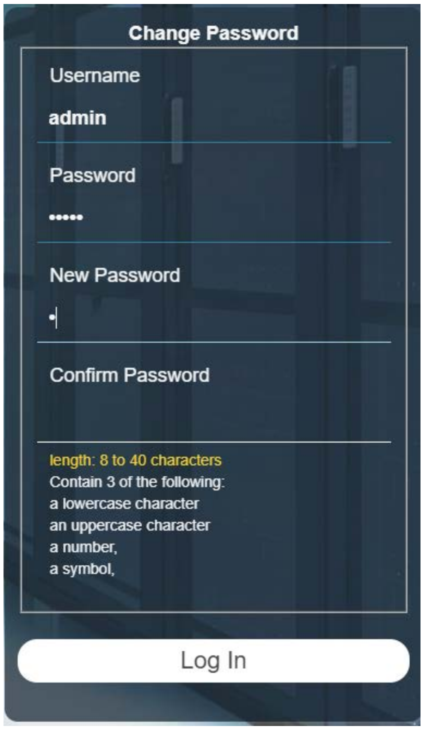
    Username: admin

    Password: admin



Username
admin
Password

11. Enter the default credentials again and enter a new password for the ‘admin’ user.



Change Password

Username

admin

Password

•••••

New Password

•

Confirm Password

length: 8 to 40 characters
Contain 3 of the following:
a lowercase character
an uppercase character
a number,
a symbol,

12. Click **Login**.

Appendix D: System Reset

Restoring *m*Power to the initial configuration is best done by uninstalling, deleting the configuration files, then reinstalling.

1. Uninstall by following the instructions in *Appendix C: Uninstalling mPower*. Follow the optional instructions to delete C:\ProgramData\Panduit *m*Power.
2. Reinstall by following the instructions in *Appendix B: Installation*.

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

UPS Technical Support

- UPS Selection
- Competitor Cross references
- Product Documentation

Email: TechSupport@panduit.com

Europe / Middle East

Customer Service

- Price & Availability
- Expedites

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

UPS Technical Support

- UPS Selection
- Competitor Cross references
- Product Documentation

Email: TechSupportEMEA@panduit.com

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

PANDUIT™