

User's Guide

PowerAlert® Device Manager (PADM) 20.0.0

WARRANTY REGISTRATION

Register your product today and be automatically entered to win an ISOBAR® surge protector in our monthly drawing!

tripplite.com/warranty



1111 W. 35th Street, Chicago, IL 60609 USA • tripplite.com/support

Copyright © 2021 Tripp Lite. All rights reserved.

Table of Contents

1. Introduction		4.7 Security	48
1.1 System Requirements	3	4.7.1 Session Management	48
2. Initial Configuration		4.7.2 User Accounts	48
2.1 IP Address Assignment	4	4.7.3 Roles & Privileges	53
2.2 Saving Configuration Changes	5	4.7.4 Security Settings	54
2.3 Default UPS System Shutdown Settings	5	4.8 Logs	
2.4 SNMP Configuration	6	4.8.1 Accounting Log	56
3. Web Interface		4.8.2 Application Log	57
3.1 Accessing the Web Interface	7	4.8.3 Data Log	58
3.2 PADM Overview	8	4.8.4 Event Log	62
3.3 Top Menu	14	4.8.5 Syslog	63
4. Main Menu		5. Technical Support	
4.1 Dashboard	25	Appendix A –	
4.2 Device	27	Privileges Chart	65
4.3 Loads	30	Appendix B –	
4.4 Batteries	33	Supplemental Information	68
4.5 Events & Actions	36	Appendix C –	
4.6 Network	45	SNMP Commands	69
4.6.1 Internet	45		
4.6.2 Services	46		
4.6.3 SMTP	46		

1. Introduction

Tripp Lite LX Platform devices contain an Ethernet network interface that enables remote configuration, monitoring and control of the device. These functions can be performed using the device's web interface, Command Line Interface (CLI) or by using SNMP-based management software applications offered by Tripp Lite and other vendors. This User's Guide focuses on configuration and management using the web interface, commonly referred to as PowerAlert® Device Manager (PADM).

This User's Guide covers PADM version 20.0.0 and later. For previous PADM versions (15.x.x.), refer to the LX Platform User's Guide (part number 93-35A4).

For information about the Command Line Interface for PADM version 20.0.0 and later, refer to the PADM20 CLI User's Guide (part number 93-3C86).

Notes: Previous versions (15.x.x) of PADM supported a Telnet/SSH/Console menu-driven text interface. Starting with PADM version 20.0.0, the menu-driven text interface is replaced by a full-featured CLI (command line interface).

- PADM version 20.0.0 introduces support of a RESTful Application Programming Interface (API). Contact Tripp Lite Technical Support for details.
- See Appendix B for information about PADM20 operational scenarios, such as firmware update from 15.x and moving a WEBCARDLX from one device to another.

1.1 System Requirements

- A Tripp Lite LX Platform Device, such as WEBCARDLX, PDU3E-series PDUs, PDU3XE-series PDUs, LX suffix PDUs and LX-compatible cooling products

Note: If updating to PADM20 from a previous firmware version, ensure the device is running version 15.5.2 or later. If the device is running 15.5.1 or earlier, update it to 15.5.7 prior to updating to PADM20.

- Ethernet network that supports the TCP/IP protocol
- One of the following options for remote configuration, monitoring and control:
 - o Web browser (Chrome, Firefox, Internet Explorer or Safari); desktop and mobile environments are supported
 - o VT-100 terminal emulator client for Telnet, SSH, and/or Serial connections (to access CLI)

Warning: Use of this equipment in life support applications where failure of this equipment can reasonably be expected to cause the failure of the life support equipment or to significantly affect its safety or effectiveness is not recommended.

Note: PADM applies the following security policies:

- On initial login with any of the pre-configured local users, **localadmin**, **localmanager** or **localguest**, PADM will force the user to change the default password.
- The preconfigured SNMPv1 and SNMPv2c users, **public** and **tripplite** respectively, are disabled by default.
- The default Authorization Password and Privacy Passphrase of the pre-configured SNMPv3 users, **localadmin**, **localmanager** or **localguest**, must be changed prior to use.

2. Initial Configuration

This section provides instructions for configuring the device's network access parameters. During the process, the device's MAC address may be required. The 12-character address (in the format XX XX XX XX XX XX) is printed on a label found on the LX Platform device.

- For devices using WEBCARDLX, the label is attached to the underside of the card
- For devices with an embedded LX interface, the label is typically affixed to the device enclosure

For instructions on loading PADM firmware or device driver updates, refer to the applicable release notes. Related documentation can be downloaded from the Tripp Lite website: triplite.com. Enter the model name of the LX Platform device in the search bar; on opening the device's product page, refer to the "Resources & Downloads" section. Ensure the LX Platform device is turned on.

2.1 IP Address Assignment

PADM supports both dynamic (DHCP) and manual IP address assignment; refer to the appropriate section below. If uncertain as to which method to use, contact your network administrator for assistance.

Dynamic IP Address Assignment

Using a standard Ethernet patch cable, connect the LX Platform device's Ethernet port to the network environment in which the DHCP server is running. The device will attempt to obtain an IP address via DHCP; this may take several minutes, depending on network performance. To learn which IP address has been assigned, contact your network administrator and provide the device's MAC address..

Notes:

- Consider requesting a long-term lease period for the IP address, depending on application.
- PADM supports IPv4 and IPv6. By default, PADM is set to receive both IPv4 and IPv6 addresses via DHCP

Static IP Address Assignment

PADM supports a single static IPv4 address (requires setting the IP address, subnet mask and gateway) and/or a single static IPv6 address. In addition, PADM can support a single static IPv4 or IPv6 DNS address (requires setting the primary DNS address, and optionally a secondary DNS address). If PADM is not assigned an IP address manually or via DHCP, it will use the default static IP address of 169.254.0.1 with a subnet mask of 255.255.0.0. Using a standard Ethernet patch cable, connect the LX Platform device's Ethernet port to the network environment. From a computer operating in the same environment, launch a web browser and enter **169.254.0.1** in the address bar. When the PADM login screen appears, enter **localadmin** for both the name and password*. Navigate to the Network > Internet menu, then overwrite the default IP address with the desired static IP address (Figure 2-1).

***Note:** On initial login, you will be required to change the password.



IPv4	
	Manual (Static IP)
Address:	10.22.0.135
Subnet Mask:	255.224.0.0
Gateway:	10.0.0.1

Figure 2-1: Assignment of a Static IPv4 Address

2. Initial Configuration

2.2 Saving Configuration Changes

Most configuration changes saved in PADM take effect immediately; PADM will typically indicate if a reboot is required for changes to take effect. Regardless, rebooting PADM is recommended to ensure that configuration changes persist. See section **3.3 Top Menu** for instructions on rebooting PADM. Rebooting PADM does not power cycle the device or any outlet on the device.

2.3 Default UPS System Shutdown Settings

WEBCARDLX and LX Platform UPS systems are pre-configured to shut down the device two minutes after receiving one of the following alert signals from the UPS:

- Low Battery
- Temperature High

To modify or disable this setting, navigate to the Events & Actions > Action menu and edit the *Default Device Shutdown* line item by clicking on its pencil icon (Figure 2-2).

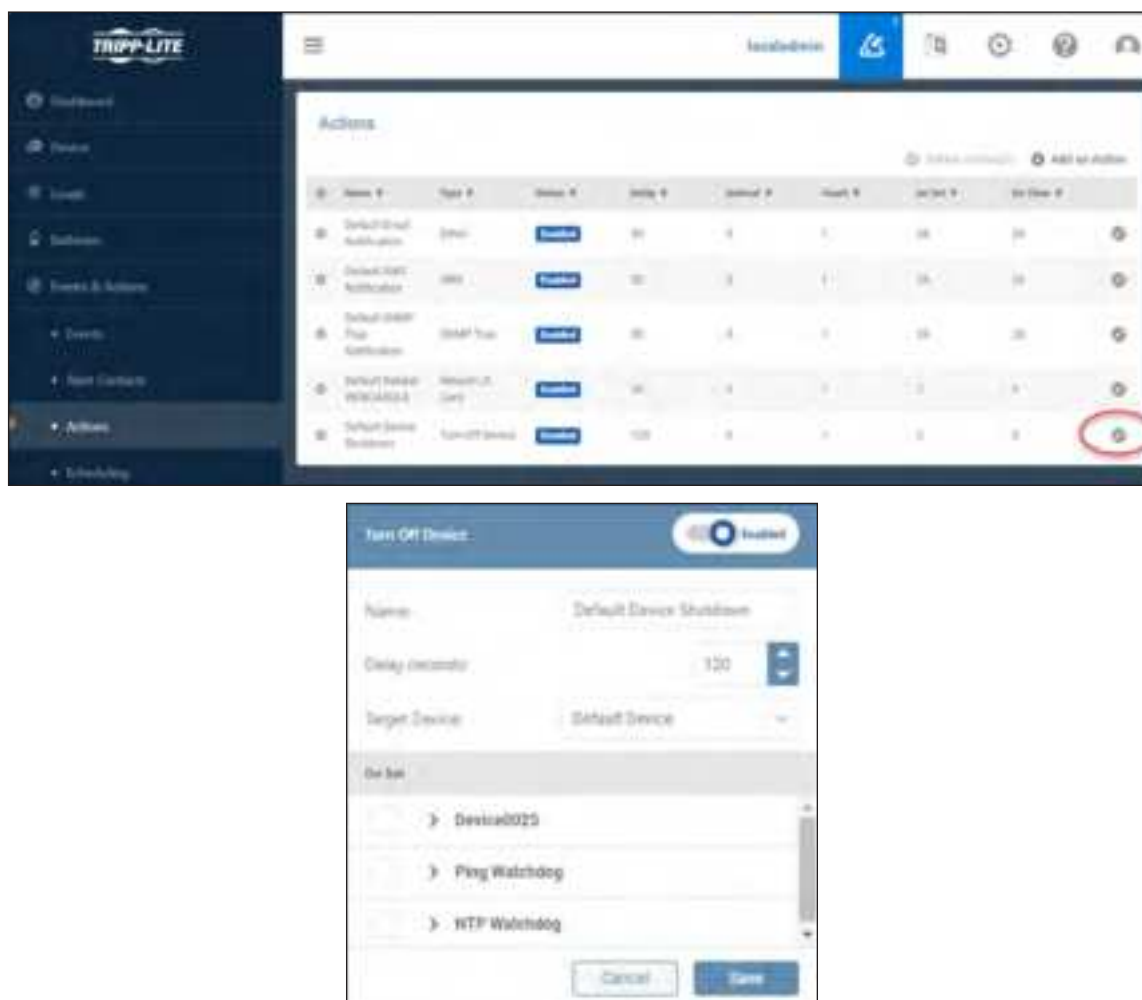


Figure 2-2: Setting the Default Device Shutdown Parameters

2. Important Safety Instructions

2.4 SNMP Configuration

PADM uses an embedded SNMP agent and Management Information Bases (MIBs) to support management over the network. The SNMP agent responds to standard SNMP commands (Get, Get Next and Set) and can generate SNMP traps (messages). The MIBs determine which parameters can be monitored and controlled. Three MIB files—TRIPPLITE.MIB, TRIPPLITE-PRODUCTS.MIB and RFC-1628-UPS.MIB—must be imported to each Network Management System (NMS) station that will be monitoring/controlling the LX Platform device. The MIB files can be downloaded from the PADM20 Top Menu > Help or from tripplite.com/support.

Note: *SNMP Users are configured in the SNMP Users tab of the Security > User Accounts menu item.*

SNMPv1 & v2c Definitions

Username:

A general name for the user. This data is not included in network communications

Community:

The key required for responses to Set or Get requests. The Community name must be between 6 and 32 ASCII characters; alphanumeric and the following special characters are allowed: !"#%&'()*+,-./:;?@[\\]^_`{|}~.

Role:

Each Role contains a set of predefined Privileges related to device functions. In order to issue Set commands --for example, load control – the SNMP User must be assigned a Role with the corresponding Privileges. See Appendix A for more details about Roles and Privileges.

SNMPv3 Definitions

Username:

The identifier of the user profile. SNMPv3 maps Gets, Sets and Traps to a user profile by matching the username of the profile to the username in the data packet being transmitted. The username cannot exceed 32 ASCII characters; alphanumeric and the following special characters are allowed: !@#%&'()*+,-./:;?@[\\]^_`{|}~.

Security Level:

The Tripp Lite implementation of SNMPv3 supports three security levels: No Authentication No Privacy (NoAuthNoPriv), Authentication No Privacy (AuthNoPriv) and Authentication Privacy (AuthPriv)

Auth. Protocol:

The Tripp Lite implementation of SNMPv3 supports MD5 and SHA authentication.

Auth. Passphrase:

A phrase of 8 to 32 ASCII characters (alphanumeric and !"#%&'()*+,-./:;?@[\\]^_`{|}~) that verifies the authenticity of the NMS. It also verifies that the message has not been changed during transmission, or that the message was communicated in a timely manner (not delayed nor copied and resent later at an inappropriate time).

Privacy Passphrase:

A phrase of 8 to 32 ASCII characters (alphanumeric and !"#%&'()*+,-./:;?@[\\]^_`{|}~) that ensures the privacy of the data (by means of encryption) sent via SNMPv3 between the NMS and the device.

Privacy Protocol:

The Tripp Lite implementation of SNMPv3 supports the AES and DES protocols for encrypting and decrypting data.

Role:

Each Role contains a set of predefined Privileges related to device functions. In order to issue Set commands --for example, load control – the SNMP User must be assigned a Role with the corresponding Privileges. See Appendix A for more details about Roles and Privileges.

3. Web Interface

3.1 Accessing the Web Interface

Use the following steps to access the PowerAlert Device Manager web interface

1. Open a web browser.
2. In the address bar, enter the IP address assigned to the LX Platform device.
3. In the login page that appears (Figure 3-1) enter the User Name and Password (case-sensitive), then click the **Login** button.

The default Administrator Username and Password are both **localadmin**. Note that on initial login, you will be required to change the password.



Figure 3-1: Login Page

3. Web Interface

On logging in, the Dashboard page is displayed (Figure 3-2).



Figure 3-2.: Dashboard Page

3.2 PADM Overview

PADM Layout

The PADM web interface is comprised of three main sections (Figure 3-3):

- 1 Top Menu – Alert summary and administrative functions
- 2 Main Menu – Navigation to device management functions
- 3 Content– Information reflective of selections made in the Main Menu or Top Menu

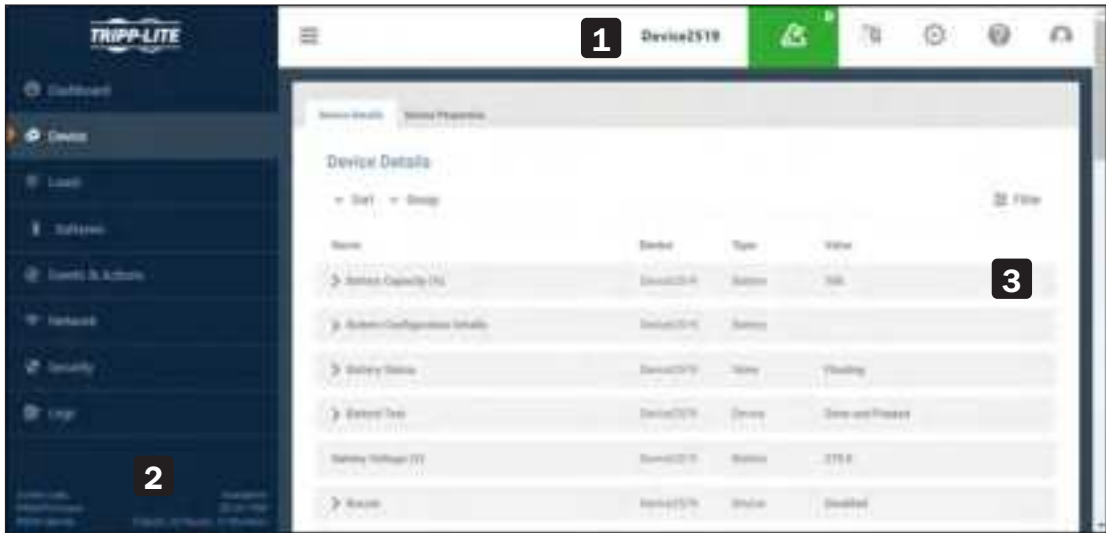


Figure 3-3: PADM Web Interface Main Sections

3. Web Interface

Navigation Elements

A number of graphical elements are used for navigation throughout the interface.

Sub-Menus – Certain menu items contain sub-menus. Click a menu item to expand the selection, displaying its sub-menu (Figure 3-4). Click the menu item again to contract the sub-menu.

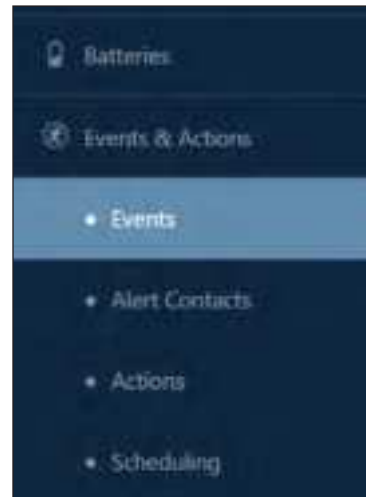


Figure 3-4: Sub-Menus

Tabs – Tabs are used to organize information of a common topic into logical groupings (Figure 3-5). Select a tab to view its content.

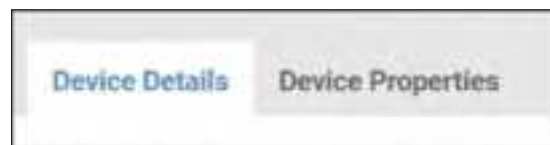


Figure 3-5: Tabs

Pages – Sequenced numbers with arrows indicate that the content exceeds one page (Figure 3-6). Select each to navigate pages as follows:

-  Go to the first pages of the content
-  Go to the previous page number
- Number** Go directly to the selected page
-  Go to the next page.
-  Go to the last page of the content



Figure 3-6: Pages

Scroll Bars – In cases where content exceeds the size of the window, vertical and/or horizontal scroll bars appear (Figure 3-7).

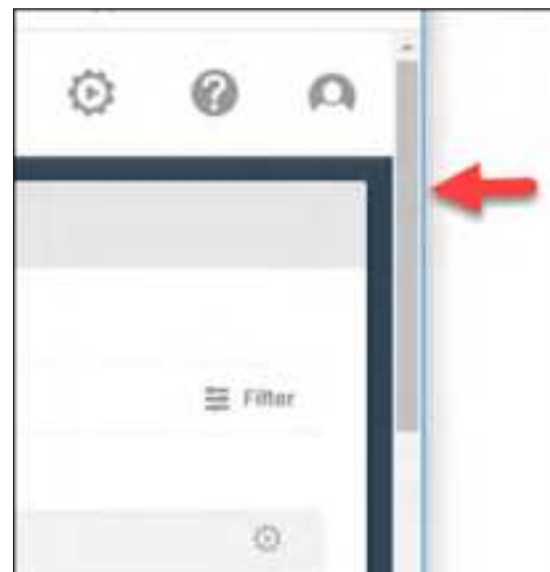


Figure 3-7: Scroll bars

3. Web Interface

Chevrons – Click the chevron next to an item to expand or contract the content of the item (Figure 3-8).



Figure 3-8: Chevrons

Adjusting Views

Sorting – When content is displayed in table format, the information can be sorted in the following manners (Figure 3-9):

- **Columns** – Click a column title to sort the table by that category, in ascending order.
- **Arrows** – Click the up or down arrow adjacent to a column title to sort the table in ascending or descending order, respectively.

Load # 	Name 	Group 
--	--	---

Figure 3-9: Columns and arrows

Filters – Click **Filter** to open a dialog box in which a variety of filtering options can be selected. Click the **Apply Filters** button to update the displayed information. It should be noted that applied filters persist, even after logout/login. Click the **Clear Filters** button to restore the default view (Figure 3-10).

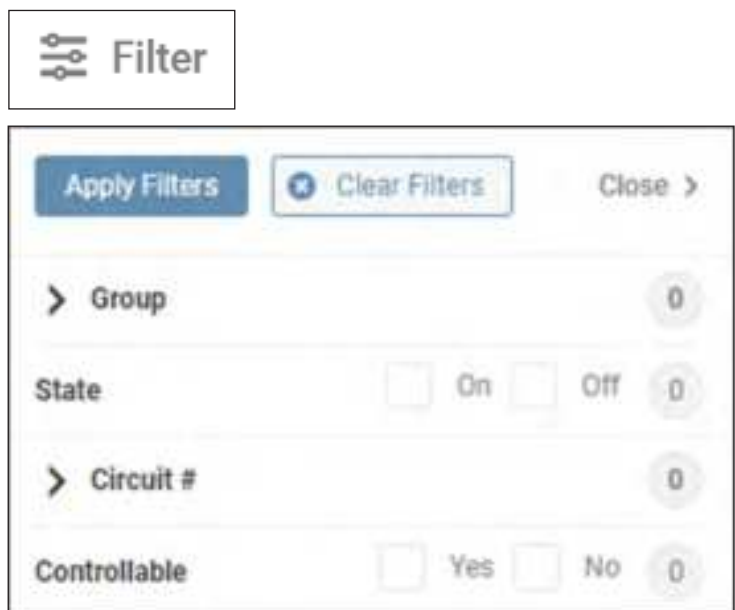


Figure 3-10: Filter functions

3. Web Interface

Columns – Click **Columns** (in Loads) to open a menu of applicable column titles (Figure 3-11). Select or unselect the preferred column titles, then click anywhere on the screen.

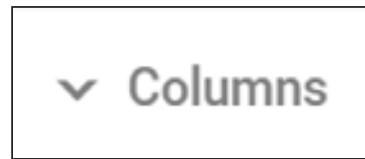
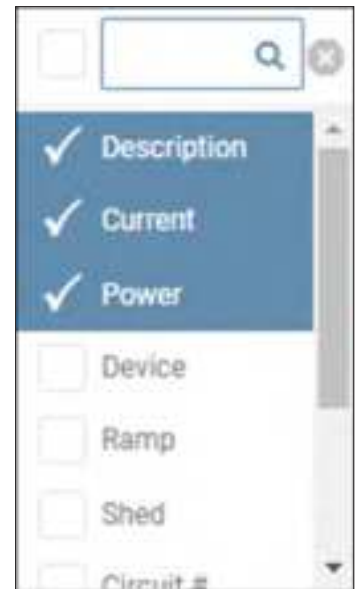


Figure 3-11: Columns



View – Click **View** (in Data Log) to open a menu of variables (Figure 3-12). Select or unselect the preferred variables, then click the Save button

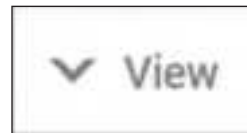


Figure 3-12: View



Refresh – Click **Refresh** to update the displayed content (Figure 3-13).

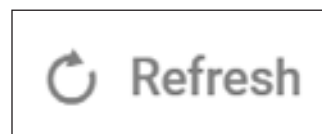


Figure 3-13: Refresh

Export – Click **Export** to configure and generate an export of the contents (Figure 3-14).



Figure 3-14: Export

3. Web Interface

Icons

Pencil – The pencil icon indicates that the item can be edited (Figure 3-15). Click the icon to open a dialog box in which the edits can be made.



Figure 3-15: Edit

Details – The 'i' icon indicates that the item contains details (Figure 3-16). Click or mouse over the icon to view the details.



Figure 3-16: Details

Control – The gear icon indicates that a control can be executed (Figure 3-17). Mouse over the icon to view a description of the control. Click on the icon to execute the action.



Figure 3-17. Control

Delete – The  icon indicates the item can be deleted (Figure 3-18). Click the icon to mark the item for deletion; the action will change the icon color to red. To complete the deletion, click the Delete xxx button (also in red).



Figure 3-18: Delete icon and Delete (Confirmation) Button.

Sliders – Sliders allow the state of the item to be manually changed. Colors and symbols reflect the condition or state of the item. Figure 3-19 shows the following sliders, from left to right: Load On, Load Off, Load Mixed State, Load On - Cycling, Load Off - Cycling, Load On - Disabled, Load Off - Disabled, Item Enabled, Item Disabled



Figure 3-19: Slider States and Colors

3. Web Interface

Tags – Colored shape tags indicate the severity of Events and Alerts (Figure 3-20):

red octagon = Critical,
blue circle = Informational,
yellow triangle = Warning.



Figure 3-20: Tags

Checkmark – Used in the in Alert summary, a blue Checkmark indicates that an item has been cleared or acknowledged (Figure 3-21).



Figure 3-21: Checkmark

3. Web Interface

3.3 Top Menu

The Top Menu is used for viewing Alerts and performing administrative functions (Figure 3-22).

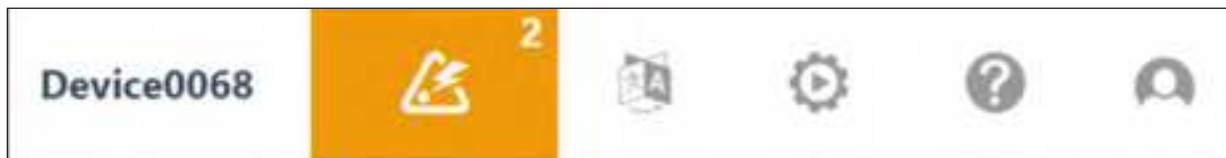


Figure 3-22: Top menu

Alerts

The Alerts icon is located to the right of device name (Figure 3-22). The icon's color (matching Tags) indicates the highest severity level of all active Alerts. The number in the upper right corner of the icon indicates the quantity of active Alerts. Click the icon to display a list of active Alerts for the device as well as any peripherals (e.g. sensors) connected to it (Figure 3-23). An Alert is active if it has not been acknowledged, nor cleared. An Alert clears when the condition that triggered the Alert is no longer in effect. An Alert can be acknowledged in one of two ways: automatically (configured in Events & Actions > Events) or manually. To manually acknowledge one or more Alerts, select the checkboxes in the **Ack.** column, then click the **Save** button. To manually acknowledge all Alerts, click the icon in the **Ack** column title, then click the **Save** button. Once an Alert has been both cleared and acknowledged, it is removed from the list. By default, the list is sorted by Date/Time, in descending order, i.e. the most recent Alerts appear at the top of the list.



Figure 3-23: Alerts screen

3. Web Interface

Click **Refresh** to update the page. Click **Filter** to open a window in which options can be selected for refining the displayed content of the Alert Log (Figure 3-24). Click **Close** once all selections have been made.

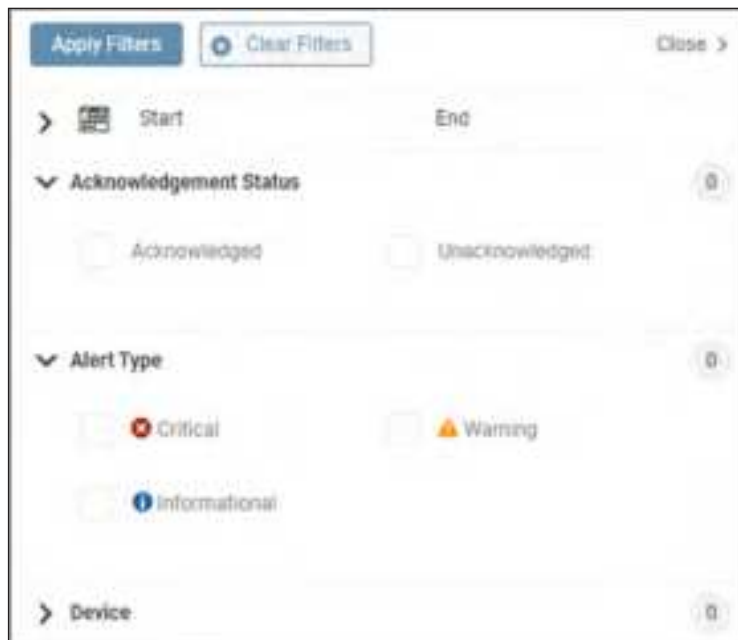
A dialog box titled "Filter" with a close button in the top right. It contains several filter sections: "Start" and "End" date pickers, "Acknowledgement Status" with radio buttons for "Acknowledged" and "Unacknowledged", "Alert Type" with radio buttons for "Critical" (red circle), "Warning" (yellow triangle), and "Informational" (blue circle), and a "Device" dropdown menu. Each section has a count of items in parentheses on the right.

Figure 3-24: Filter

Click **Export** to open a window in which the desired file format (CSV or XML) and export destination can be selected (Figure 3-25). Select the Download option to locally export the log. Upon selecting the Email option, a table of recipients will appear, one of which can be selected. Refer to section **4.5 Events & Actions** > Alert Contact sub-menu item for creating email recipients. Click the **Continue** button to execute the export.

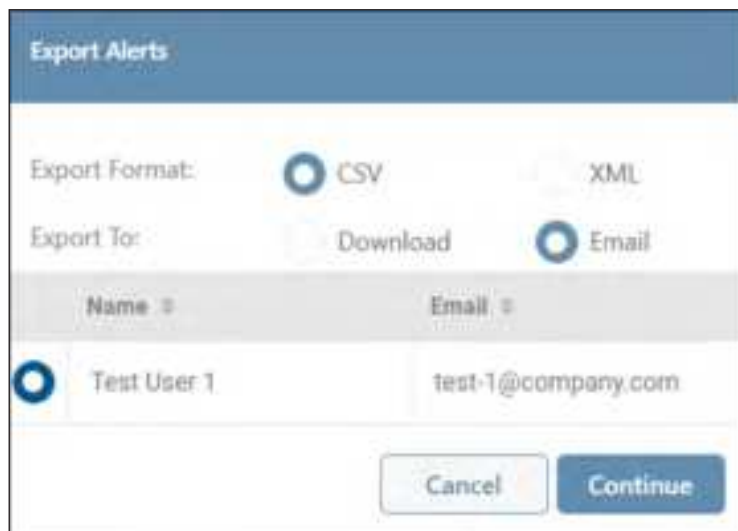
A dialog box titled "Export Alerts". It has two sections: "Export Format:" with radio buttons for "CSV" (selected) and "XML", and "Export To:" with radio buttons for "Download" and "Email" (selected). Below "Export To:", there is a table with two columns: "Name" and "Email". The table has one row with "Test User 1" and "test-1@company.com". At the bottom right are "Cancel" and "Continue" buttons.

Figure 3-25: Alert export options

3. Web Interface

Language

Click the Language icon to select a personal preference for the desired language (Figure 3-26). Note that this selection applies only to the logged-in user; the default language for all users is set using the [Global Settings](#) function. GUI contents, email notifications and generated reports will all reflect the selected language.



Figure 3-26: Language icon

Administration

Click the Gear icon to display a sub-menu of Administrative functions (Figure 3-27). Note that if the 'Restart Device', 'Turn Off Device' and 'Turn On Device' items do not appear in the pulldown menu, the device does not support these functions.

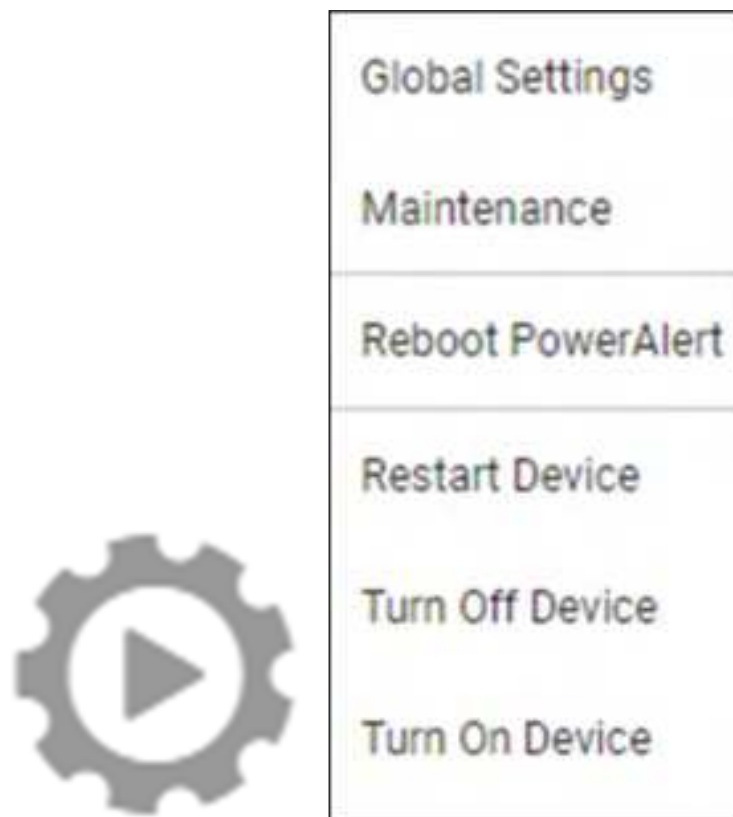


Figure 3-27: Administration Icon and Sub-Menu

3. Web Interface

Global Settings

This option allows for configuration of global settings, including time, date, temperature and language (Figure 3-28). All users accessing the device are subject to these settings. Users have the option of individually overriding these settings using the **Preferences** function. Once all configuration parameters have been entered, click the **Save** button.



Figure 3-28: Global settings

Note that it is possible to change the Current Local Time once the Time Source has been saved as 'Real-time clock (Manual)'. Click the pencil icon to open a Calendar window in which the date and time can be selected (Figure 3-29). Once the time and date have been set, click the **Save** button.



Figure 3-29: Adjusting Current Local Time

3. Web Interface

Maintenance

This option allows for execution of maintenance functions – firmware update and backup management (Figure 3-30).



Figure 3-30: Device Maintenance

Click the **Check for Updates** button to confirm availability of a firmware update at the Tripp Lite website. Click the **Update Firmware** button to initiate the firmware update process. In the dialog box that opens, select the firmware file using the **Browse** button, then click the **Upload** button. Once the file has been uploaded, click the **Continue** button. A warning box will appear; click **Update Now** to continue the process (Figure 3-31). Completing the update requires a reboot.

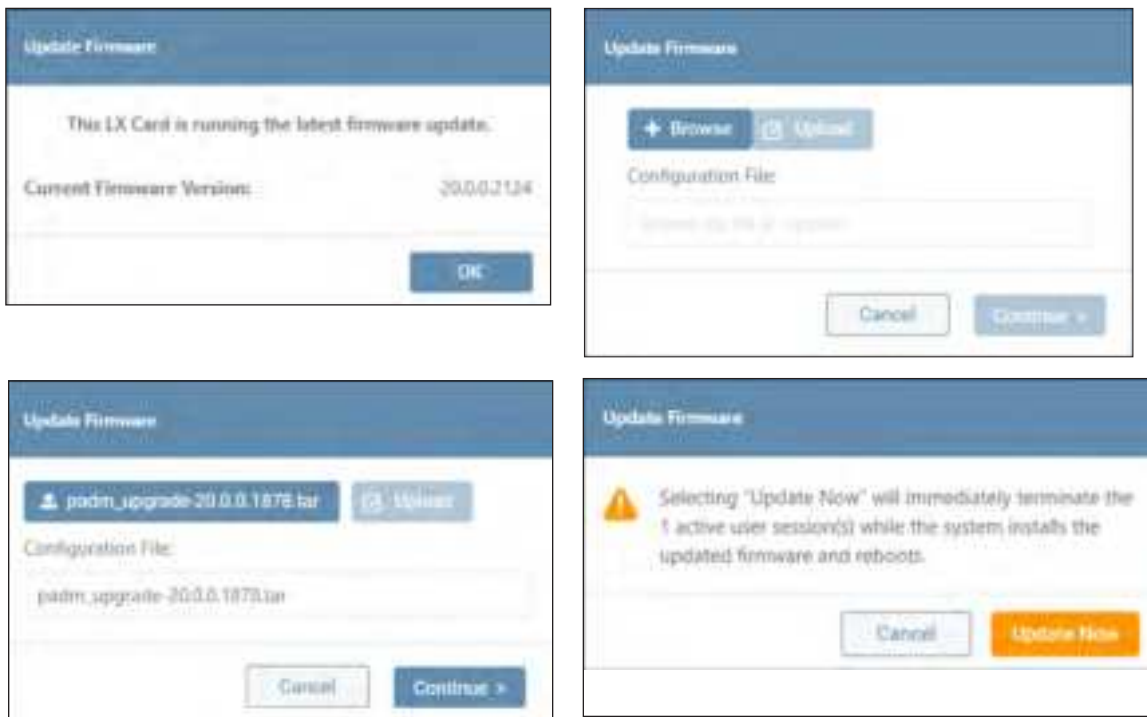


Figure 3-31: Update Firmware

3. Web Interface

Click the **Backup PowerAlert Settings Now** button, followed by the **Continue Backup** button to store the configuration on the device (Figure 3-32). On completing the backup, click the **Download** button to optionally save the configuration to the local environment (Figure 3-32).

The download file name will be in the format “card (x).bck”, which is used by other downloads. Consider renaming the file to distinguish it from similar files, e.g. “Device123backup_07_31_2021.bck”.

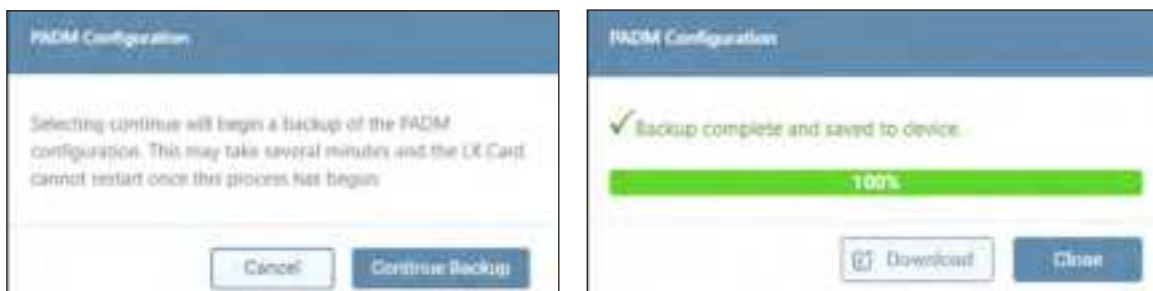


Figure 3-32. Performing a PADM Configuration Backup

Click the **Restore from Saved Backup** button to upload a configuration file (Figure 3-33). If a previous Backup on the device does not exist, the configuration source must be selected using the **Browse** button. Upon selecting the file, click **Upload**, then **Continue**. If a Backup on the device exists, the configuration source can be either System Backup (stored on the device) or External Backup (**Browse** to select).

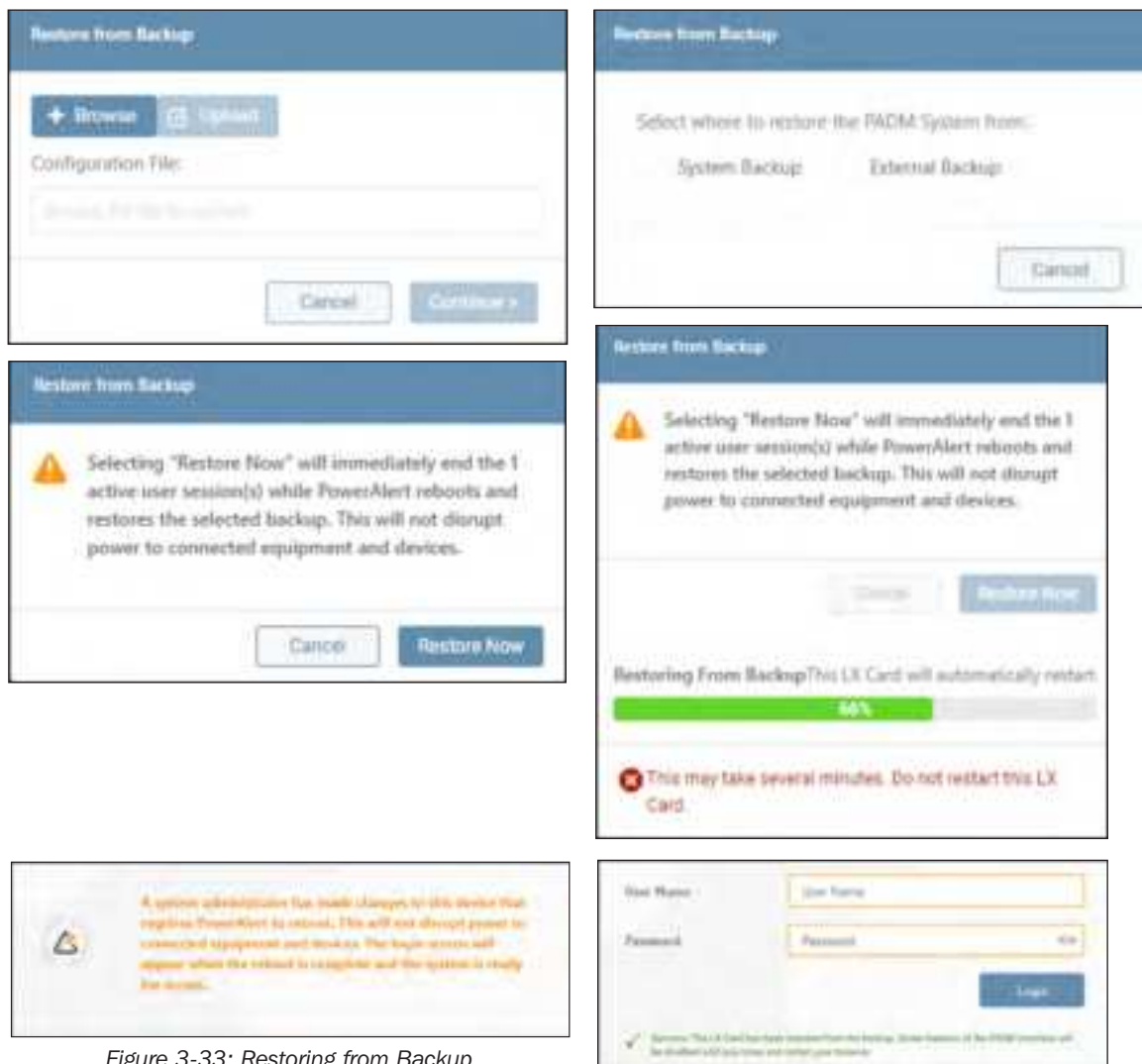


Figure 3-33: Restoring from Backup

3. Web Interface

Click the **Restore PowerAlert to Factory Defaults** button to overwrite the existing configuration with the default parameters set in the factory, either with preserving current network settings or without doing so (Figure 3-34).

Note: Restoring PowerAlert will terminate all active sessions.

When performing the “Restore PowerAlert” function using the “maintain current network settings” option, the following occurs:

Internet

- Domain, IPv4, IPv6 and DNS settings do NOT change; all settings are retained

Services

- The enabled/disabled status of SNMPv1, SNMPv2c and SNMPv3 are NOT retained
- The port values for SNMP Get/Set and Trap do NOT change; they are retained
- HTTP/HTTPS and Telnet settings do NOT change; they are retained
- SFTP/SCP are NOT retained if SSH is enabled

SMTP

- Server, Authentication and Email Format all change; settings are not retained

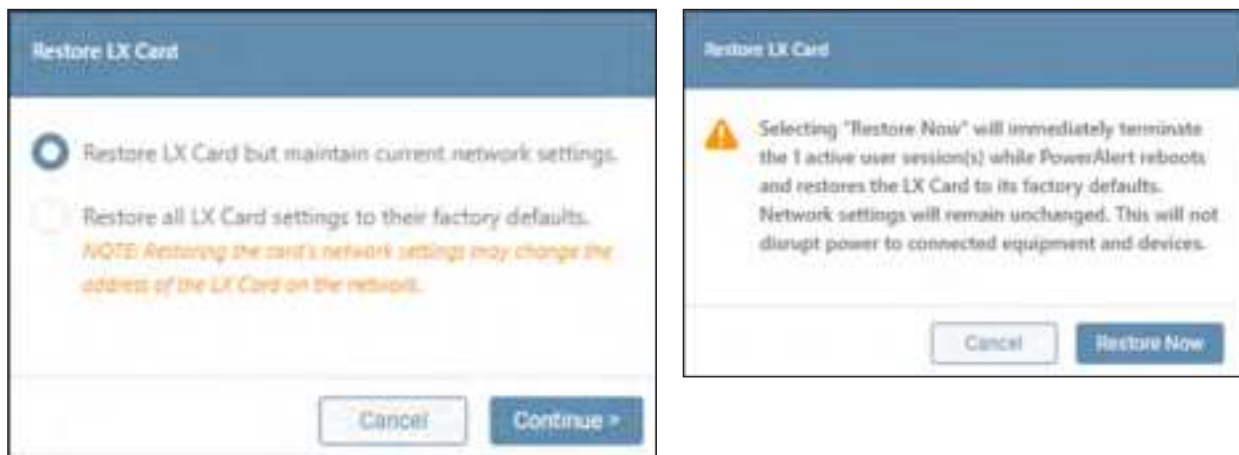


Figure 3-34: Restoring PowerAlert to Factory Defaults

3. Web Interface

Reboot PowerAlert – This item performs a reboot of the LX Platform device's network interface (Figure 3-36). This operation does not power cycle the device itself or any outlet on the device.

Note: Rebooting the LX Card will terminate all active sessions.



Figure 3-36. Reboot PowerAlert

Restart Device – This item turns off the device after a specified delay time, then turns it on after a specified delay (Figure 3-37).

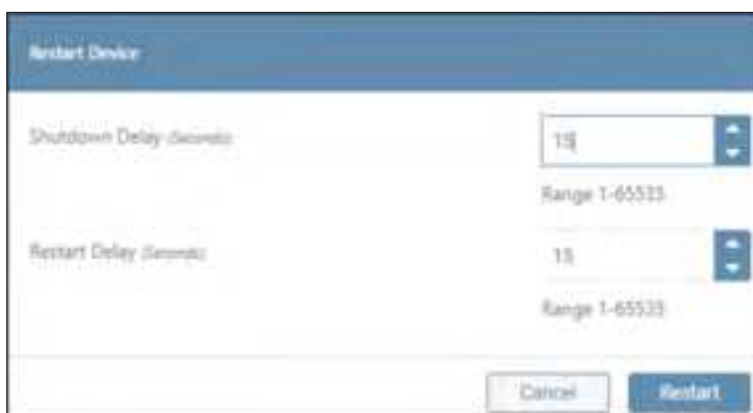


Figure 3-37: Restart device

3. Web Interface

Turn Off Device – This item turns off the host device (e.g. UPS) after the specified delay (Figure 3-38). Note that the device's network interface (PADM) will remain active even though the device is operationally off.



Figure 3-38: Turn Off device

Turn On Device – This item turns on the device after the specified delay (Figure 3-39).



Figure 3-39: Turn On device

Support

Click the Question icon to display a sub-menu of Support items. Click **Help/Contact** to display links for online support and customer support. In the upper right corner, click the **Generate Support Report** button to compile a report that can be shared with Tripp Lite Customer Support for troubleshooting; click the **Continue** button to generate the report. Upon successful completion, a banner will appear; click the **Save Report** button to save the report to the computer's Downloads folder. The download file name will be in the format "card (x).bck", which is used by other downloads. Consider renaming the file to distinguish it from similar files, e.g. "SupportReport001.bck".

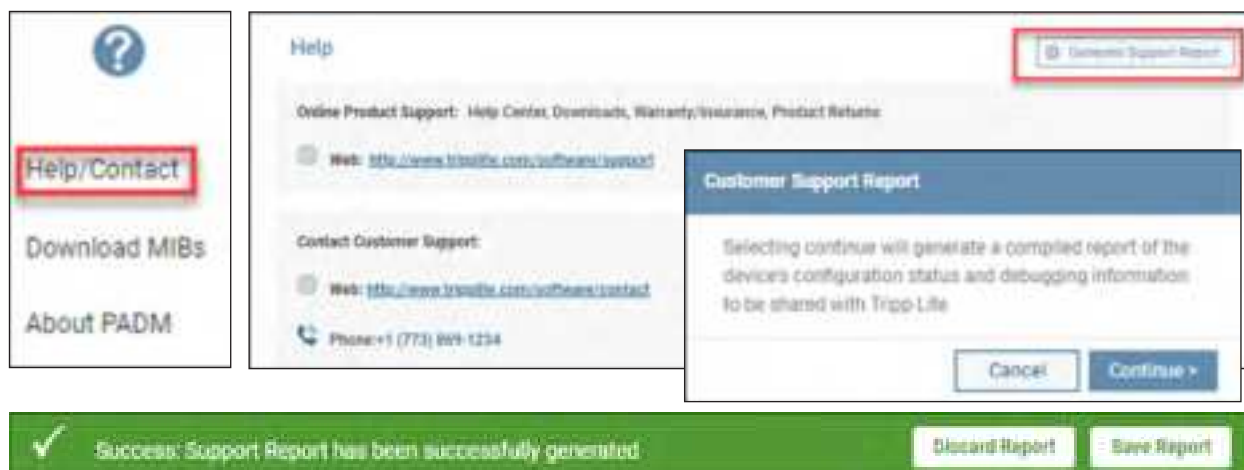


Figure 3-40: Help/Contact

3. Web Interface

Click **Download MIBs** to automatically download the Tripp Lite MIB package to the computer's Downloads folder. Click **About PADM** to display information related to the PowerAlert Device Manager interface (Figure 3-41).



Figure 3-41: Download MIBs and About PADM

User

Click the Person icon to display a sub-menu of options related to the login. Click **Change Password** to change the existing password of the logged-in user. Click on the 'eye' icon to view the plaintext password entered. Click **Log Out** to terminate the current session (Figure 3-42).

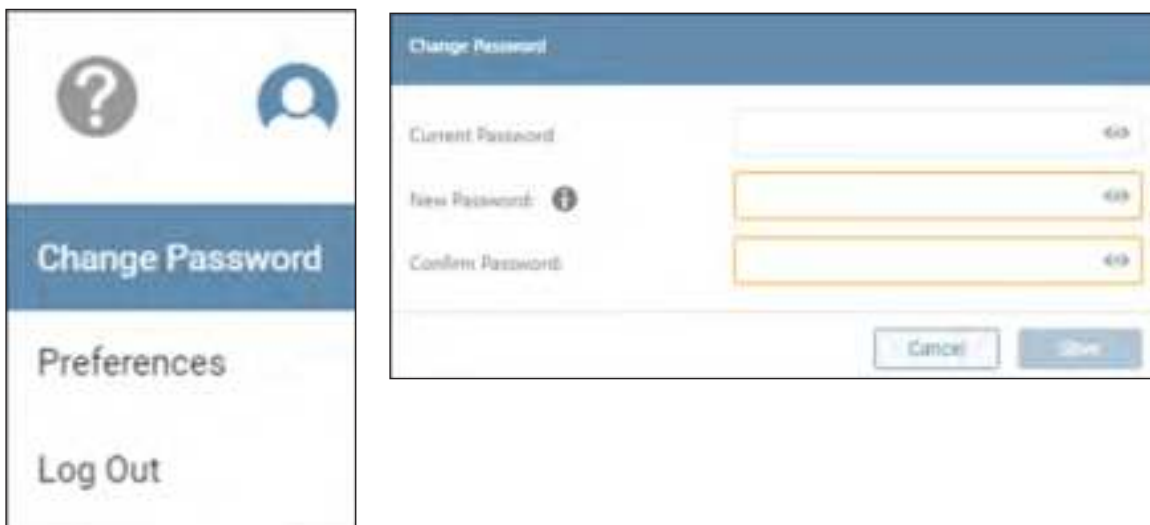
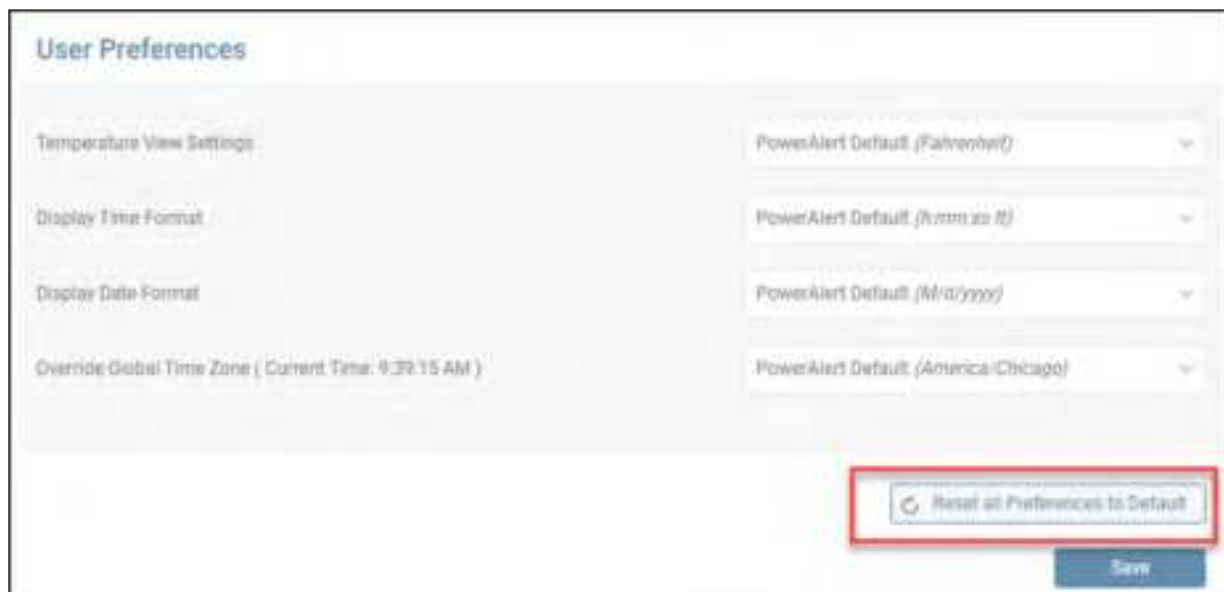


Figure 3-42: User Menu, Change Password and Logout

3. Web Interface

Click **Preferences** to override the global settings for Temperature, Time, Date and Time Zone settings (Figure 3-43). Click **Reset all Preferences to Default** to restore the settings set using the Global Settings. Once all settings have been made, click the **Save** button.

Note: Policies related to password length and character use are set in the Security menu.



The screenshot shows the 'User Preferences' web interface. It features a title 'User Preferences' at the top left. Below it, there are four rows of settings, each with a label on the left and a dropdown menu on the right. The settings are: 'Temperature View Settings' with a dropdown showing 'PowerAlert Default (Fahrenheit)'; 'Display Time Format' with a dropdown showing 'PowerAlert Default (h:mm:ss tt)'; 'Display Date Format' with a dropdown showing 'PowerAlert Default (M/d/yyyy)'; and 'Override Global Time Zone (Current Time: 9:39:15 AM)' with a dropdown showing 'PowerAlert Default (America/Chicago)'. At the bottom right, there is a button labeled 'Reset all Preferences to Default' with a circular arrow icon, which is highlighted by a red rectangle. Below this button is a blue 'Save' button.

Figure 3-43: User Preferences

4. Main Menu

The Main Menu enables navigation to the configuration, monitoring and control functions of the device. Each of the Main Menu items (Figure 4-1) is described in the following sections..



Figure 4-1: Main Menu

4.1 Dashboard

The Dashboard menu item displays a graphical summary of the device's operational status, as well as the status of connected peripherals, in the form of Gauges and Graphs (Figure 4-2).



Figure 4-2. Dashboard Gauges and Graphs

4. Main Menu

Gauges

To select which gauges to display on the Dashboard, click **Gauges** in the upper right corner, make the desired selections, then click **Apply Gauges** (Figure 4-3). Certain gauges are interactive – if the cursor changes when moving over the gauge, click on it to open a window in which its parameters can be edited. Note that these adjustments can also be made in the Device > Device Details menu item.

In the event that the threshold supports both “Warning” and “Critical” level bounds, ensure that the “Warning” values are within the range/do not equal to or exceed the limits set by the “Critical” values.

Figure 4-3 displays the Gauges configuration interface, showing the selection of gauges to display on the Dashboard and the configuration of thresholds and bounds.

The top section shows the 'Gauges' configuration window for 'Device0077'. It includes buttons for 'Apply Gauges', 'Clear Gauges', and 'Close'. The selected gauges are:

- Input Frequency - Phase 2 (Hz) (checked)
- Input Frequency - Phase 3 (Hz) (checked)
- Input Frequency - Phase 1 (Hz) (checked)
- Output Power (W) (unchecked)

The bottom section shows the 'Thresholds and Bounds' configuration window. It includes a table with columns for Name, Min (), Value (), and Max ().

Name	Min ()	Value ()	Max ()
Low Critical	0	5	44
High Critical	6	45	100
Alert Tolerance (margin before retriggering an event)		0	

Buttons for 'Cancel', 'Apply Changes', and 'Save & Close' are located at the bottom of the window.

Figure 4-3: Gauges

4. Main Menu

Graphs

Click **Add Graph** in the upper right corner to select which graphs to display on the Dashboard (Figure 4-4). After entering a Name and selecting the desired Device, Category and variables, click **Save**. To edit the graph, click the pencil icon in the upper right corner of the graph. To remove the graph, click on the  icon next to the pencil icon.



Figure 4-4: Graphs

4.2 Device

The Device menu item is comprised of two tabs: Device Details and Device Properties (Figure 4-5).



Figure 4-5: Device Details and Device Properties

4. Main Menu

Device Details

This tab displays the metrics of the device and all peripherals connected to it (Figure 4-6). Use the **Group** and **Filter** functions to customize the displayed information. Icons to the right of an item indicate whether edits or controls can be performed.

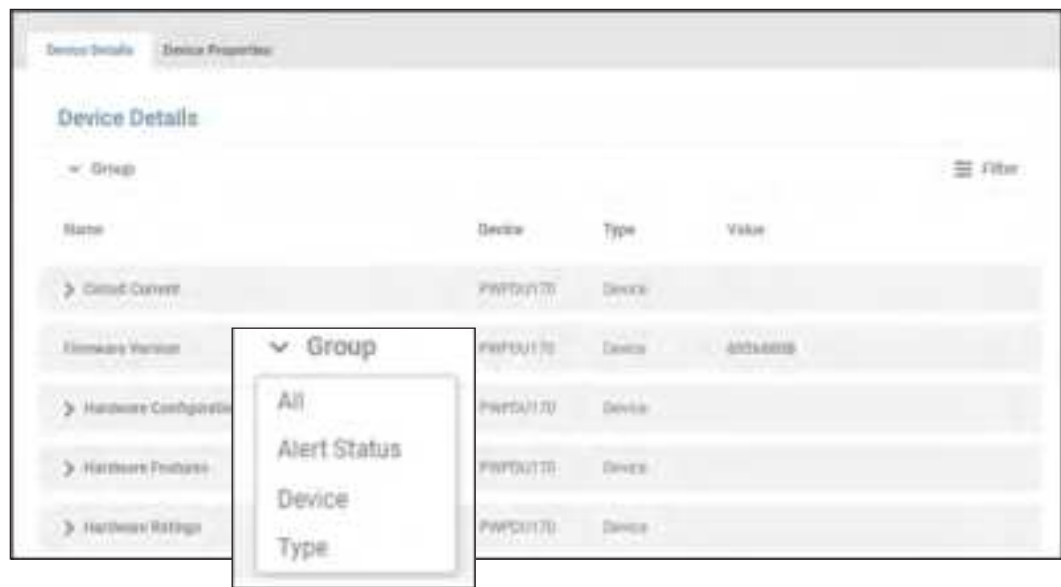


Figure 4-6: Device Details

Note that certain metrics – denoted with a chevron – need to be expanded in order to display their editable / actionable content. For example, in Figure 4-7, expanding “Battery Charge Remaining” reveals that Thresholds and Bounds can be edited. Click the pencil icon to open a window in which these edits can be made. In the event the threshold supports both “Warning” and “Critical” level bounds, ensure the “Warning” values are within the range / not equal to or exceeding the limits set by the “Critical” values.

In general, when a parameter Threshold is crossed, an Alert will be generated. The Tolerance sets the amount that the parameter must ‘return’ for the Alert to clear. Example: the Low Warning threshold is set to 50% and the Alert Tolerance is set to 2%. If the Battery Charge falls below 50%, an Alert will be generated. The Alert will clear when the Battery charge rises above 52%.

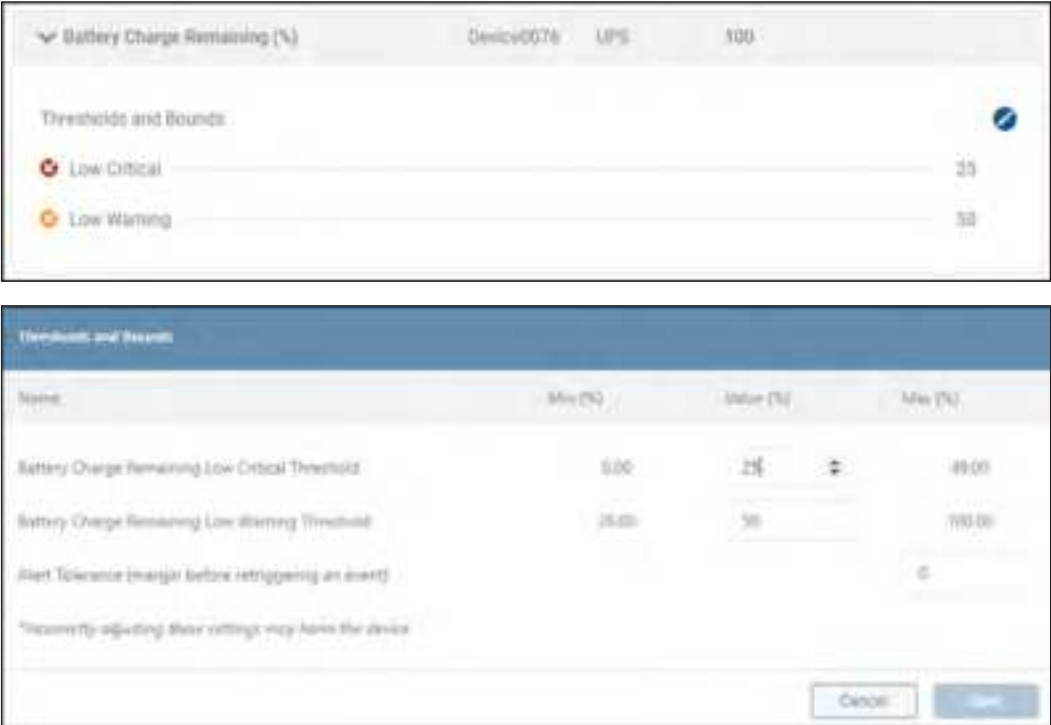


Figure 4-7: Expanding Device Details and Editing Thresholds

4. Main Menu

Device Properties

This tab displays information related to the identity of the device and any peripherals connected to it (Figure 4-8). Certain parameters, such as “Device Name”, “Location” and “Installation Date” are editable; click the pencil icon to enter or modify these parameters.

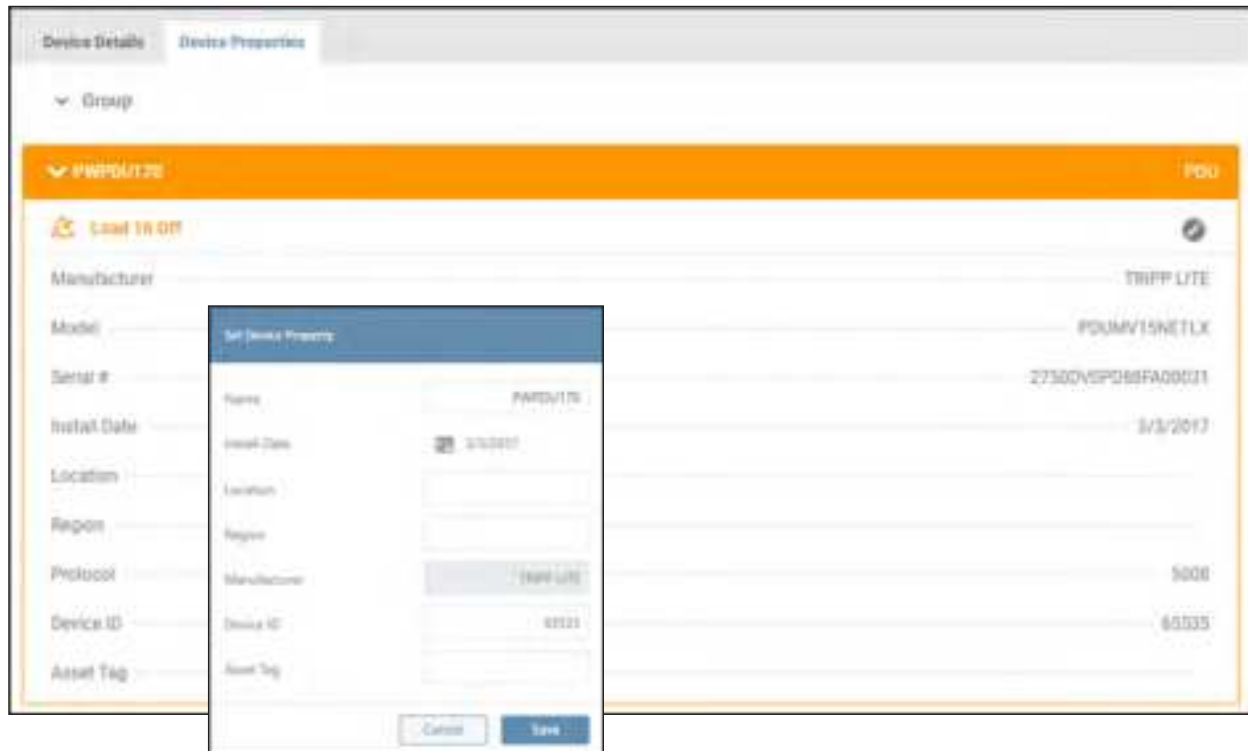


Figure 4-8: Displaying and Editing Device Properties

In the event a peripheral becomes disconnected from the host device, it will be tagged as an “Inactive Device.” To remove the Inactive Device from the display, click the  icon adjacent to the tag (Figure 4-9).

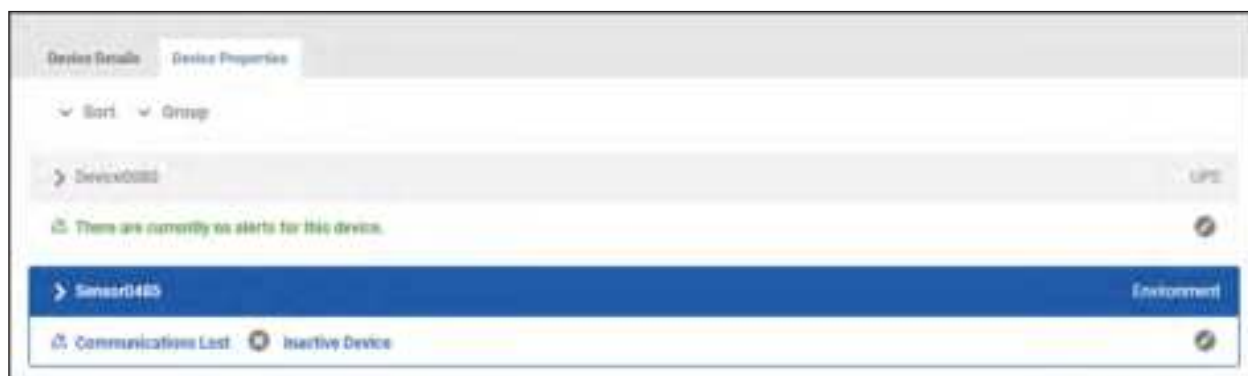


Figure 4-9: Inactive device

4. Main Menu

4.3 Loads

The Loads menu item will appear only for devices that support loads. It is comprised of three tabs: Loads Overview, Loads Ramp/Shed and Load Groups.

Note: PADM will display only the tabs that the device supports.



Figure 4-10: Loads Tabs

Loads Overview

This tab displays a summary of the device’s loads, including status and outlet-level metrics, if applicable (Figure 4-11). Move the sliders to change the state of the Main Load or individual Loads (if supported by the device). Use the **Columns** and **Filter** functions to customize the displayed information. To edit Load details and view additional outlet-level information, click the pencil icon to the left of the item. Click the **Save** button once all edits have been made.



Figure 4-11: Loads Overview Tab and Editing Load Details

4. Main Menu

Loads Ramp/Shed

Loads Ramp/Shed is supported only by UPS systems with two or more controllable loads and switched PDUs. This tab displays a summary of Ramp and Shed settings across all Loads (Figure 4-12). To adjust the state and delay times for each Load, click the **Edit** button then use the sliders and up/down arrows. Click the **Save** button once all edits have been made. Click the **Begin Ramp** or **Begin Shed** buttons to immediately execute the respective action.

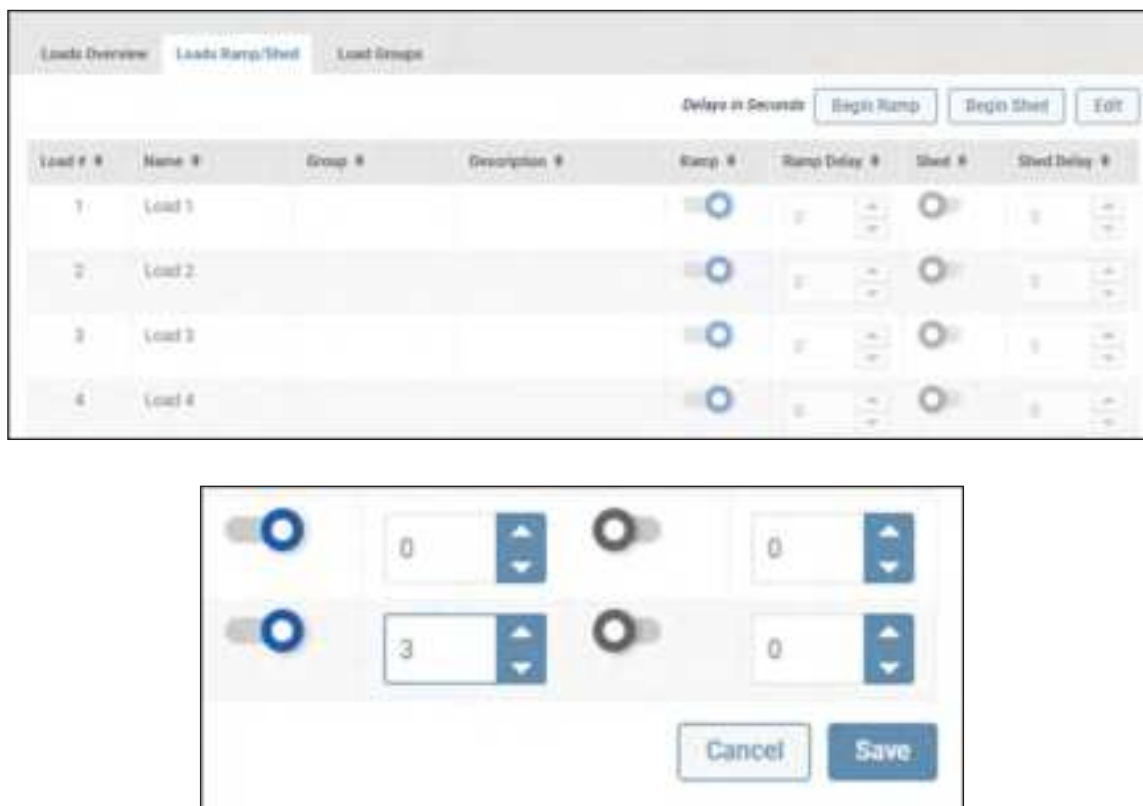


Figure 4-12: Load Ramp/Shed

Load Groups

Load Groups are supported only by UPS systems with two or more controllable loads and switched PDUs. This tab displays a summary of configured Load Groups (Figure 4-13). To create a Load Group, click **Add Load Group**. In the dialog box that appears, enter a Name for the Load Group (required) and, optionally, a Description. Next, from the Load list, select which Loads are to belong to the Load Group. To filter the list to display only loads that have not yet been assigned to a load group, click **All Loads** and select the **Unassociated** menu item (Figure 4-14). Click the **Save** button at the bottom of the window once all edits have been made. Click the pencil icon at right to edit the item. All newly-created Load Groups are enabled, by default; to disable the Load Group, shift the slider to the left (Figure 4-14).



Figure 4-13: Load Ramp/Shed

4. Main Menu

Load Group

Enabled

Name

Group A

Description

Servers 1-3

	Load #	Name	Group	Description	Receptacle Type	
☐	1	Load 1			C19	
☒	2	Load 2			C13	
☒	3	Load 3			C13	
☒	4	Load 4			C13	
☐	5	Load 5			C13	
☐	6	Load 6			C19	

▼ All Loads

All Loads

Unassociated

Figure 4-14: Adding and Editing a Load Group

To delete one or more Load Groups, click the icon to the left of each line item (Figure 4-15). On doing so, the **Delete Load Group(s)** button becomes active (turns red); click the button to complete the deletion.

Loads Overview | Loads Ranges/Sheet | Load Groups

Delete Load Group(s) Add Load Group

Status	Name	State	Description	# of Loads
Enabled	Group A		Servers 1-3	3

Figure 4-15: Deleting a Load Group

4. Main Menu

4.4 Batteries

This menu item is displayed only for UPS systems that support the use of External Battery Packs. The Batteries menu item summarizes the status and metrics of all batteries in use by the device (Figure 4-16). Click on the pencil icon to the right of the line item to edit the item. In the window that appears, click on the calendar icon to set or modify the Installation and Replacement dates. Use the up-down arrows to adjust the Battery Age Thresholds. Once all edits have been completed, click the **Save** button.

Batteries

Import a Battery Configuration File

DetailsAdd

Battery Status

Running

Battery Remaining

400

Capacity

100

Seconds on Battery

0

Voltage

284.0 V

Name	Internal	Smart	Model	Installed On	Replace On
Internal-1	Yes	No	1224	6/04/2022	9/04/2020

Battery

Names

Internal-1

Installed On:

2/5/2023

Replace On:

2/5/2020

Battery Age High Warning Threshold (Years)

Min 0.00

Value 3

Max 4.90

Battery Age High Critical Threshold (Years)

Min 3.10

Value 5

Max 5.00

Cancel

Save

Figure 4-16: Summary List of Batteries and Editing a Battery

4. Main Menu

To add and configure External Battery Packs (EBPs), click the **Add** button at the top of the summary page. When adding External Battery Packs (EBPs), PADM20 uses an embedded configuration file. Updates to this file are posted occasionally on the Tripp Lite website. If such an update has been downloaded, click the **Import a Battery Configuration File** button to upload it to PADM20 (Figure 4-17). In the next step, use the up-down arrows to select the EBP model and quantity to be added to the battery profile, then click the **+Add** button. Repeat this step for all additional EBPs. Click the x icon to the left of the EBP to remove it from the battery profile. Once all EBPs have been added, click the **Apply** button. This initiates a process whereby the runtime of the battery profile – which includes the internal battery—is calculated and added to the device configuration. A window will appear displaying progress of the configuration.



Figure 4-17: Adding an EBP and Configuring the Battery Profile

4. Main Menu

Once the process is complete, the newly added EBPs will appear in the summary list (Figure 4-18). To delete one or more external batteries, click the  icon to the left of each line item. On doing so, the **Delete** button becomes active (turns red); click the button to complete the deletion. Upon confirming the deletion, the system will automatically re-configure using the revised battery profile.

NOTE: Internal batteries cannot be deleted.

When smart external batteries are connected to a UPS, PADM20 will 'discover' and identify them as such in the "Smart" column of the "Batteries" list. Under certain conditions, the External Battery Pack configuration utility embedded in PADM20, or the PowerAlert External Battery Pack Utility (PAEBPU) does not need to be used.

- With smart internal batteries and up to six external smart battery packs are installed, the UPS calculates the runtime. The embedded EBP utility or PAEBPU should not be used.
- With smart internal batteries and more than six external smart battery packs are installed, the embedded EBP utility or PAEBPU should be used to calculate runtime. Note that PADM20 (and the local display on the UPS) will treat these additional (>6) batteries as 'non-smart'.
- With a combination of smart and non-smart internal and external battery packs, the embedded EBP utility or PAEBPU should be used to calculate runtime.



Name	Connected	Smart	Manufacturer	Model	Installed On	Replaced On
Internal 1	Yes				2/1/2022	2/1/2022
External 1-C	Yes				2/1/2022	2/1/2022

Figure 4-18: Deleting an EBP

4. Main Menu

4.5 Events & Actions

Events

This sub-menu item summarizes the status and configuration of all events applicable to the device and connected peripherals (Figure 4-19). To enable Auto-Acknowledgement and Logging for all events, select the appropriate check boxes at the top of the Events list.



Events									
Sort		All		Auto Acknowledge		Logging		Filter	
>	Overheat		Device	Value	Device0001		☒ Acknowledge	☒ Log	
>	Communications Lost		Device	Value	Device0001		☐ Acknowledge	☐ Log	
>	On Battery		Device	Value	Device0001		☒ Acknowledge	☒ Log	
>	Battery Low		Device	Value	Device0001		☒ Acknowledge	☒ Log	
>	General Fault		Device	Value	Device0001		☒ Acknowledge	☒ Log	
>	Battery Capacity Below Warning Level		Device	Value	Device0001		☒ Acknowledge	☒ Log	
>	Battery Self Test Failed		Device	Value	Device0001		☒ Acknowledge	☒ Log	

Figure 4-19: Event Summary

Click the pencil icon to the right of an Event to open a dialog box in which Event settings can be modified (Figure 4-20). If an Event is disabled, it will not be logged, nor can it be selected as a trigger for an Action. Logging and Auto-Acknowledgement of the event can be set using the respective check boxes; note that this will override the Auto-Acknowledge and Logging selections made on the Events list.



Event

Label/Name: Overheat

Clear Event Name: Load Okay

Severity: critical

Auto Acknowledge: ☒

Log: ☒

Cancel

Save

Figure 4-20: Editing an Event

4. Main Menu

Click the chevron to the left of the Event name to expand or close the section summarizing all Actions associated with the Event (Figure 4-21). To remove one or more actions from the event, click the  icon to the left of each item. On doing so, the **Remove action(s)** button becomes active (turns red); click the button to complete the deletion. To edit an action, click the pencil icon to the right of the item. A window will open asking you to specify whether the edit is to be applied to the specific event (occurrence) or to all events containing the action. On making the selection, an edit window will open in which action parameters can be edited. Click **Save** once all edits have been made.

Notes:

- Actions can also be edited in the Events & Actions > Actions sub-menu.
- Delays apply only to Set actions. Clear actions will execute immediately.

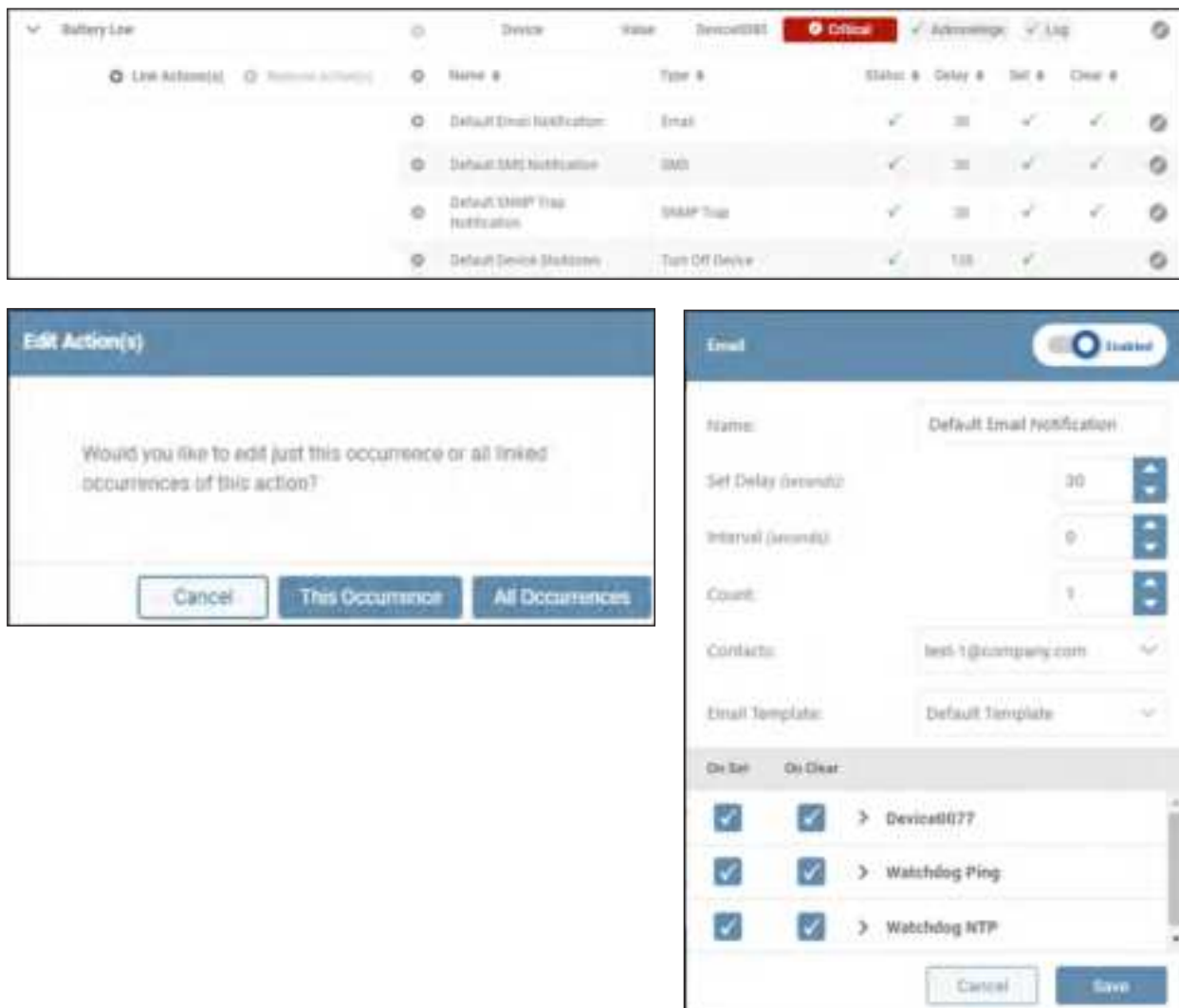


Figure 4-21: Editing Event Actions

4. Main Menu

Click **Link Action(s)** to select which Actions are to be triggered by the Event (Figure 4-22). In the window that opens, select whether the Clear and/or Set Event(s) triggers the Action. When all edits have been made, click the **Link Action(s)** button. Refer to the Action menu item for adjusting action parameters.

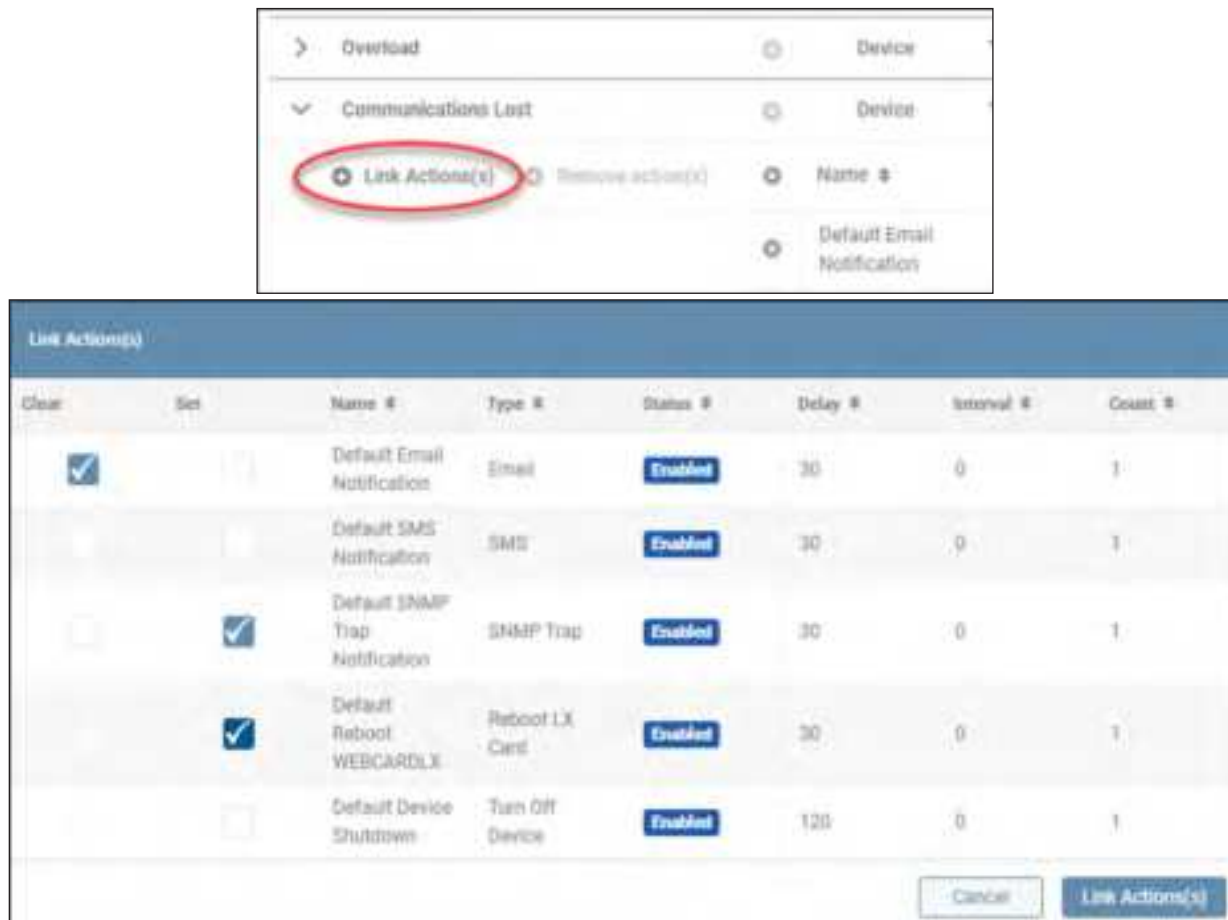


Figure 4-22: Adding an Action to an Event

Alert Contacts

This sub-menu item allows for management of Alert notification recipients. Three types of Alert contacts can be created: Email, SMS and SNMP. The main page displays a summary of all Alert contacts (Figure 4-23).

Alert Contacts						
			Delete Contact(s)		Add an Alert Contact	
Status #	Label/Name #	Contact Details #	Type #	Trap Port #	Set Port #	
Enabled	John Doe	john.doe@company.com	Email	N/A	N/A	
Enabled	SNMPuser1	192.168.10.10	SNMPv1	160	161	
Enabled	SNMPuser2	192.168.22.22	SNMPv2c	160	161	
Enabled	Jane Doe	1-800-123-4567	SMS	N/A	N/A	

Figure 4-23: Alert Contacts

4. Main Menu

To create a new contact, click **Add An Alert Contact** and select the contact type from the menu. A dialog box appears, reflecting the configuration parameters for the selected recipient type. Examples of dialog boxes for SNMPv1 and Email recipients are shown in Figure 4-24. New entries are enabled, by default; to disable the entry, move the slider to the left. A disabled entry will not receive Alert notifications. To confirm that contacts can receive notifications, click the **Send Test** button; the results of the test will appear to the right of the button. Once all configuration parameters have been entered, click the **Save** button. There is no practical limit to the number of Alert contacts that can be created.

The figure consists of three screenshots illustrating the process of adding an alert contact. The top-left screenshot shows the 'Add an Alert Contact' menu with options for Email, SMS, SNMPv1, SNMPv2, and SNMPv3. The bottom-left screenshot shows the 'Email Alert Contact' configuration form, which includes fields for 'Label/Name' (John Doe) and 'Email' (johndoe@company.com), a 'Send Test' button, and 'Cancel' and 'Save' buttons at the bottom. The right screenshot shows the 'SNMPv1 Alert Contact' configuration form, which includes fields for 'Label/Name' (SNMPUser1), 'Host' (192.168.10.10), 'Community' (password), 'Enable Trap' (checked), 'Trap Type' (Trap), 'Port' (162), and buttons for 'Test Trap', 'Enable Set' (checked), 'Port' (161), 'Test Set', 'Cancel', and 'Save'.

Figure 4-24: Adding an Alert Contact – SNMPv1 and Email Examples

To edit a contact, click the pencil icon to the right of an entry. Once all edits have been completed, click the **Save** button. To delete one or more contact, click the  icon to the left of each line item. On doing so, the **Delete Contact(s)** button becomes active (turns red); click the button to complete the deletion.

Note: Newly created Alert Contacts are automatically assigned as recipients to default notifications and to Actions where “Contacts:” is set to “All”. Refer to the Actions menu, “Default Email Notification” item to edit this setting.

4. Main Menu

Actions

This sub-menu item summarizes the status and configuration of all Actions applicable to PowerAlert, the device and connected peripherals (Figure 4-25). Click the pencil icon to the right of an Action to configure its settings. If an Action is disabled, it cannot be selected when configuring Events (Link Actions). To delete one or more actions, click the  icon to the left of each line item. On doing so, the **Delete Action(s)** button becomes active (turns red); click the button to complete the deletion.

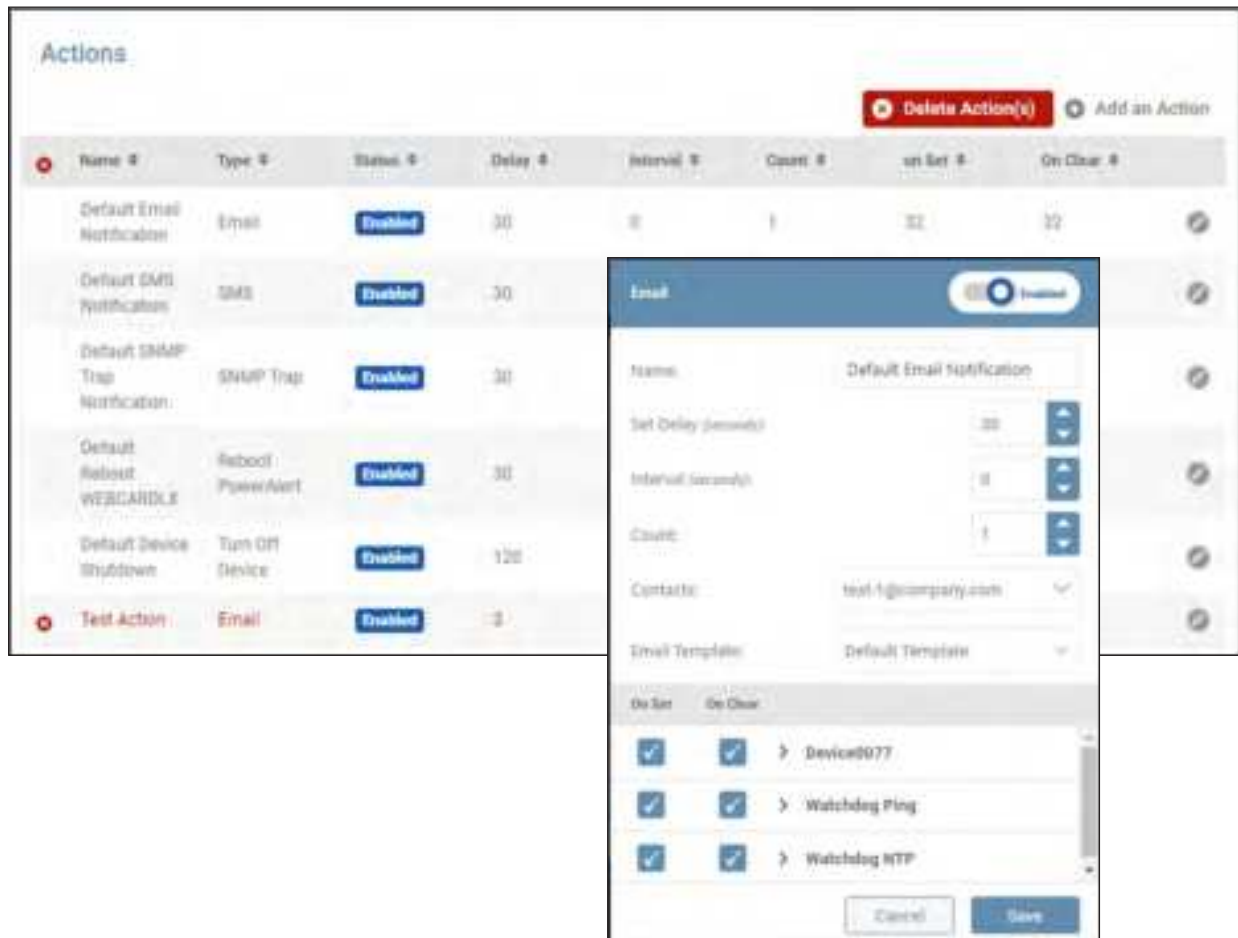


Figure 4-25: Actions Summary and Editing an Action

To create a new action, click **Add an Action** and select one of the action types (Figure 4-26). A window will appear containing configuration parameters specific to the selected action type. Enter a name for the action as well as the action-dependent parameters, such as:

- Set Delay – the number of seconds the action will wait to execute after the On Set event occurs.
- Target Device – the device undergoing the action
- Load(s) – one or more loads undergoing the action
- Load State – the outcome of the Load action, i.e. turn on, off or cycle
- Interval – the number of seconds between successive executions of the action
- Count – the number of times the action will be executed; if set to 0 (zero), the action will repeat indefinitely until it clears
- Contacts – one or more notification/trap/set recipients

4. Main Menu

Next, select one or more trigger events for the action in the **On Set / On Clear** section of the window. Click on the chevrons to view all events related to the object. Note that not all action types support both On Set and On Clear events. For example, “Ramp” only supports On Clear events. Within the list of objects are the default Autoprobes, as well as any user-created (custom) Autoprobes. Refer to the AutoProbe section of this document for information about creating custom AutoProbes.

New actions are enabled, by default; to disable the entry, move the slider to the left. A disabled action will not execute when its trigger event occurs. Once all parameters have been set, click the **Save** button.



Figure 4-26: Creating an Action

Scheduling

This sub-menu item allows for the management of scheduled actions applicable to PowerAlert, the device and connected peripherals. The main page displays a summary of all Schedules (Figure 4-27). Click the pencil icon to the right of a Scheduled Action to edit its parameters. To delete one or more schedules, click the  icon to the left of each line item. On doing so, the **Delete Schedule(s)** button becomes active (turns red); click the button to complete the deletion.



Figure 4-27: Summary of Scheduled Actions and Editing a Scheduled Action

4. Main Menu

To create a new schedule, click Add Schedule and select the action type from the menu (Figure 4-28). In the window that opens, enter a name for the action then proceed through the configuration tabs:

- Action – select the target device and other parameters, if required
- Frequency – define how often the action is to be executed
- Range – set the starting date and time (Run On) as well as the end criteria.
Click on the calendar icon to enter the time and date.

New schedules are enabled by default; to disable the schedule, move the slider to the left. Disabling a schedule prevents it from executing. Click on the **Save** button once all edits been completed.

Newly created Scheduled Actions cannot have a Run-On time sooner than 10 minutes before the current PADM UTC time. Doing so will automatically add 10 minutes to the desired Run-On. This issue may also arise if changes to PADM date and time settings are made after new schedules are created. For instance, if the PADM time is set back by one hour, the Run On time of the newly created schedule will automatically change to the current time plus 10 minutes.

The figure consists of four screenshots illustrating the process of creating a scheduled action in a software interface.

- Screenshot 1 (Top Left):** A vertical menu titled "Add schedule" with a blue plus icon. It lists several action types: Load(s), Ramp, Reboot PowerAlert, Restart Device, Shed, Turn On Device, and Turn Off Device.
- Screenshot 2 (Top Right):** The "Scheduled Action: Load(s)" configuration window. It is titled "Scheduled Action: Load(s)" and has an "Enabled" toggle. The "Name" field is empty. Below are three tabs: "1. Action", "2. Frequency", and "3. Range". The "1. Action" tab is active, showing fields for "Load(s)", "Target Device" (set to "Device0077"), "Load(s)" (set to "Load 1"), and "Load State" (set to "Off"). "Cancel" and "Next >" buttons are at the bottom.
- Screenshot 3 (Bottom Left):** The "Scheduled Action: Battery Self-Test" configuration window. It is titled "Scheduled Action: Battery Self-Test" and has an "Enabled" toggle. The "Name" field is set to "Bi-monthly self-test". Below are three tabs: "Action", "Frequency", and "Range". The "Frequency" tab is active, showing a dropdown for "Monthly", a field for "of every" set to "1", and a dropdown for "Month(s)". Below this, there are radio buttons for "First" (selected) and "Sunday", and a field for "Of Every" set to "2" with a dropdown for "Month(s)". "Cancel" and "Save" buttons are at the bottom.
- Screenshot 4 (Bottom Right):** The "Scheduled Action: Battery Self-Test" configuration window. It is titled "Scheduled Action: Battery Self-Test" and has an "Enabled" toggle. The "Name" field is set to "Bi-monthly self-test". Below are three tabs: "Action", "Frequency", and "Range". The "Range" tab is active, showing a "Run On" date of "09:42 Feb 13, 2020". There are radio buttons for "Repeat Forever", "Repeat" (set to "1"), and "Repeat Until" (set to "09:42 Feb 13, 2030"). "Cancel" and "Save" buttons are at the bottom.

Figure 4-28: Creating a Scheduled Action

4. Main Menu

AutoProbe

This sub-menu allows for the management of AutoProbes, which automatically execute a prescribed action (e.g. cycle a load, send an email), when the device loses network communications with a specified target device. The main page displays a summary of all AutoProbes (Figure 4-29). Click the pencil icon to the right of an entry to configure its settings. To delete one or more AutoProbes, click the  icon to the left of each line item. On doing so, the **Delete** button becomes active (turns red); click the button to complete the deletion.

Note: the two default AutoProbes – Watchdog Ping and Watchdog NTP – cannot be deleted. Both are linked to the Reboot PowerAlert action.



State	Op. Status	Name	Description	Type	IP	Details
Disabled	Unknown	Watchdog Ping	Default Watchdog Ping Probe	Ping		 
Disabled	Unknown	Watchdog NTP	Default Watchdog NTP Probe	NTP		 

Figure 4-29: Auto-Probe Summary

To create a new AutoProbe, click **Add Probe** and select one of the available probe options: Ping, NTP or SNMP GET. A window appears, containing configuration parameters specific to the selected probe type (Figure 4-30). Pertinent AutoProbe parameters include:

- Label/Name – a name for the AutoProbe entry; this field is required.
- Interval – the number of minutes between successive AutoProbe tests. The valid range is 3 minutes to 1440 minutes (24 hours). The default is 3 minutes.
- Retry – the number of consecutive AutoProbe tests that must fail in order to trigger the alert. The valid range is 3 to 10 retries; the default value is 3.
- Primary Address – the IP Address or hostname of the primary device being probed.
- Port – the communication port of the device being probed.
- Primary OID – the Object Identifier target of an SNMP GET probe to the Primary Address.
- Secondary Address – the IP Address or hostname of the secondary device being probed.
- Secondary OID – the Object Identifier target of an SNMP GET probe to the Secondary Address.

All probes require a Primary Address; Secondary Address is optional, as is Description. If a Secondary Address/Port/OID is specified, the AutoProbe tests to both addresses must concurrently meet the trigger requirements in order for the alert to be generated. Conversely, re-establishing communication with either the Primary or Secondary Address will clear the alert condition.

4. Main Menu

New entries are enabled by default. To disable the entry, move the slider to the left. Click the **Save** button once all edits have been made. A maximum of 64 AutoProbes can be created. All enabled AutoProbes will appear in the On **Set/On Clear** section of Action edit windows, allowing them to be selected as event triggers for the Action.

New AutoProbes will automatically create new events bearing the same name.

Refer to the Tripp Lite website for details on configuring and using Auto Probes.

The figure consists of three screenshots. The leftmost screenshot is a vertical menu titled 'Add Probe' with a blue plus icon. It lists three options: 'Ping Probe', 'NTP Probe', and 'SNMP GET', each with a person icon. The top-right screenshot shows the 'SNMP GET Probe' configuration form. It has tabs for 'Details' and 'Security'. The 'Details' tab is active, showing fields for 'Label/Name' (set to 'test'), 'Description' (set to 'get snmpd'), 'Interval (minutes)' (set to 1), 'Retry (3 of times)' (set to 1), 'Primary Address' (set to '192.168.1.1'), 'Port' (set to 162), 'SNMP' (set to '1.94.02.1.2.1.1.0'), 'Secondary Address' (set to 'Monitor's address'), 'Port' (set to 162), and 'SNMP' (set to '00'). The bottom-right screenshot shows the 'Security' tab for the 'SNMP GET Probe'. It has fields for 'SNMP Type' (set to 'SNMPv2'), 'User Name' (set to 'admin@snmp'), 'Privacy Mode' (set to 'authPriv'), 'Auth Protocol' (set to 'SHA'), 'Auth Password' (set to 'password'), 'Privacy Protocol' (set to 'DES'), and 'Privacy Password' (set to 'password').

Figure 4-30: Creating an Auto-Probe

4. Main Menu

4.6 Network

The Network menu item allows for configuration of Internet, Network Services, and SMTP settings; each is covered in the sections, below.

Note: This menu item is visible only to those with Administrator privileges. Refer to the “Roles and Privileges” section for details.

4.6.1 Internet

This sub-menu allows for configuration of the Internet settings identified below. Click the **View Network Connection Details** button to view a summary of the currently-established network connection (Figure 4-31). Click the **Save** button once all edits have been made.

Domain

- To change or edit the Host Name, enter a new name in the provided field.
- Optionally enter a System Contact in the provided field.

IPv4

- Select the desired addressing method: Automatic, Manual or Disabled.
- If Static, enter valid values for IP Address, Subnet Mask and Gateway.

IPv6

- Select the desired addressing method: Automatic, Manual or Disabled.
- If Static, enter valid values for IP Address, Prefix and Gateway.

DNS

- Use the slider to enable or disable Manual DNS.
- If enabled, a Primary DNS server IP address or hostname must be entered.
- Optionally enter Secondary and Tertiary DNS Server addresses or host names.

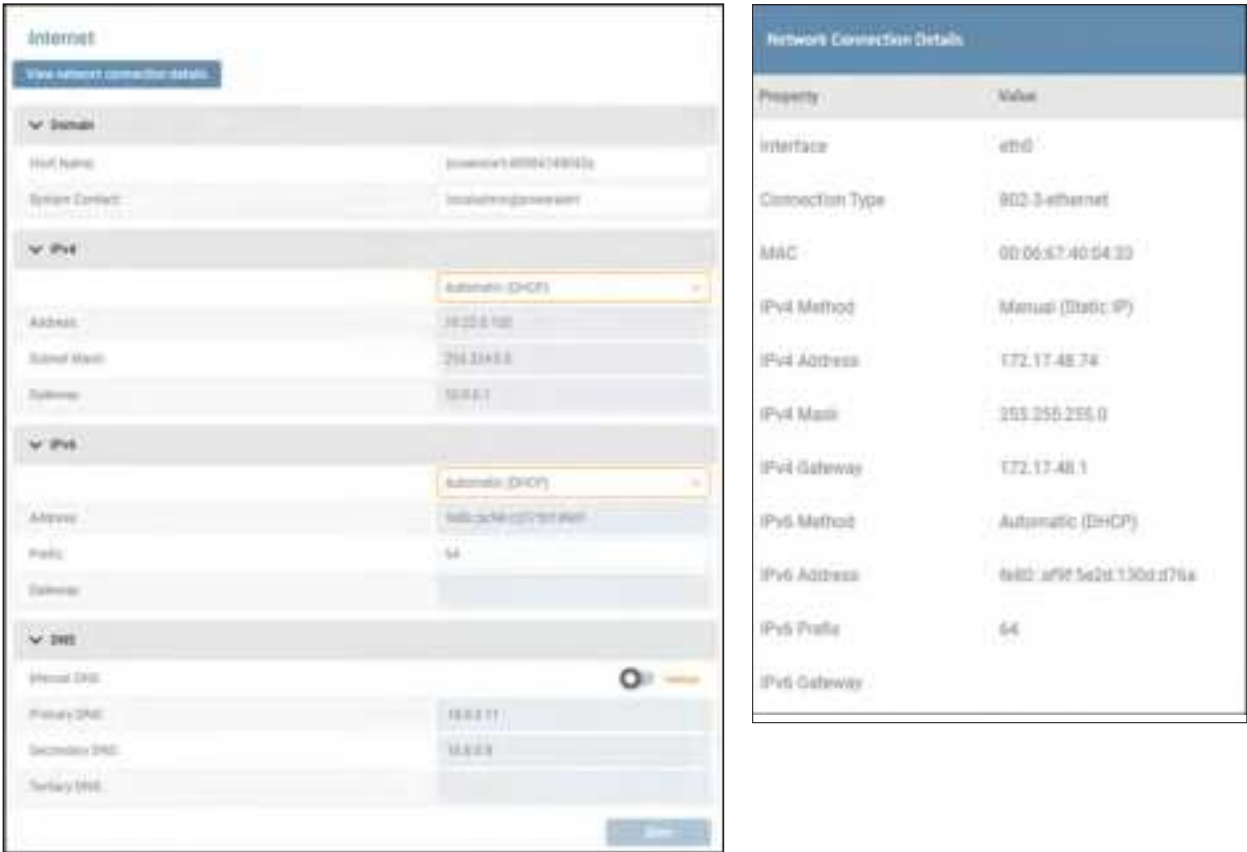


Figure 4-31: Internet Settings and Network Connection Details

4. Main Menu

Note that saved changes may require a reboot of PowerAlert in order to take effect. If so, a warning message will appear at the top of the page. Click the **Apply Now** button to proceed with the reboot (Figure 4-32). To avoid multiple reboots, make all required network configuration changes prior to executing **Apply Now**.

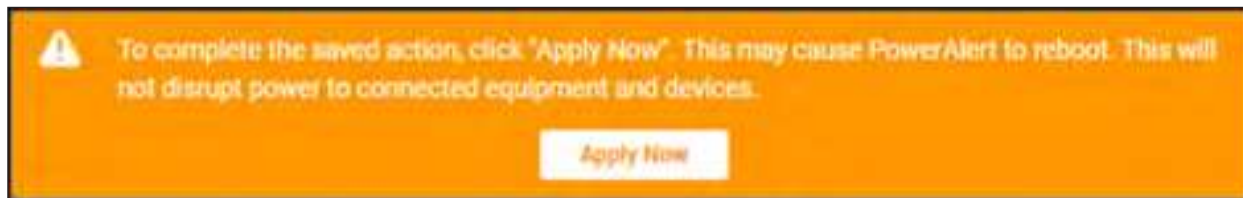


Figure 4-32: "Apply Now" message

4.6.2 Services

This sub-menu allows for configuration of the network services identified below (Figure 4-33) . Use the slider to the right of a service to enable/disable it. To change a port number, enter the new value in the appropriate field. Click the **Save** button once all edits have been made.

SNMP

- SNMPv1, SNMPv2c and SNMPv3 are all enabled, by default
- Default Get/Set Port = 161
- Default Trap Port = 162

HTTP

- HTTP, HTTPS and HTTP-to-HTTPS Redirection are all enabled, by default.
- Default HTTP Port = 80
- Default HTTPS Port = 443

SSH / SFTP / SCP

- SSH and SFTP/SCP are both enabled, by default
- Default Port = 22

Telnet

- Telnet is enabled by default
- Default Port = 23



Figure 4-33: Network Services Configuration

4.6.3 SMTP

This sub-menu allows for configuration of Simple Mail Transfer Protocol (SMTP) parameters and Email format settings. Click the **Save** button once all edits have been made.

SMTP Server

- Move the slider to enable or disable SMTP; default = disabled.
- Enter the IP address, host name or FQDN of the SMTP server. Disabled by default.
- Default Port = 25.

4. Main Menu

SMTP Authentication

- Move the slider to enable or disable SMTP Authentication; default = disabled.
- If enabled, enter valid values for SMTP User Name and SMTP Password.
- Select the applicable Security Type from the pulldown menu.

Email Format Settings

- Select the desired language from the pulldown menu.
- In the “From Line” field, enter the name that will appear as the sender of notification messages.

Note: When using SMTP servers such as Office365 and Gmail/Gsuite, consider using identical text for the “From Line” and “SMTP Username” fields. While PADM supports the use of different “From Line” and “SMTP Username” values, some SMTP servers may block emails if these fields are mismatched.

- In the “Subject Line” field, enter the information that will appear in the subject line of notification messages.



Figure 4-34: SMTP Configuration

If changes have been made, but not saved, a warning message will appear if there is an attempt to navigate away from the page (Figure 4-35).



Figure 4-35: Review Changes warning

4. Main Menu

4.7 Security

The Security menu item allows for configuration of User Accounts, Role & Privileges, Security Settings and Session Management.

Note: This menu item is visible only to those with Administrator privileges. Refer to the Roles and Privileges section for details.

4.7.1 Session Management

This sub-menu displays a list of all active users (i.e. users that are currently logged in), along with parameters pertinent to their sessions (Figure 4-36).



The screenshot shows the 'Active User Sessions' page. At the top right, there are links for 'Filter' and 'End Session(s)'. Below is a table with the following columns: Username, Name, Type, Location, Logged On, and Session Length. There are two rows of data.

Username	Name	Type	Location	Logged On	Session Length
locadmin		WEB	172.16.127.35	1/17/2020 2:55:11 PM	3m
locadmin		CONSOLE	172.16.127.35	1/17/2020 2:58:31 PM	5m

Figure 4-36: Session Management

The system supports the ability to terminate one or more sessions. Click the  icon to the left of each line item. On doing so, the **End Session(s)** button becomes active (turns red); click the button to complete the termination.



The screenshot shows the 'Active User Sessions' page with the 'End Session(s)' button highlighted in red. The table below shows the same data as Figure 4-36, but with a minus icon in the first column of the second row.

Username	Name	Type	Location	Logged On	Session Length
locadmin		WEB	172.16.127.35	1/17/2020 2:55:11 PM	3m
 locadmin		CONSOLE	172.16.127.35	1/17/2020 2:58:31 PM	5m

Figure 4-37: Terminating User Sessions

4.7.2 User Accounts

This sub-menu allows for the creation and management of user accounts, comprised of Local Users, SNMP Users and Remote Servers. Click on each tab to view its contents.

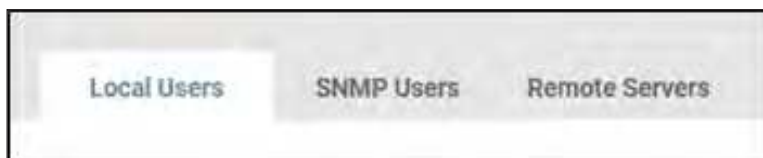


Figure 4-38: User Account tabs

4. Main Menu

LOCAL USERS. This tab displays a list of all individuals with login access to the system, as well as their status and related parameters (Figure 4-39). Five preconfigured Local Users are provided by default: *localadmin*, *localmanager*, *localguest*, *sysadmin* and *technician*. Click the pencil icon to the right of an entry to open a dialog box in which its settings can be adjusted. To delete one or more Local Users, click the  icon to the left of each line item. Upon doing so, the **Delete User(s)** button becomes active (turns red); click the button to complete the deletion.

Note: the default *localadmin*, *sysadmin* and *technician* users cannot be deleted.



	Status	Username	Full Name	Role	Description	IP	Timeout
		localadmin		Administrator			
		localmanager		Manager			
		localguest		Guest			
		sysadmin		System			
		technician		System			

Figure 4-39: Local Users

To create a new Local User, click **Add User**. In the User tab of the dialog box that opens, enter the required information; boxes outlined in color indicate required fields (Figure 4-40). Note that the Username must be at least 6 characters long. Minimum password length is set in the **Security Settings** sub-menu.

The role of System is reserved for maintenance and provisioning purposes; it cannot be assigned to new users. See the “Roles & Privileges” section for details.

By default, new Local Users are enabled. Move the title bar slider left to disable the user. A disabled user cannot log into the system nor receive system notifications. To override Global Password Age settings – as set in **Security Settings** – move the appropriate slider to the right, exposing the two settings:

- Minimum Age (days) – the number of days that the password must be used before it can be changed. The default value is 1 day.
- Maximum Age (days) – the number of days after which the password must be changed. The default value is 30 days.

Next, click on the *Session* tab to optionally adjust the following settings:

- Override Global Session Timeout – the amount of time, in minutes, that the session can be active before it is automatically terminated. The default value is 360 minutes.
- Override Global Idle Timeout -- the amount of time, in minutes, that the session can be idle (inactive) before it is automatically terminated. The default value is 60 minutes.

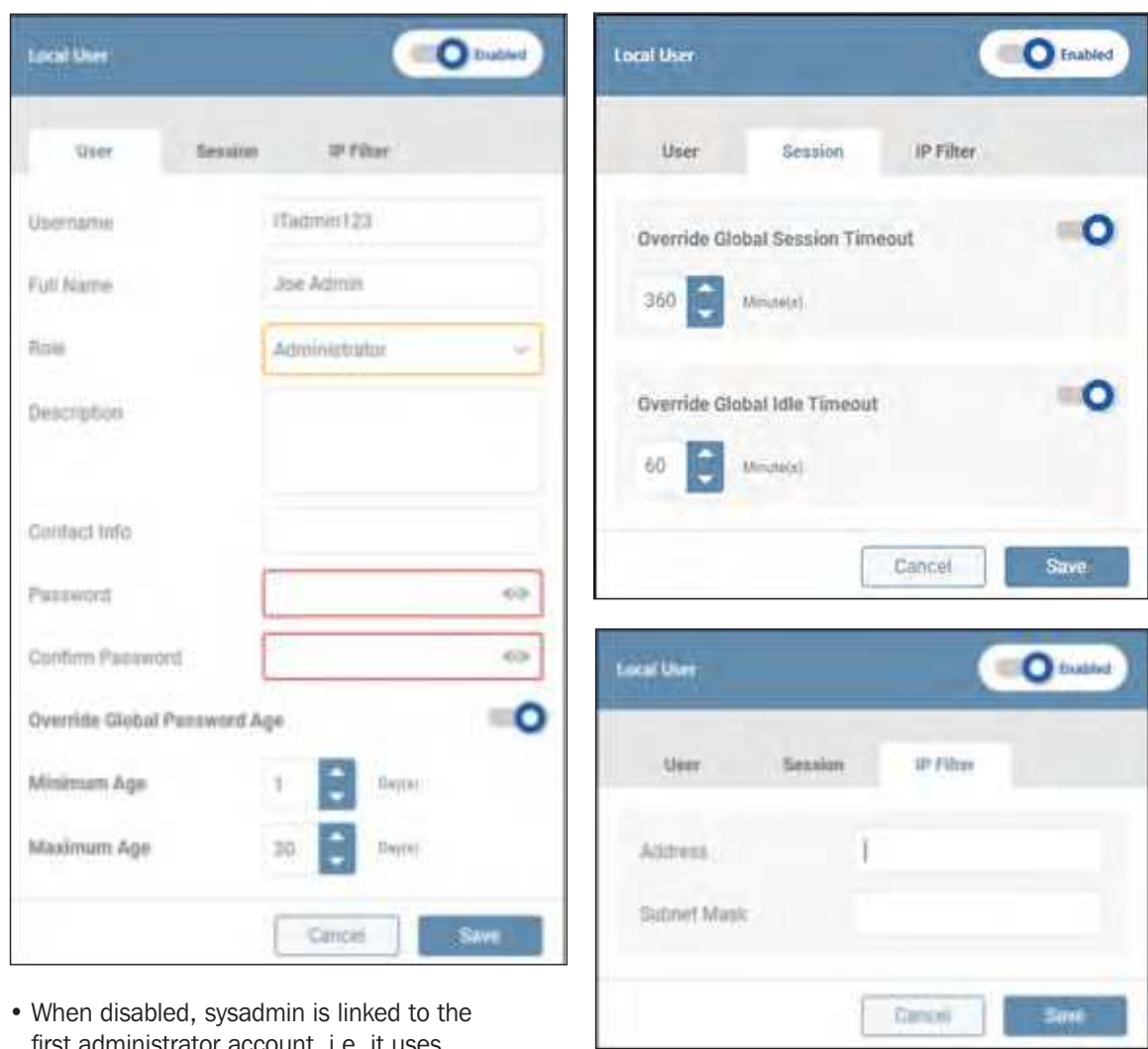
To change either setting, move the slider to the right position and adjust the time using the up and down arrows. The range of viable values is 1 to 999 minutes.

Click on the *IP Filter* tab to optionally specify an IP Address (and Subnet Mask) from which the Local User must log in, i.e. login from any other network location is prohibited. Click the **Save** button once all entries/edits have been made. PADM supports up to 64 local users.

4. Main Menu

The credentials for Local Users are as follows

User	Default Password
localadmin	localadmin
localmanager	localmanager
localguest	localguest
technician	TrippLite
sysadmin	See note below



- When disabled, sysadmin is linked to the first administrator account, i.e. it uses administrator’s password.
- When enabled, sysadmin is decoupled from the administrator account and can have its own password.

Figure 4-40: Adding a Local User

4. Main Menu

SNMP USERS. This tab displays a list of all entities having SNMP access to the system, as well as their status and related parameters (Figure 4-41). These entities are commonly used by network management systems and SNMP utilities for inbound SNMP Sets, SNMP Gets, and SNMP Walks to PADM. For outbound SNMP Traps, Informs, or SNMP Sets from PADM to external systems, see **Alert Contacts**. Click the pencil icon to the right of the SNMP User entry to open a dialog box in which its settings can be adjusted. To delete one or more SNMP Users, click the  icon to the left of each line item. On doing so, the **Delete User(s)** button becomes active (turns red); click the button to complete the deletion.

Status	Username	Role	Description	Type	IP
Disabled	admin	Guest		SNMPv1	
Disabled	mgmt	Manager		SNMPv2c	
Disabled	admin	Administrator		SNMPv3	
Disabled	mgmt	Manager		SNMPv3	
Disabled	mgmt	Guest		SNMPv3	

Figure 4-41: SNMP Users

To create a new SNMP User click **Add User** and select one of the SNMP versions; a corresponding dialog box opens. Enter the required information, denoted by the boxes outlined in color. Note: Usernames cannot contain spaces.

For SNMPv1 and SNMPv2c Users, click on the **IP Filter** tab to optionally specify the IP Address (and Subnet Mask) from which the user must log in, i.e. the user will not be able to login from any other IP Address.

When using IPv4 to allow a range of addresses, use the starting IP address of the range and the desired subnet mask. For example, to allow the range 192.168.1.0-192.168.1.255, use 192.168.1.0 (IP) and 255.255.255.0 (subnet mask). To allow only a single IPv4 address, use a /32 subnet (255.255.255.255) and the specific IP address you wish to allow. For example, to allow 10.20.30.40 ONLY, use 10.20.30.40 (IP) and 255.255.255.255 (mask).

By default, the user will be enabled. Move the title bar slider left to disable the user. A disabled user cannot access the system nor receive system communications. Click the **Save** button once all entries/edits have been made.

Figure 4-41: Creating an SNMP User – v1 and v3 Examples

4. Main Menu

REMOTE SERVERS. This tab displays a list RADIUS and LDAP servers configured to communicate with the system, as well as their status and related parameters (Figure 4-42). Click the pencil icon to the right of the Remote Server entry to open a dialog box in which its settings can be adjusted. To delete one or more Remote Servers, click the  icon to the left of each line item. On doing so, the **Delete Server(s)** button becomes active (turns red); click the button to complete the deletion.



Status	Label Name	Host Name/IP	Type	Auth. Port	Auth. Port #	Priority	
Enabled	RADsrv1	192.168.2.2	RADIUS	1812	1812	1	
Enabled	RADsrv2	192.168.2.2	RADIUS	1812	1812	2	
Enabled	LDAPsrv1	192.168.4.4	LDAP		389	3	

Figure 4-42: Remote Servers

To create a new Remote Server entry click **Add a Server** (Figure 4-43) and select one of the server types: RADIUS or LDAP; a corresponding dialog box opens. Enter the required information, denoted by the boxes outlined in color.

For RADIUS Server entries, either Authentication Port or Accounting Port (or both) must be selected. The default Authentication Port value is 1812. To test authenticated communications to RADIUS and/or LDAP Server entries, click the **Test Authentication** button. A message will appear to the right of the button indicating whether or not the test was successful. By default, new entries are enabled; move the title bar slider left to disable the entry. Disabling the entry will disallow it from communicating with the system. Click the **Save** button once all entries/edits have been made.

Note: the default role of **Administrator** cannot be authorized by LDAP servers. To resolve this, create new roles with equivalent privileges (see **LOCAL USERS** section). LDAP users will be authorized based on group membership (the “memberof” attribute). For example, an Active Directory user in the group “UPSadmin” would be authorized to access PADM based on the privileges assigned to the “UPSadmin” role created in PADM.



The figure shows two dialog boxes for adding servers. The top dialog is for a RADIUS Server, with fields for Label Name (RADsrv1), Host Name/IP Address (192.168.2.2), Authentication Port (1812), Accounting Port (1812), Priority (1), and a Test Authentication button. The bottom dialog is for an LDAP Server, with fields for Label Name (LDAPsrv1), Host Name/IP Address (192.168.4.4), Port (389), Priority (3), LDAP Server Type (Open LDAP), and a Test Authentication button. Both dialogs have a 'Save' button at the bottom right.

Figure 4-43: Adding a RADIUS Server and an LDAP Server

4. Main Menu

4.7.3 Roles & Privileges

This sub-menu allows for the management of default roles as well as the creation of custom roles (Figure 4-43). In general, the default roles have the following privileges:

- *Administrator* – read/write access to all areas of the interface.
- *Manager* – read/write access to operational areas of the interface.
A Manager does NOT have access to Network configuration or Security settings.
- *Monitor* – read-only access to all areas of the interface.
- *Guest* – read-only access to operational areas of the interface.
- *System* – this role is reserved and cannot be assigned to users. User *technician* allows access to the LX Platform device interface via the console port for provisioning purposes. User *sysadmin* provides limited system-level access to the LX Platform device interface for troubleshooting purposes.

Refer to Appendix A for a detailed summary of the default privileges for *Administrator*, *Manager*, *Monitor* and *Guest*.

Click the pencil icon to the right of the Role entry to open a dialog box in which its settings can be adjusted.

Note: the default *Administrator*, *Monitor* and *System* Roles cannot be edited.



Figure 4-44: Roles & Privileges

To create a customized Role, click **Add a Role**. In the dialog box that appears, enter a name for the Role and, optionally, a description (Figure 4-45). Note that names cannot contain spaces. Next, click on the Privileges tab to view and select applicable privileges. Privileges will vary based on device type and model. Click the **Save** button once all entries/edits have been made. To delete one or custom Roles, click the  icon to the left of each line item. On doing so, the **Delete Role(s)** button becomes active (turns red); click the button to complete the deletion.

Note:

- The default Roles cannot be deleted.
- To achieve the same functionality of the “Realms” feature (available in previous firmware versions), click on the applicable load Privilege. In the window that opens, select all applicable loads, then click the **Save** button.

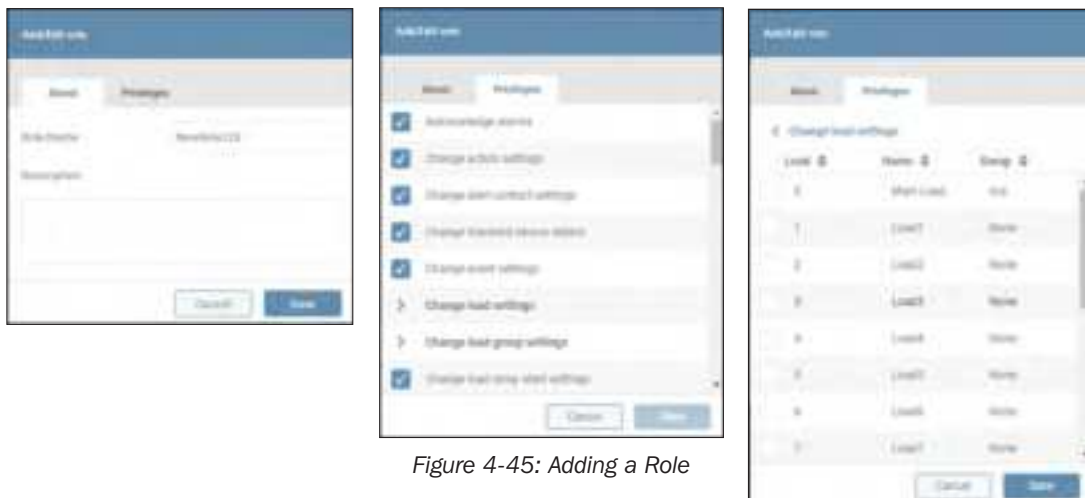


Figure 4-45: Adding a Role

4. Main Menu

4.7.4 Security Settings

This sub-menu allows for configuration of Global Security Settings (Figure 4-46).

- Global Session Timeout – the amount of time, in minutes, that sessions can be active, after which they are automatically terminated. The default value is 360 minutes.
- Global Idle Timeout -- the amount of time, in minutes, that sessions can be idle (inactive) after which they are automatically terminated. The default value is 60 minutes.

Use the up and down arrows to adjust the settings. The range of viable values is 1 to 999 minutes

To apply and modify Password Age Requirements, move the appropriate slider to the right.

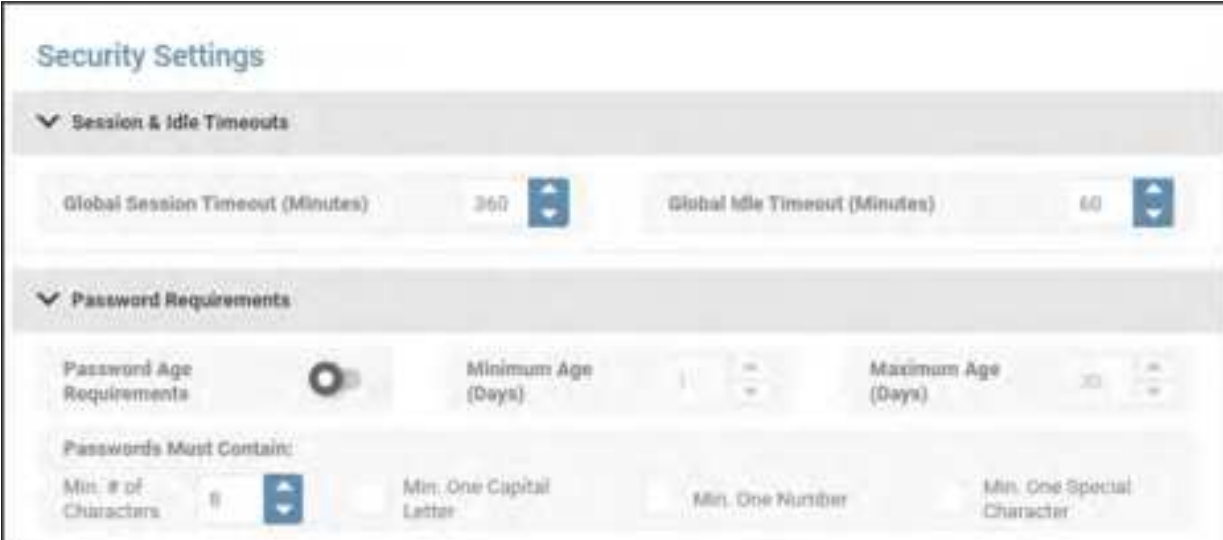
- Minimum Age – the number of days that the password must be used before it can be changed. The default value is 7 days. The viable range is 0 to 999 days.
- Maximum Age – the number of days after which the password must be changed. The default value is 60 days. The viable range is 1 to 999 days.

Use the up and down arrows to adjust the settings.

Note: The Maximum Age must be larger than the Minimum Age

The default minimum number of characters required of all passwords is 8. Use the up and down arrows to adjust this value. Optionally select whether passwords must contain a minimum of one capital letter, one number and/or one special character.

Changes to password policies will take effect the next time the password is changed.



The screenshot displays the 'Security Settings' interface. It is divided into two main sections: 'Session & Idle Timeouts' and 'Password Requirements'. In the 'Session & Idle Timeouts' section, there are two settings: 'Global Session Timeout (Minutes)' with a value of 360 and 'Global Idle Timeout (Minutes)' with a value of 60. Both have up and down arrows for adjustment. The 'Password Requirements' section includes a toggle for 'Password Age Requirements' which is currently turned on. Below this, there are sliders for 'Minimum Age (Days)' and 'Maximum Age (Days)'. The 'Minimum Age' is set to 7 and the 'Maximum Age' is set to 60. At the bottom, there is a section titled 'Passwords Must Contain:' with four checkboxes: 'Min. # of Characters' (set to 8), 'Min. One Capital Letter', 'Min. One Number', and 'Min. One Special Character'.

Figure 4-46: Setting Timeouts and Password Requirements

4. Main Menu

PADM20 allows the import of a Secure Socket Layer (SSL) Certificate (Base64 .pem format). Click the **Add SSL Certificate** button to open a dialog box in which the SSL Certificate and SSL Key can be located and selected (Figure 4-47). Upon entering the Password, click the **Upload** button. Click the **View Certificate** button to view the details of the Certificate in use. Click the **Download Certificate** button to locally save the SSL Certificate.



Figure 4-47: Adding an SSL Certificate

To set the preferred Authorization and Accounting Schemes, select the desired setting from the respective pulldown menus (Figure 4-48).

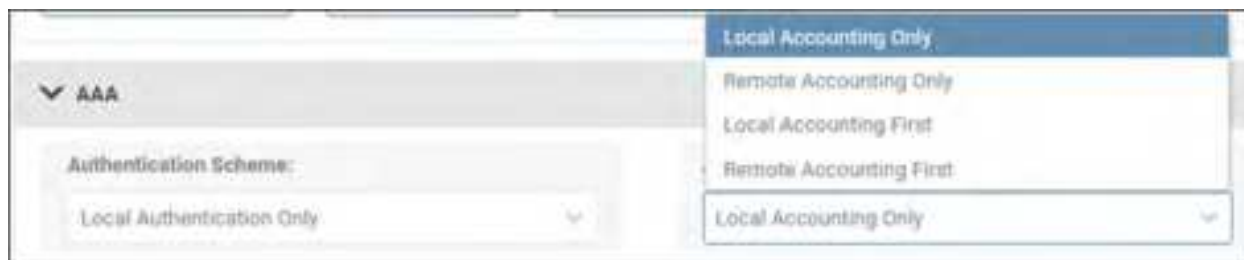


Figure 4-48: AAA Settings

Once all Security Settings have been set, click the **Save** button.

4. Main Menu

4.8 Logs

The Logs menu item allows for configuration, viewing and export of the Event, Data and Accounting Logs, as well as configuration of Syslog and the Application Log.

Note: All logs are exported as .gz files. To view the log information, the .gz file must first be decompressed using a program like 7zip or WinRAR® (Windows) or gzip (Linux/macOS).



Figure 4-49: Logs Menu Item

4.8.1 Accounting Log

The Accounting Log documents events related to access of the device interfaces, displaying the most recent events at the top of the log (Figure 4-50). Click **Filter** to customize the information displayed in the log. To perform an on-demand log export, click the **Export** button; a window will appear in which the file format (CSV or XML) and export destination can be selected. Select the **Download** option to locally export the log. On selecting the **Email** option, a table of recipients will appear, one of which can be selected. Refer to the **Alert Contacts** section of the **Events & Actions** menu item for creating email recipients.

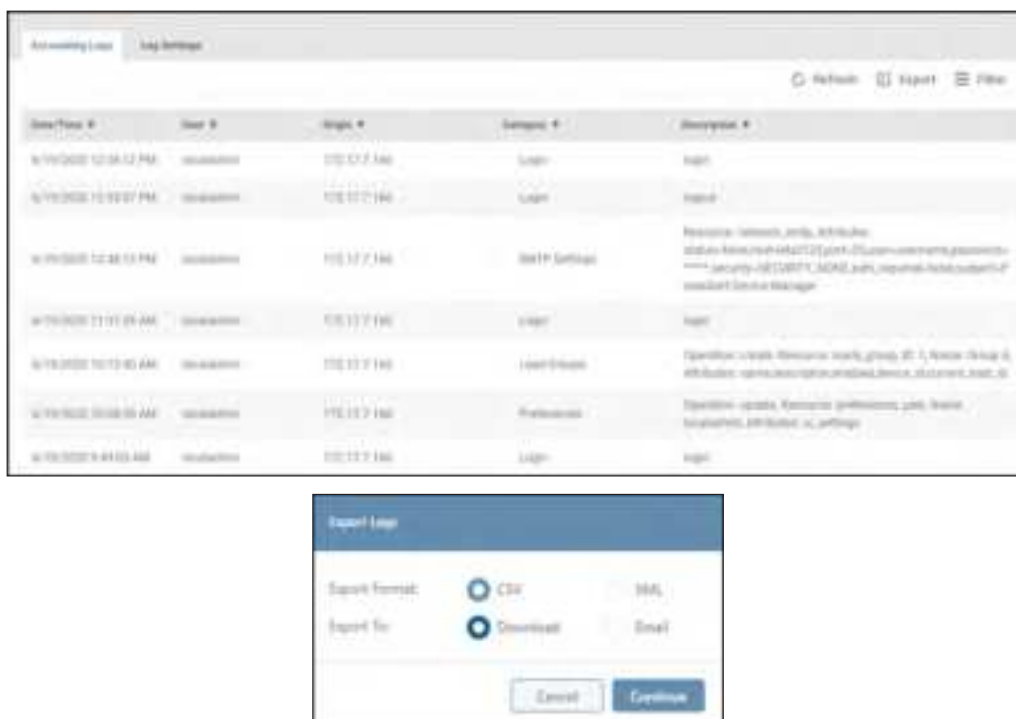


Figure 4-50: Accounting Log Summary and Export

4. Main Menu

To configure log size and automatic log exporting, click on the Log Settings tab (Figure 4-51). The maximum number of log entries is 10,000; this is also the default value. The minimum log size is 1,000 entries. Upon reaching the maximum log size, entries are purged in a first-in-first-out manner. To enable the Automatic Export option, move the slider to the right position. Select the preferred export format: CSV or XML. Click the **Select Recipients** button to set which email contacts are to receive the export (email recipients are created in Security > User Accounts).

Note: Automatic Export is applied to the older half of the Log. For example, if the maximum number of stored entries is set to 5000 (entry #1 being the most recent), upon reaching the maximum, entries #2500 through #5000 would be exported and simultaneously purged from the viewable Accounting Log.

Click **Save** once all edits have been made.



Figure 4-51: Accounting Log Settings

4.8.2 Application Log

The Application Log is not locally displayed. To view the Application log, click **Export Application Logs Now** button and select either the Download or Email option (Figure 4-52); for Email, select up to five recipients (created in Events & Actions > Alert Contacts). To purge the Application log after exporting, check the appropriate box. Click the **Continue** button to execute the export. Use a standard text editor application to view the exported file. To enable the Automatic Export option, move the slider to the right position. Click the Select Recipients button to set which email contacts are to receive the export (email recipients are created in Security > User Accounts).

Note: The frequency of automatic exports will vary depending on log size. Once per hour is the shortest interval between exports.



Figure 4-52: Application Log and manual export

4. Main Menu

To set the minimum severity level at which items are to be recorded, click the Minimum Severity Setting menu and select the desired level. For instance, a setting of ‘Critical’ will also record the Alert and Emergency items (Figure 4-53).



Figure 4-53: Minimum Severity Setting

4.8.3 Data Log

The Data Log provides two views: Time-Series and Historical Roll-Up. The Time Series view displays the device’s metrics taken at 1-minute increments, with the most recent readings appearing at the top of the log (Figure 4-54).

Data Log											
Data Log Buttons		Log Settings									
		View Refresh Export Filter									
Device Name		DeviceID:1									
Sample Time	Runtime Remaining (Min)	Battery		Input		Output					
		Battery Charge Remaining	Battery Voltage	Battery Temperature (C)	Battery Temperature (F)	Input Frequency	Input Voltage	Output Frequency	Output Current	Output Utilization	Temp (F)
		%	V	C	F	Hz	V	Hz	A	%	F
1/23/2020 10:05:00 AM	417	100.0	27.3	34.0	93.2	58.7	120.1	58.7	0.0	0.0	
1/23/2020 10:06:00 AM	437	100.0	27.3	34.0	93.2	58.6	120.0	58.7	0.0	0.0	
1/23/2020 10:07:00 AM	437	100.0	27.3	34.0	93.2	58.7	120.1	58.7	0.0	0.0	
1/23/2020 10:08:00 AM	437	100.0	27.3	34.0	93.2	58.8	120.0	58.8	0.0	0.0	

Figure 4-54: Data Log, Time Series View.

4. Main Menu

Click the **View** button to select which data variable are to be displayed (Figure 4-55). Click **Filter** to refine the time period of data log entries to be displayed; click the calendar icon to establish the start and end time/date. To perform an on-demand log export, click the **Export** button; a window will appear in which the export destination can be selected. Select the Download option to locally export the log. On selecting the Email option, a table of recipients will appear, one of which can be selected. Refer to **Alert Contacts** in section 4.5 Events & Actions for details on creating email recipients. Data logs can be exported only in CSV format.

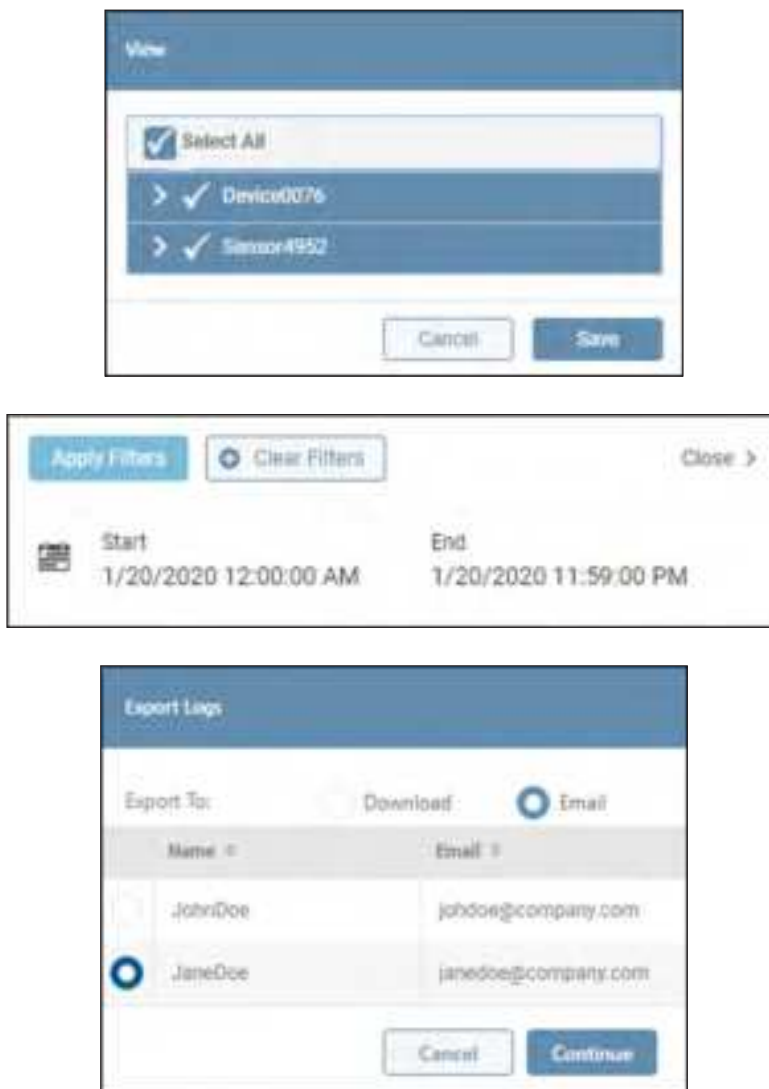


Figure 4-55. Changing the Viewed Data, Applying Filters and Configuring On-Demand Log Export

4. Main Menu

The Historical Roll-Up view displays a summary view of the device's metrics at the following increments: hourly, daily, weekly, monthly and yearly (Figure 4-56).

Time Log

Time Log Roll-up

Log Settings

▼ View

↺ Refresh

📄 Export

Sensor Name													
Date/Time	Input Frequency 1			Input Frequency 2			Input Frequency 3			Input Voltage (1-12)			
	Low	High	Average	Low	High	Average	Low	High	Average	Low	High	Average	Low
	Min	Max	Avg	Min	Max	Avg	Min	Max	Avg	V	V	V	V
Hourly	50.5	60.0	55.0	50.5	60.0	55.0	50.5	60.0	55.0	212.5	213.0	214.0	214.4
Daily	50.5	60.0	55.0	50.5	60.0	55.0	50.5	60.0	55.0	212.2	221.0	216.4	216.4
Weekly	50.5	60.0	55.0	50.5	60.0	55.0	50.5	60.0	55.0	212.5	222.4	217.0	215.1
Monthly													
Yearly													

4

Figure 4-56: Data Log, Roll-up View

To configure log recording parameters and automatic log exporting, click on the Log Settings tab. Set the frequency at which data is collected by adjusting the interval; the supported range is 10 to 60 seconds, in increments of 10 seconds. A message will appear showing the estimated amount of data (in days) that will be recorded, based on the selected interval (Figure 4-57).

Based on the time intervals selected 6 day(s) of Data Logs will be saved.
Note: The Data Log time period may be lengthened by reducing the number of variables and/or increasing the interval between saves.

Figure 4-57: Data Log Settings Message

By default, all metrics of the host device and all connected sensors are selected. Click the pencil icon and use the pulldown menus to select which variables are to be logged. To enable Automatic Export, move the slider to the right position. By default, the "Export to all contact recipients" box is checked. Otherwise, click the **Select up to five Recipients** button to set which email contacts are to receive the export. Refer to **Alert Contacts** in section **4.5 Events & Actions** for details on creating email recipients. Click the **Save** button once all edits have been made (Figure 4-58).

Note: changing the logging interval will purge the Data Log prior to logging records at the new interval. If desired, export the Data Log prior to applying the interval change.

4. Main Menu

Automatic export of the Data Log occurs once per day (at midnight) or twice per day (noon and midnight), depending on the log settings. If the Data Log Settings message states that only one day of records will be collected/displayed, then the auto-export will occur twice per day. For all other cases, the auto-export will occur once per day.

The screenshot displays the 'Data Log Settings' interface. At the top, there are tabs for 'Data Logs', 'Data Log Bulkops', and 'Log Settings'. The 'Log Settings' tab is active. Below the tabs, the 'Export Criteria' section includes a dropdown for 'Interval in seconds to record data' set to '60'. A table lists the devices and their variable counts:

Device #	# of Variables #
Device0076	11
Sensor4552	3

Below the table, a note states: 'Based on the filter intervals selected 5 day(s) of Data Logs will be saved. Note: The Data Log time period may be lengthened by reducing the number of variables and/or decreasing the interval between saves.' The 'Export logs automatically' checkbox is checked. To the right, the 'Export to all contact recipients' checkbox is also checked, with a 'Select Log to Save Recipients' button. Below these, there are five empty input fields for recipients. A 'Save' button is at the bottom right. An inset window titled 'Select Variables to Log' is open, showing a list of variables with checkboxes. The variables are grouped by device: Device0076 (checked), Device (checked), Battery (checked), Maritime Remaining (Min) (checked), Battery Charge Remaining (checked), Battery Voltage (checked), Battery Temperature (C) (checked), Battery Temperature (F) (checked), Input (checked), Output (checked), Sensor4552 (unchecked), and Environment (unchecked). 'Cancel' and 'Save' buttons are at the bottom of the inset.

Figure 4-58: Data Log Settings

4. Main Menu

4.8.4 Event Log

The Event Log tracks device and system-related events, displaying the most recent events at the top of the log (Figure 4-59). Click **Filter** to customize the information displayed in the log. To perform an on-demand log export, click the **Export** button; a window will appear in which file format (CSV or XML) and export destination can be selected. Select the **Download** option to locally export the log. On selecting the **Email** option, a table of recipients will appear, one of which can be selected. Refer to **Alert Contacts** in section 4.5 Events & Actions for details on creating email recipients. To purge the log after exporting, check the appropriate box.



The screenshot shows the 'Event Log' tab in a web interface. At the top right are buttons for 'Refresh', 'Export', and 'Filter'. Below these is a table with four columns: 'Type', 'DateTime', 'Device', and 'Description'. The table contains three entries, all marked as 'Warning'. The first entry is 'PowerAlert Started' at '1/20/2020 9:22:03 AM' from 'PowerAlert'. The second is 'Watchdog NTP Probe Failed' at '1/20/2020 9:21:54 AM' from 'Same Autoprobe'. The third is 'Watchdog Ping Probe Failed' at '1/20/2020 9:21:52 AM' from 'Same Autoprobe'. Each entry has a small information icon to its right. At the bottom of the table are navigation controls for pagination.

Type	DateTime	Device	Description
Warning	1/20/2020 9:22:03 AM	PowerAlert	PowerAlert Started
Warning	1/20/2020 9:21:54 AM	Same Autoprobe	Watchdog NTP Probe Failed
Warning	1/20/2020 9:21:52 AM	Same Autoprobe	Watchdog Ping Probe Failed

Figure 4-59: Event Log

To configure log recording parameters and automatic log exporting, click on the **Log Settings** tab (Figure 4-60). The maximum number of log entries is 10,000; this is also the default value. The minimum log size is 1,000 entries. Upon reaching the maximum log size, entries will be purged in a first-in-first-out manner. To enable Automatic Export, move the slider to the right position. Click the **Select Recipients** button to set which email contacts are to receive the export.

Note: Automatic Export is applied to the older half of the log. For example, if the maximum number of stored entries is set to 5000, (entry #1 being the most recent), upon reaching the maximum, entries #2500 through #5000 would be exported and simultaneously purged from the viewable Event Log.

Click the **Save** button once all edits have been made.



The screenshot shows the 'Log Settings' tab. It includes a 'Maximum number of stored log entries' field set to 10000. Below this is a section for 'Export logs automatically' with a slider set to 'On'. A yellow warning box states: 'Automatic log export will remove older log entries upon completion.' The 'Export Format' is set to 'XML'. To the right, there is a 'Select recipients' button and a list of email addresses for export destinations.

Figure 4-60: Event Log Settings

4. Main Menu

4.8.5 Syslog

This sub-menu allows for creation and management of Syslog server entries. Placing the cursor over the information icon in the “Logs” column displays the log types selected for the Syslog server entry. Click the pencil icon to the right of the entry to open a dialog box in which its settings can be adjusted. To delete one or more Syslog Server entries, click the  icon to the left of each line item. Upon doing so, the **Delete Syslog Server(s)** button becomes active (turns red); click the button to complete the deletion.



Status	Label/Name	Host	Port	Facility	Severity	Logs
 Enabled	syslogABC	192.168.33.33	514	23	Alert	 
 Enabled	syslog123	192.168.44.35	515	22	Debug	 

Figure 4-61: Syslog Servers

To add a Syslog entry, click **Add Syslog Server**. In the dialog box that opens, enter the required information: Label/Name, Host, Port, Facility (13 and 15 are reserved for system use) and Severity. Note that the selected severity level determines the minimum level at which items are to be recorded. For instance, a setting of ‘Critical’ will also record the Alert and Emergency items. For the “Logs” item, set which log type records are to be sent to the Syslog server entry. By default, new entries are enabled; move the title bar slider left to disable the entry. Syslog messages will not be sent to a disabled entry. Click the **Save** button once all edits have been made.



Syslog Servers Enabled

Label/Name

syslogABC

Host

192.168.33.33

Port

514

Facility

23

Severity

Alert

Logs

☐ Application ☒ Data ☒ Event

Cancel

Save

Figure 4-62: Adding and Deleting a Syslog Server

5. Technical Support

For questions or information related to PADM, please contact Tripp Lite Tech Support:

Phone: 773.869.1234 (7am – 6pm CST).

Web: tripplite.com/support

Email: techsupport@tripplite.com

Note: *Online Product Support and Tripp Lite Technical Support contact information are also available via the Help icon in the PADM Top Menu.*

Appendix A – Privileges Chart

TOP MENU		Administrator	Manager	Guest	Monitor
Alerts	View, Sort, Filter	✓	✓	✓	✓
	Acknowledge	✓	✓		
	Export	✓	✓		
Language	Set Language preference	✓	✓	✓	✓
Global Settings	View Global Settings	✓	✓	✓	✓
	Set Defaults: Language, Time, Date...	✓			
Maintenance	Check for Firmware Updates	✓			
	Update Firmware	✓			
	Backup PowerAlert	✓			
	Restore from Saved Backup	✓			
	Restore PowerAlert to Factory Defaults	✓			
Reboot PowerAlert		✓	✓		
Restart Device		✓	✓		
Shutdown Device		✓	✓		
Help	View Help, About PADM, Download MIBs	✓	✓	✓	✓
User	Change Password, Set Preferences, Log Out	✓	✓	✓	✓

Appendix A – Privileges Chart

MAIN MENU		Administrator	Manager	Guest	Monitor
Dashboard	View Dashboard	✓	✓	✓	✓
	Add/Edit Graphs and Gauges	✓	✓	✓	✓
	Edit Gauge Thresholds	✓	✓		
Device	View and Filter Details and Properties	✓	✓	✓	✓
	Edit Details and Properties	✓	✓		
	Delete Inactive Devices	✓	✓		
	Execute Controls (e.g. self-test, buzzer)	✓	✓		
Loads	View, Sort and Filter Loads/Load Groups	✓	✓	✓	✓
	Edit Load Parameters and Properties	✓	✓		
	Add, Edit and Delete Load Groups	✓	✓		
	Edit Load Ramp and Shed Parameters	✓	✓		
	Execute Controls (on/off/cycle)	✓	✓		
Batteries	View and Sort Batteries	✓	✓	✓	✓
	Edit Battery Parameters and Properties	✓	✓		
	Add / Delete External Batteries	✓	✓		
Events & Actions	View, Sort and Filter Events	✓	✓	✓	✓
	Edit Event Parameters	✓	✓		
	Link and Edit Actions	✓	✓		
	View and Sort Alert Contacts	✓	✓	✓	✓
	Add, Edit and Delete Alert Contacts	✓	✓		
	View and Sort Actions	✓	✓	✓	✓
	Add, Edit, Delete Actions	✓	✓		
	View and Sort Scheduled Actions	✓	✓		✓
	Add, Edit, Delete Scheduled Actions	✓	✓		
	View, Sort and Filter AutoProbes	✓	✓	✓	✓
	Add, Edit, Delete Auto-Probes	✓	✓		
Network	View Network Settings	✓			✓
	Edit Network Settings	✓			

Appendix A – Privileges Chart

MAIN MENU		Administrator	Manager	Guest	Monitor
Security	View, Sort and Filter Active User Sessions	✓			✓
	Terminate User Sessions	✓			
	View and Sort all Users (Local, SNMP, Remote)	✓			✓
	Add, Edit Delete all Users	✓			
	View Roles	✓			✓
	Add, Edit and Delete Roles	✓			
	View Security Settings	✓			✓
	Set Global Timeout settings	✓			
	Set Global Password Requirements	✓			
	View and Download SSL Certificate	✓			✓
	Add SSL Certificate	✓			
	Set AAA Settings	✓			
Logging	View, Filter, Sort and Refresh Accounting Log	✓			✓
	Export Accounting Log	✓			
	View Accounting Log Settings	✓			✓
	Edit Accounting Log Settings	✓			
	Export Application Log	✓			
	View Application Log Settings	✓			✓
	Edit Application Log Settings	✓			
	View, Filter, Sort and Refresh Data+Rollup Log	✓	✓		✓
	Export Data Log	✓	✓		
	View Data Log Settings	✓	✓		✓
	Edit Data Log Settings	✓			
	View, Filter, Sort and Refresh Event Log	✓	✓	✓	✓
	Export Event Log	✓	✓		
	View Event Log Settings	✓	✓		✓
	Edit Event Log Settings	✓			
	View Syslog Entries	✓			✓
	Add, Edit and Delete Syslog Entries	✓			

Appendix B – Supplemental Information

This section describes certain operations and scenarios which may be encountered when using Power Alert Device Manager.

- When updating firmware from 15.x.x to 20.x.x, the device configuration will be maintained, but the event and data logs will be erased. To retain a record of the event and data logs, use the export function prior to performing the firmware update.
- For UPS models beginning with SU5KRT and SU6KRT, when the Power Module is disconnected from one detachable PDU and connected to a different one, the Power Module will not automatically detect the difference. Performing a “Restore LX to Factory Defaults” will allow the Power Module to read the outlet configuration of the new detachable PDU.
- When updating firmware from 15.x.x to 20.x.x, existing SNMPv3 users will become two discrete users. For each 15.x.x SNMPv3 user, a Local User with a matching username and password and SNMP User with a matching username, authorization passphrase, and privacy passphrase (as applicable) will be created in 20.x.x.
- The only supported major release downgrade (20.x.x to 15.x.x) is to 15.5.7. If a downgrade is needed to an earlier version, first perform the major release downgrade to 15.5.7, then a second downgrade to the desired version. Note that the major release downgrade to 15.5.7 will reset the LX interface to Factory Default Settings and will not retain network settings; it will revert to DHCP.
- In firmware version 15.x.x, thresholds operate on the “greater than” and “less than” principle, i.e. the measured value has to exceed the set threshold in order to trigger an event. In firmware version 20.x.x, thresholds operate on the “greater than or equal to” and “less than or equal to” principle, i.e. the event will trigger when the measured value reaches the threshold.
- In firmware version 20.x.x, certain usernames are reserved for system use. As a result, when updating firmware from 15.x.x to 20.x.x, users with a reserved user name will NOT be migrated. The following are the reserved user names: daemon, www-data, backup, nobody, systemd-network, systemd-resolve, messagebus, freerad, syslog, _chrony, telnetd, padm.service.
- The “Realms” feature supported in 15.x.x grants users management access to (only) specified individual loads. PADM20 does not have “Realms”, but supports the same functionality (see Roles & Privileges). When updating firmware from 15.x.x to 20.x.x, any Realms assigned to users will automatically convert to the equivalent load Privileges.
- For devices that support temperature measurement, the accuracy resolution will vary by device model. When adjusting temperature settings (e.g. thresholds), PADM may round up or round down a decimal value to a whole number. This rounding difference may be amplified during conversion to Fahrenheit or Celsius; as a result, the setting may vary by as much as 2 degrees from the entered value.
- If an E2 sensor is connected to an active LX platform device, the PowerAlert Device Manager will not automatically acknowledge it in the GUI. For instance, the data log will not begin displaying data from the sensor. Log out, then log back into the device to begin displaying the sensor’s data and events.

If a WEBCARDLX is moved from one device to another, the behavior will vary depending on whether the devices are “similar” or “dissimilar”.

“Similar” devices = same or similar model e.g. two UPSes of the same model, two PDUs with similar feature sets, etc.

“Dissimilar “ devices = different models or device types e.g. SRCOOL air-conditioner to an online UPS.

- For Dissimilar devices: An “inactive device” reference may appear in the GUI of the new device. This occurs because WEBCARDLX retains the identity information from the previous device. To remove references to ‘inactive device’, click on the delete icon next to the line item.
- For Similar devices: The WEBCARDLX will retain settings (e.g. power-on delay, output voltage settings, power strategy, thresholds, etc) from the previous device and will attempt to apply them to the new device. This may be undesirable, especially if the new device is a different model. To prevent the previous settings being applied to the new device, perform a Factory Default reset of the WEBCARDLX before installing it in the new device.

Appendix C – SNMP commands

When issuing SNMP Set commands to add certain records, firmware version 20.x.x. requires multiple data fields to be concurrently entered, i.e. a “bulk set”. By contrast, firmware version 15.x.x. allows individual data fields to be entered

For example, to create Load Groups in 20.x.x, the tlpPduOutletGroupRowStatus.1.1 OID cannot be Set by itself. The tlpPduOutletGroupName.1.1 OID and tlpPduOutletGroupDescription.1.1 OID must be included to successfully Set the tlpPduOutletGroupRowStatus.1.1 OID.

Example:

```
$ snmpset -v2c -ctripplite 10.22.0.52 tlpPduOutletGroupRowStatus.1.1 i 5 tlpPduOutletGroupName.1.1 s "Load Group Name" tlpPduOutletGroupDescription.1.1 s "Load Group Description"
```

```
TRIPPLITE-PRODUCTS::tlpPduOutletGroupRowStatus.1.1 = INTEGER: createAndWait(5)
```

```
TRIPPLITE-PRODUCTS::tlpPduOutletGroupName.1.1 = STRING: Load Group Name
```

```
TRIPPLITE-PRODUCTS::tlpPduOutletGroupDescription.1.1 = STRING: Load Group Description
```

Tripp Lite has a policy of continuous improvement. Specifications are subject to change without notice. Photos and illustrations may differ slightly from actual products.

