

# User's Guide

## PowerAlert® Office

### WARRANTY REGISTRATION

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

**[tripplite.com/warranty](http://tripplite.com/warranty)**



1111 W. 35th Street, Chicago, IL 60609 USA • [tripplite.com/support](http://tripplite.com/support)

Copyright © 2021 Tripp Lite. All rights reserved.

# Table of Contents

<b>1. Introduction</b>		<b>4.7 Security</b>	<b>48</b>
1.1 System Requirements	3	4.7.1 Session Management	48
<b>2. Initial Configuration</b>		4.7.2 User Accounts	48
2.1 SNMP Configuration	4	4.7.3 Roles & Privileges	53
<b>3. PowerAlert Office</b>		4.7.4 Security Settings	54
3.1 Accessing the Interface	5	<b>4.8 Logs</b>	<b>55</b>
3.2 PowerAlert Overview	7	4.8.1 Accounting Log	56
3.3 Top Menu	12	4.8.2 Application Log	57
<b>4. Main Menu</b>		4.8.3 Data Log	58
4.1 Dashboard	25	4.8.4 Event Log	62
4.2 Device	27	4.8.5 Syslog	63
4.3 Loads	30	<b>5. Technical Support</b>	<b>64</b>
4.4 Batteries	33	<b>Appendix A –</b>	
4.5 Events & Actions	36	Features by Package	65
4.6 Network	45		
4.6.1 Internet	45		
4.6.2 Services	46		
4.6.3 SMTP	46		

# 1. Introduction

PowerAlert software provides monitoring and control functions of one or two UPS systems. PowerAlert software is installed on a desktop PC or networked server which connects to the UPS system(s) through a serial or USB cable connection. This software can be configured to automatically shut down the computer in the event of a power failure. PowerAlert software also allows the UPS system to appear as an SNMP-manageable device on the network, enabling remote monitoring and control via PowerAlert Network Management System (PANMS) software or a third-party Network Management System.

PowerAlert software is available in three packages:

- **Office** - Advanced monitoring and control functions
- **Home** - Basic monitoring and control functions
- **Medical** - Monitoring and control functions optimized for use with Tripp Lite Medical Cart solutions

Refer to Appendix A for an overview of the functions supported by each of the PowerAlert software packages.

This User Guide covers the features and functions of the Office package.

## 1.1 System Requirements

- Personal computer with a supported operating system: Windows 8 or 10; Windows Server 2012, 2016 or 2019
- CPU: 4 core 2.0 GHz or higher
- Memory: Minimum of 4 GB
- Available disk space: Minimum of 300 MB
- Ethernet network that supports the TCP/IP protocol
- Supported web browser: Google Chrome, Mozilla Firefox, Edge, Internet Explorer 10 or later, Safari

Download the latest version of PowerAlert software from the Tripp Lite website at [tripplite.com/products/management-software](http://tripplite.com/products/management-software)

For detailed instructions on installing PowerAlert software, refer to the PowerAlert Office/Home/Medical Installation Guide.

Note that the three PowerAlert packages are mutually exclusive--only one can be installed at a given time. An existing installation of PowerAlert software must be uninstalled before a different package can be installed.

## 2. Initial Configuration

For instructions on installing PowerAlert software, refer to the PowerAlert Installation Guide. Once installed and launched, PowerAlert software will automatically attempt to detect a connected UPS system. If the UPS system is not detected, refer to the **Scan for Device** function in Device Maintenance (Top Menu).

### 2.1 SNMP Configuration

PowerAlert software 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 device. The MIB files can be downloaded directly from the PowerAlert software interface; see Section 3, Figure 3-44.

**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

## 2. Initial Configuration

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. PowerAlert Office

### 3.1 Accessing the System Tray

The PowerAlert System Tray App provides a quick-reference graphical summary of UPS status. To launch the app, go to the computer's Start Menu, scroll down to the Tripp Lite folder, and click "PowerAlert System Tray App" (Figure 3-1) .

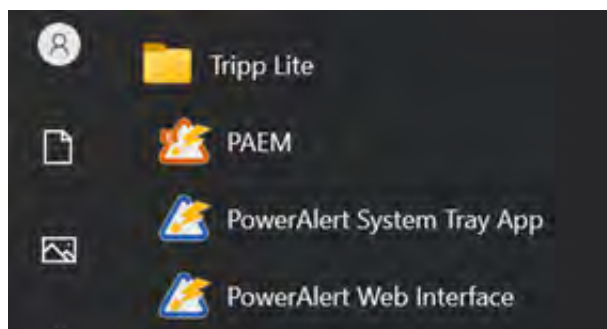


Figure 3-1: Start Menu / Tripp Lite Folder

Open the computer's system tray, then click the PowerAlert icon to generate a graphic showing the status of the UPS (Figure 3.2).

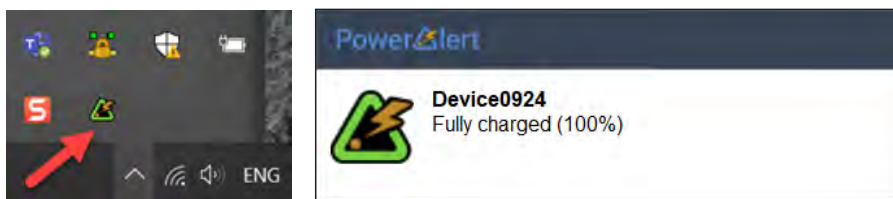


Figure 3-2: System Tray Icon and UPS Status Graphic

During installation of the PowerAlert software, a PowerAlert Web Interface icon is added to the computer's desktop. To access the interface, double-click the icon. Alternatively, the interface can be accessed from the Tripp Lite folder in the Start menu (Figure 3-3).

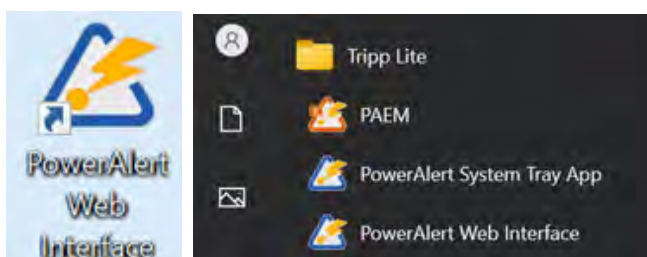


Figure 3-3: Web Interface Desktop Icon and Start Menu item

### 3. PowerAlert Office

The default Administrator Username and Password are both **localadmin**. Note that on initial login, you will be required to change the password. Double-click the PowerAlert Web Interface icon to open the login page of the PowerAlert Office interface (Figure 3-4).

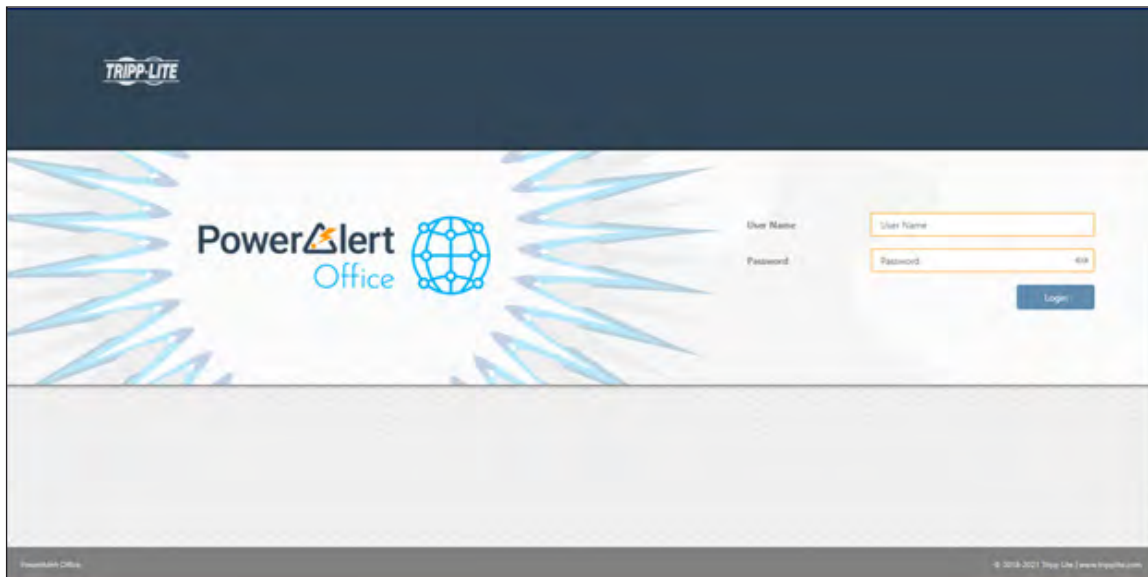


Figure 3-4: PowerAlert Office Login Page

#### Remote Access

To access PowerAlert software remotely, open a supported web browser. In the address bar, enter the IP address of the server on which PowerAlert is installed, followed by the configured port, e.g. <http://192.168.1.1:8080> (Figure 3-5).

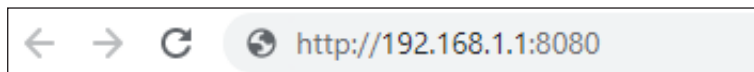


Figure 3-5: Accessing PowerAlert from a Web Browser

On logging in, the Dashboard page is displayed (Figure 3-6).



Figure 3-6: Dashboard Page

## 3. PowerAlert Office

### 3.2 PowerAlert Overview

#### PowerAlert Layout

The PowerAlert Office web interface is comprised of three main sections (Figure 3-7):

- 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

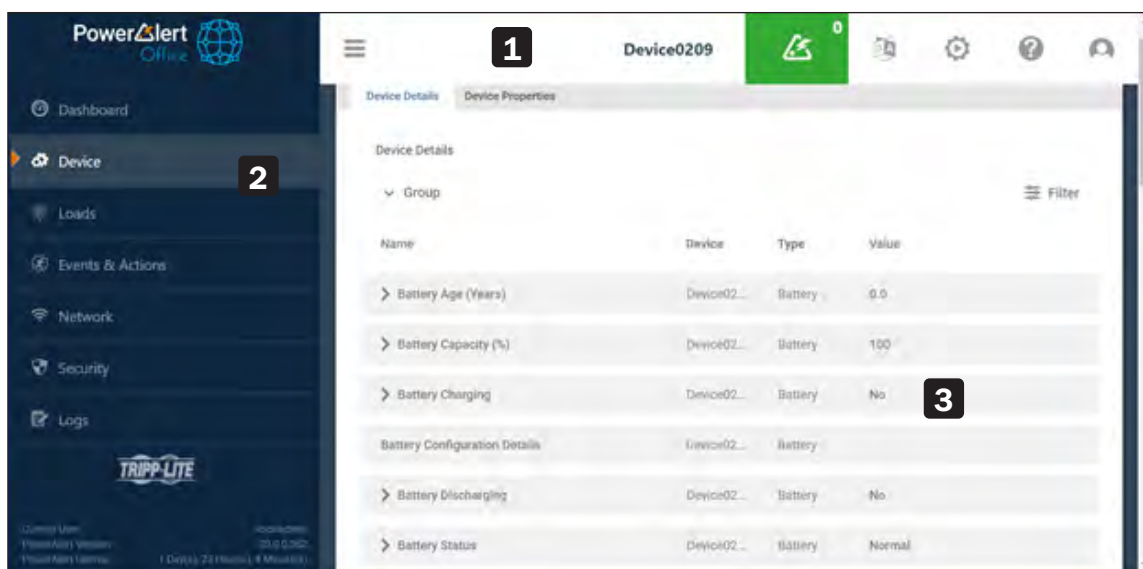


Figure 3-7: PowerAlert Interface Main Sections

## 3. PowerAlert Office

### 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 3-8). Click the menu item again to contract the sub-menu.

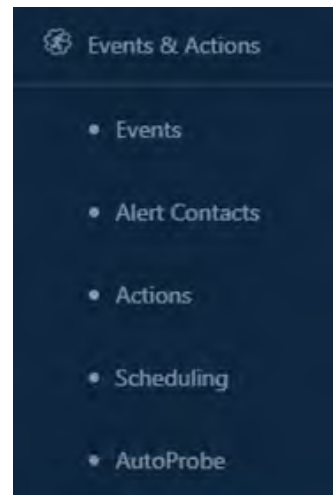


Figure 3-8: Sub-Menus

**Tabs** – Tabs are used to organize information of a common topic into logical groupings (Figure 3-9). Select a tab to view its content.

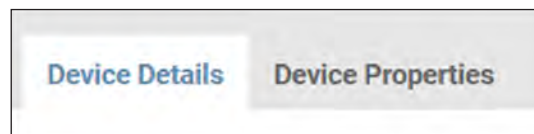






Figure 3-9: Tabs

**Pages** – Sequenced numbers with arrows indicate that the content exceeds one page (Figure 3-10). Select each to navigate pages as follows:



Figure 3-10: Pages

- |   |                                      |
|---|--------------------------------------|
|  | Go to the first pages of the content |
|  | Go to the previous page number       |
| <b>Number</b>   | Go directly to the selected page     |
|  | Go to the next page                  |
|  | Go to the last page of the content   |

**Scroll Bars** – In cases where content exceeds the size of the window, vertical and/or horizontal scroll bars appear (Figure 3-11).

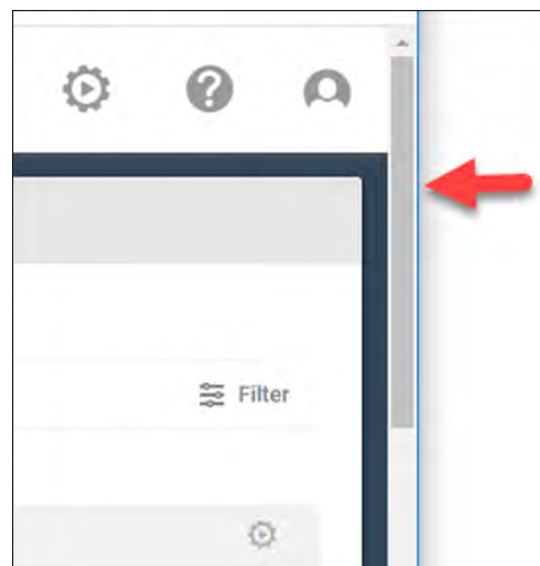


Figure 3-11: Scroll bars



### 3. PowerAlert Office

**Chevrons** – Click the chevron next to an item to expand or contract the content of the item (Figure 3-12).

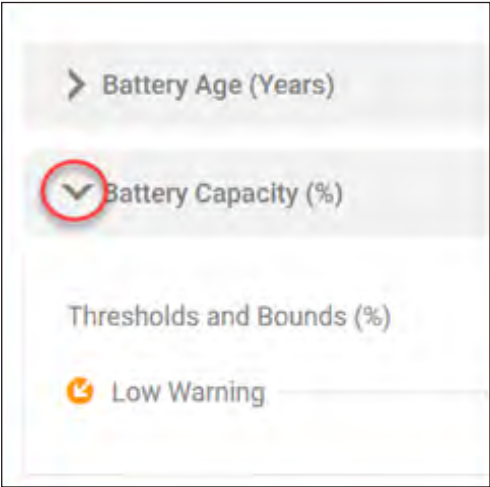


Figure 3-12: Chevrons

### Adjusting Views

**Sorting** – When content is displayed in table format, the information can be sorted in the following manners (Figure 3-13):

- **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 3-13: 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. Click the **Clear Filters** button to restore the default view (Figure 3-14).

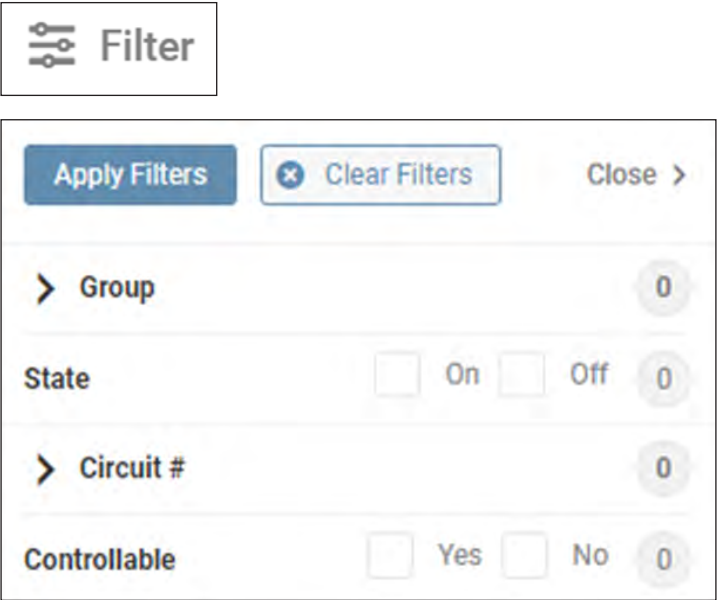


Figure 3-14: Filter functions

### 3. PowerAlert Office

**Columns** – Click **Columns** (in Loads) to open a menu of applicable column titles (Figure 3-15). Select or unselect the preferred column titles, then click anywhere on the screen.

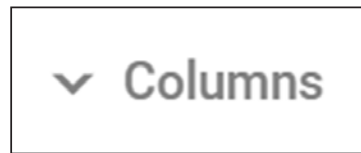
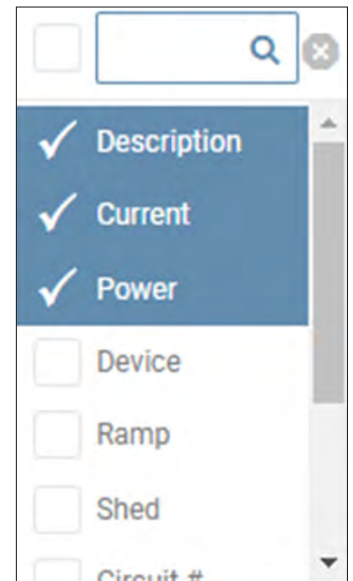


Figure 3-15: Columns



**View** – Click **View** (in Data Log) to open a menu of variables (Figure 3-16). Select or unselect the preferred variables, then click the Save button.



Figure 3-16: View



**Refresh** – Click **Refresh** to update the displayed content (Figure 3-17).

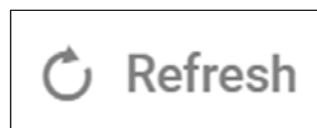


Figure 3-17: Refresh

**Export** – Click **Export** to configure and generate an export of the contents (Figure 3-18).

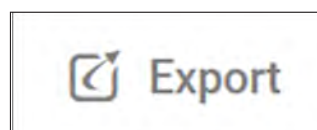


Figure 3-18: Export

## 3. PowerAlert Office

### Icons

**Pencil** – The pencil icon indicates that the item can be edited (Figure 3-19). Click the icon to open a dialog box in which the edits can be made.



Figure 3-19: Edit

**Details** – The 'i' icon indicates that the item contains details (Figure 3-20). Click or mouse over the icon to view the details.




Figure 3-20: Details

**Control** – The gear icon indicates that a control can be executed (Figure 3-21). Mouse over the icon to view a description of the control. Click the icon to execute the action.



Figure 3-21. Control

**Delete** – The  icon indicates the item can be deleted (Figure 3-22). Click the icon to mark the item for deletion; the action will change the icon color to red. To complete the deletion, click the confirmation Delete button (also in red).

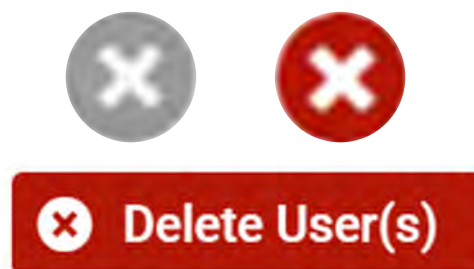


Figure 3-22: Delete icon and Delete (confirmation) Button.

**Sliders** – Sliders allow the state of the item to be manually changed. Colors and symbols reflect the condition or state of the item. Figure 3-23 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 3-23: Slider States and Colors

### 3. PowerAlert Office

**Tags** – Colored shape tags indicate the severity of Events and Alerts (Figure 3-24):

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

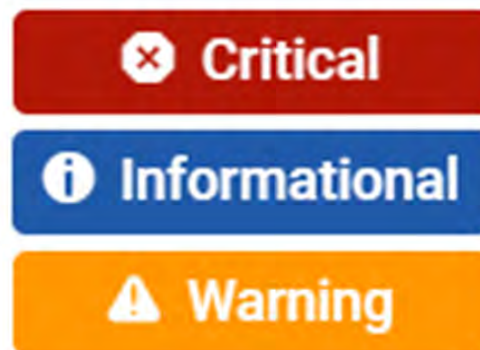


Figure 3-24: Tags

**Checkmark** – Used in the Alert summary, a blue Checkmark indicates that an item has been cleared or acknowledged (Figure 3-25).



Figure 3-25: Checkmark

#### 3.3 Top Menu

The Top Menu is used for viewing Alerts and performing administrative functions (Figure 3-26).



Figure 3-26: Top menu

## 3. PowerAlert Office

### Device

The device name appears to the left of the colored Alert icon. To edit the device name, refer to the Device > Device Properties section of this document. If the computer detects two connected UPSs, the name will become interactive. Click the name to display a pulldown menu containing the device name of each connected UPS. By selecting a device from this menu, the content of the Web Interface will update to reflect the selection (Figure 3-27). In the event that a previously connected device was disconnected, it may appear as (Inactive) in the Device name field. To remove it, go to the Device menu item, Device Properties tab, and click the delete icon (Figure 3-28).



Figure 3-27: Device Selection

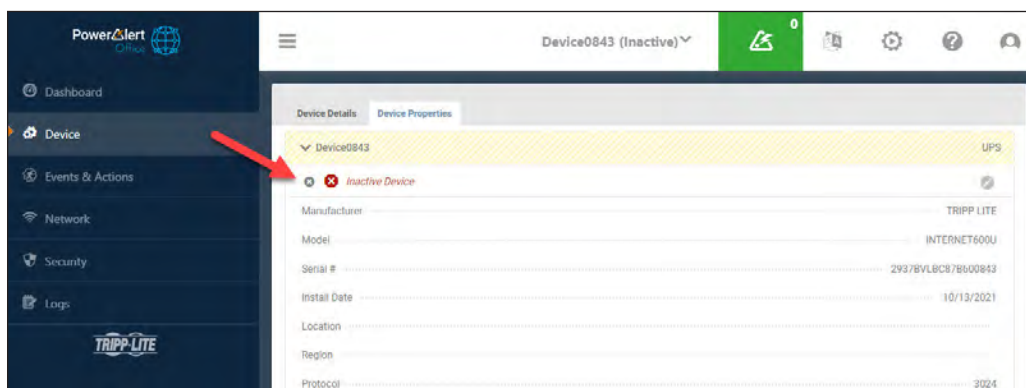


Figure 3-28: Inactive Device

### Alerts

The Alerts icon is located to the right of device name (Figure 3-29). 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 3-26). 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.

**Note:** If two UPS systems are connected, the Alerts for both devices will be displayed at all times.

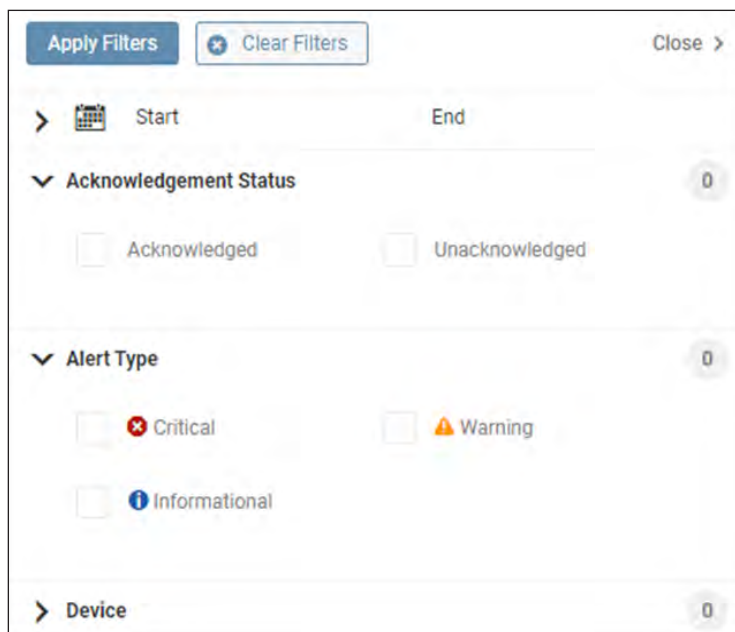
A screenshot of the Alerts screen in the PowerAlert Office web interface. The screen shows a table of alerts with columns: Ack., Cleared, Type, Date/Time, Device, and Event. There are two alerts listed, both with a yellow warning icon and a checkmark in the Ack. column. The alerts are for Device0077, one for 'Load 01 Off' and one for 'Loads Not All On', both dated 8/26/2020 4:41:25 PM. The table has a 'Save' button at the bottom right.

Ack.	Cleared	Type	Date/Time	Device	Event
<input checked="" type="checkbox"/>	<input type="checkbox"/>		8/26/2020 4:41:25 PM	Device0077	Load 01 Off
<input checked="" type="checkbox"/>	<input type="checkbox"/>		8/26/2020 4:41:25 PM	Device0077	Loads Not All On

Figure 3-29: Alerts screen

### 3. PowerAlert Office

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 3-30). Click **Close** once all selections have been made.



The Filter dialog box is used to refine the displayed content of the Alert Log. It features a top bar with 'Apply Filters' and 'Clear Filters' buttons, and a 'Close' button with a right arrow. Below the top bar, there are several filter sections, each with a dropdown arrow, a title, and a count of items. The 'Start' and 'End' fields are at the top. The 'Acknowledgement Status' section has two checkboxes: 'Acknowledged' and 'Unacknowledged'. The 'Alert Type' section has three checkboxes: 'Critical' (with a red 'x' icon), 'Warning' (with a yellow triangle icon), and 'Informational' (with a blue 'i' icon). The 'Device' section is at the bottom.

Start	End

**Acknowledgement Status** 0

☐ Acknowledged ☐ Unacknowledged

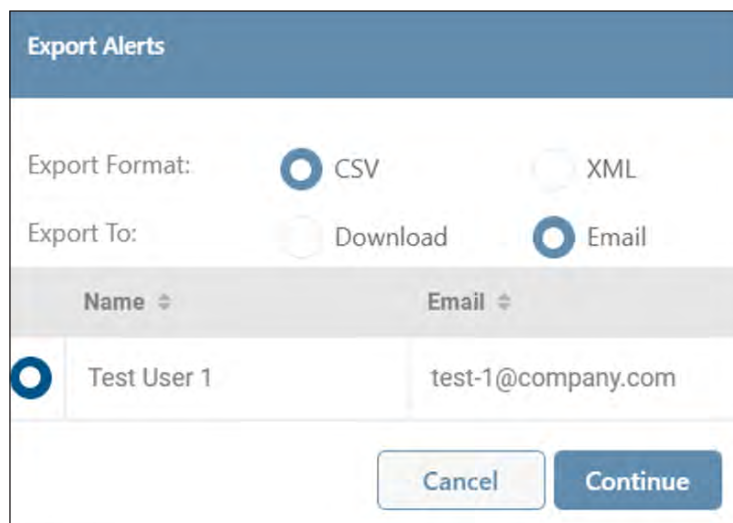
**Alert Type** 0

☐ Critical ☐ Warning ☐ Informational

**Device** 0

Figure 3-30: Filter

Click **Export** to open a window in which the desired file format (CSV or XML) and export destination can be selected (Figure 3-31). 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.



The Export Alerts dialog box is used to select the desired file format and export destination. It features a top bar with the title 'Export Alerts'. Below the top bar, there are two sections: 'Export Format' and 'Export To'. The 'Export Format' section has two radio buttons: 'CSV' (selected) and 'XML'. The 'Export To' section has two radio buttons: 'Download' and 'Email' (selected). Below the 'Export To' section, there is a table of recipients. The table has two columns: 'Name' and 'Email'. The first row shows 'Test User 1' and 'test-1@company.com'. At the bottom of the dialog box, there are two buttons: 'Cancel' and 'Continue'.

**Export Alerts**

Export Format: ☒ CSV ☐ XML

Export To: ☐ Download ☒ Email

Name	Email
<input checked="" type="radio"/> Test User 1	test-1@company.com

Figure 3-31: Alert export options

## 3. PowerAlert Office

### Language

Click the Language icon to select a personal preference for the desired language (Figure 3-32). 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.

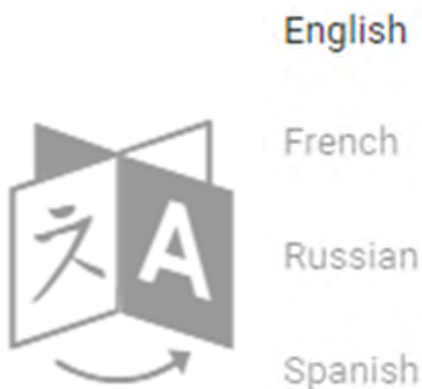


Figure 3-32: Language icon

### Administration

Click the Gear icon to display a sub-menu of Administrative functions supported by the device (Figure 3-33). Note that if 'LED Configuration', 'Restart Device', 'Turn Off Device' or 'Turn On Device' do not appear in the pulldown menu, the device does not support these functions.

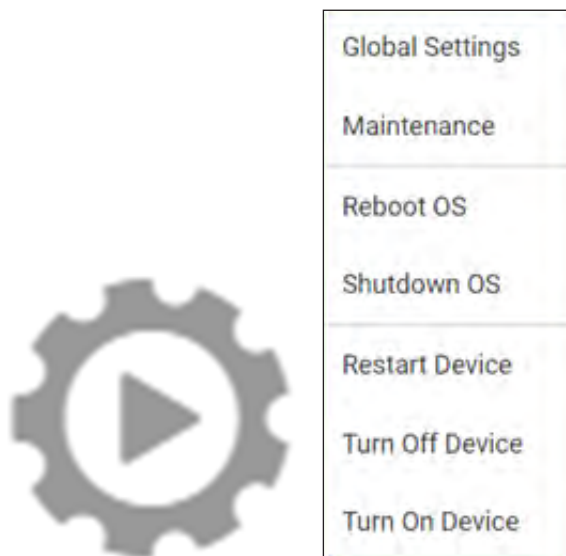
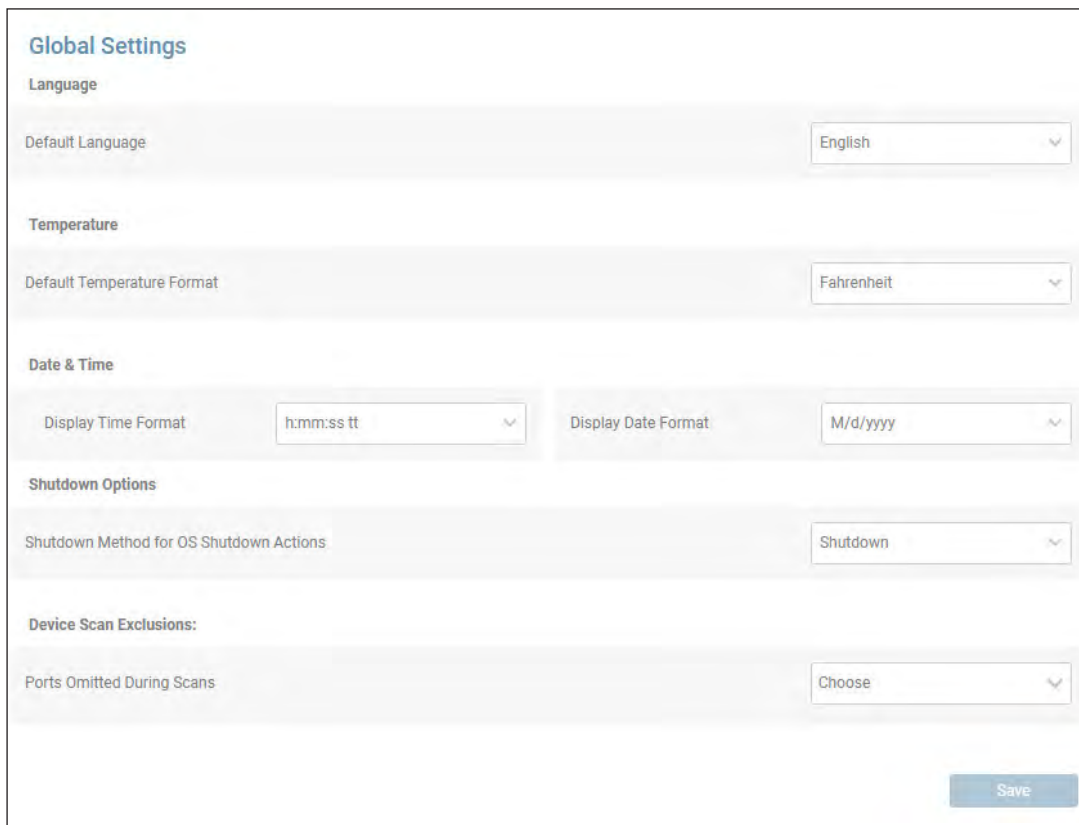


Figure 3-33: Administration Icon and Sub-Menu

## 3. PowerAlert Office

### Global Settings

This option allows for configuration of global settings, including language, temperature, date & time, as well as shutdown option (Figure 3-34). To exclude a computer port from being used during device scans, select and/or enter the port value in the Device Discover Scanning pulldown menu (Figure 3-35). All users accessing the device are subject to these settings. Users have the option of individually overriding the time zone using the **Preferences** function. Once all configuration parameters have been entered, click the **Save** button.




The screenshot shows the 'Global Settings' page with the following sections and controls:

- Language**
  - Default Language: English (dropdown menu)
- Temperature**
  - Default Temperature Format: Fahrenheit (dropdown menu)
- Date & Time**
  - Display Time Format: h:mm:ss tt (dropdown menu)
  - Display Date Format: M/d/yyyy (dropdown menu)
- Shutdown Options**
  - Shutdown Method for OS Shutdown Actions: Shutdown (dropdown menu)
- Device Scan Exclusions:**
  - Ports Omitted During Scans: Choose (dropdown menu)

A 'Save' button is located at the bottom right of the form.

Figure 3-34: Global settings



The screenshot shows the 'Device Scan Exclusions' section with the following controls:

- Device Scan Exclusions:**
  - Ports Omitted During Scans: Choose (dropdown menu)

The dropdown menu is open, showing a checkbox next to 'COM3'.

Figure 3-35: Device Scan Exclusions



### 3. PowerAlert Office

#### Maintenance

This option allows for execution of maintenance functions – software update and backup management (Figure 3-36).

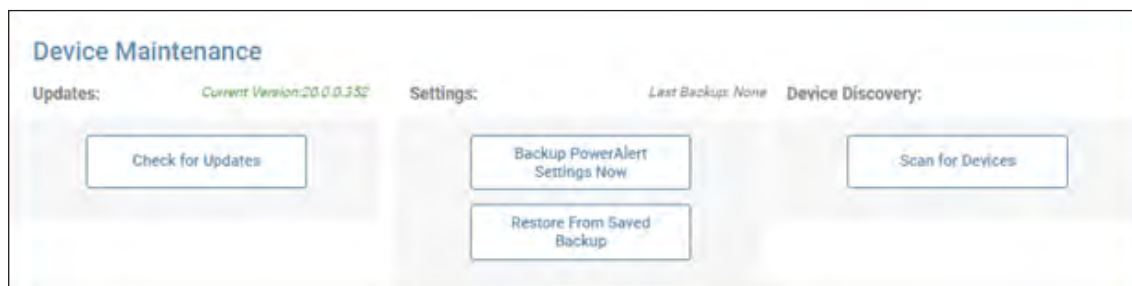


Figure 3-36: Maintenance

Click the **Check for Updates** button to confirm availability of a PowerAlert Office update at the Tripp Lite website (Figure 3-37).

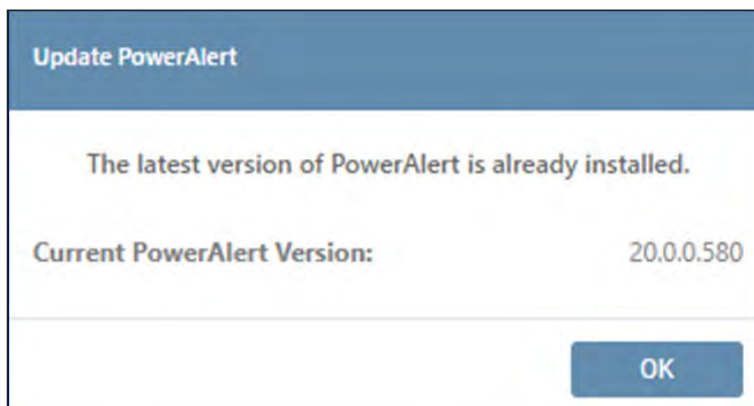


Figure 3-37: Check for Updates

### 3. PowerAlert Office

Click the **Backup PowerAlert Settings Now** button, followed by the **Continue Backup** button to store the configuration on (Figure 3-38). On completing the backup, click the **Download** button to optionally save the configuration to the local environment (Figure 3-38).

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. “PowerAlert\_backup\_07\_31\_2021.bck”.

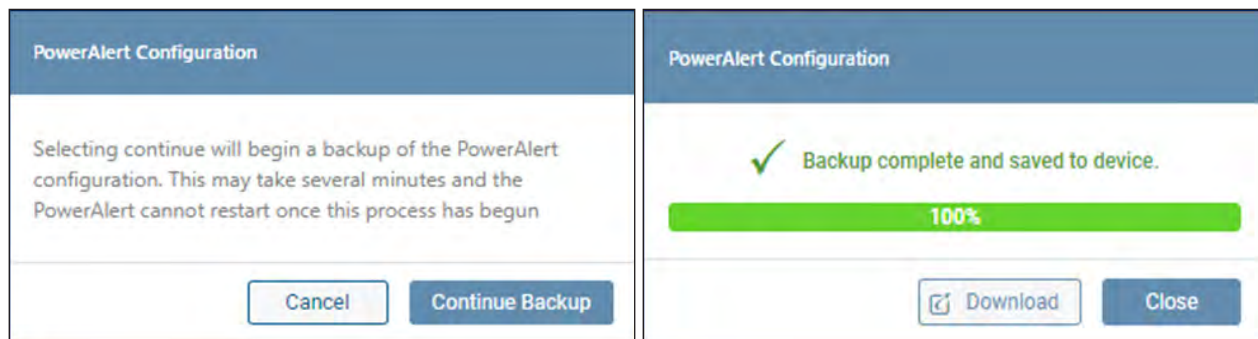


Figure 3-38: Performing a PowerAlert Configuration Backup

Click the **Restore from Saved Backup** button to upload a configuration file (Figure 3-39). If a previous Backup 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).

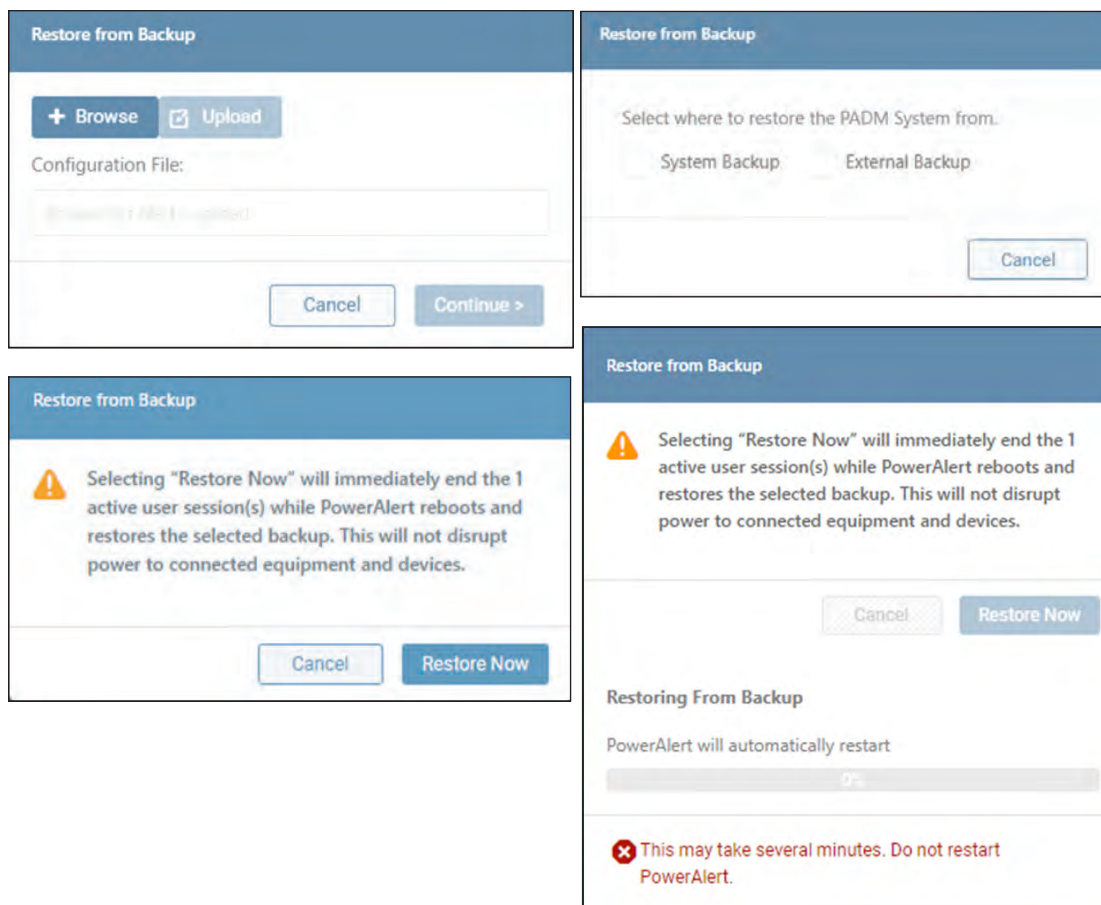


Figure 3-39: Restoring from Backup

### 3. PowerAlert Office

**Scan for Devices** - This item scans the host computer's ports for connection to Tripp Lite devices. In certain cases, PowerAlert may fail to establish or maintain contact with a device; for example, if the USB connection to the computer is removed then re-inserted. Click the **Scan for Devices** button, followed by the **Scan Now** button to execute the scan (Figure 3-40).

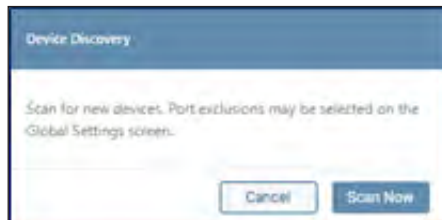


Figure 3-40: Scan for Devices

#### Reboot OS

This item performs a reboot of the host computer's Operating System. Press the **Reboot Now** button to execute the action (Figure 3-41).

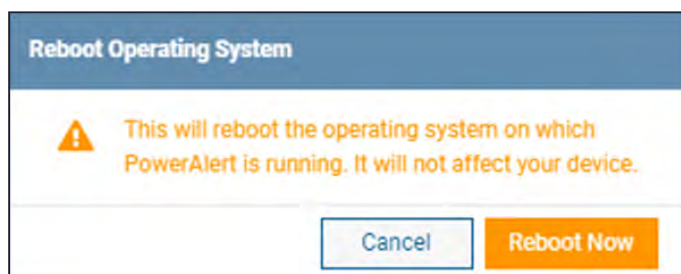


Figure 3-41: Reboot Operating System

#### Shutdown OS

This item performs a shutdown of the host computer's Operating System. Press the **Shutdown Now** button to execute the action (Figure 3-42).

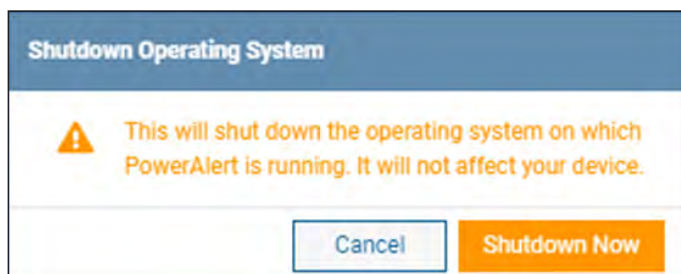


Figure 3-42: Shutdown Operating System

### 3. PowerAlert Office

**Restart Device** – Click the “Shutdown Operating System” checkbox in order to gracefully shut down the OS prior to shutting down the device. Optionally, specify a Shutdown OS Delay Time. On clicking the **Restart** button, the OS Delay will begin counting down. On completion of the OS Shutdown, the device Shutdown Delay will begin counting down, after which the device will restart (Figure 3-43).

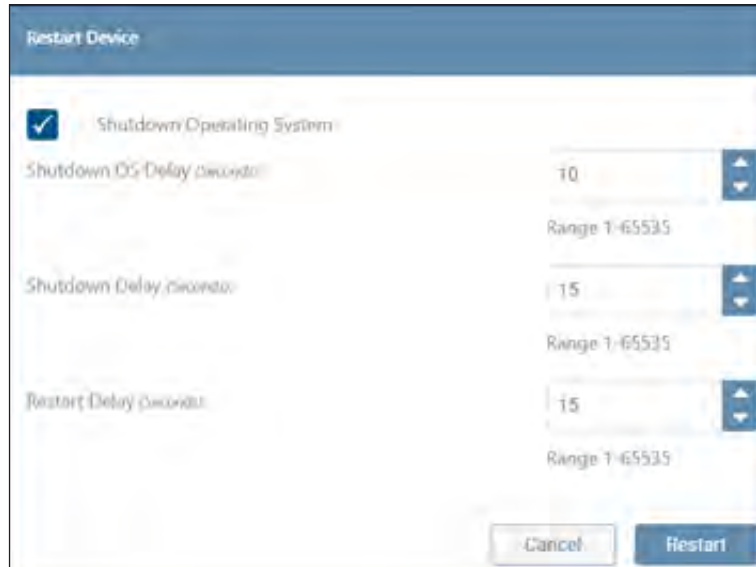


Figure 3-43: Restart device

**LED Configuration** – For UPS systems that support controllable LED Banks (e.g. SMART1000PSGLCD), the LED Configuration menu item provides an interface for setting the Brightness, Illumination Effect, Color and Speed of the front and bottom LED banks (Figure 3-44). For details on use of this utility, refer to the LED Configurator User Guide which can be downloaded from the Tripp Lite website.

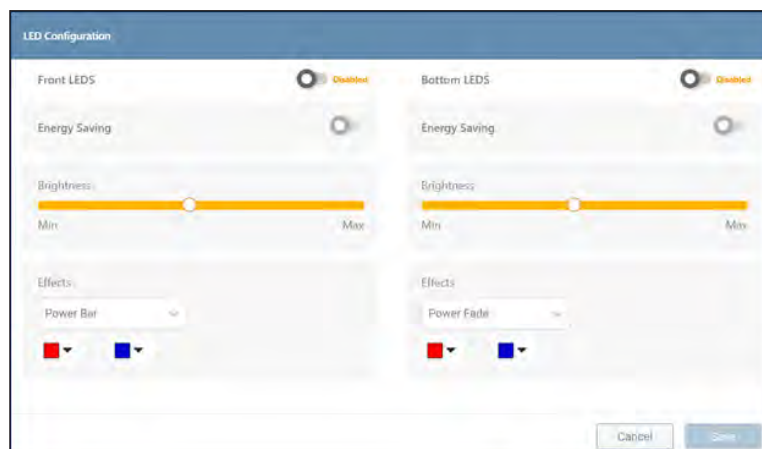
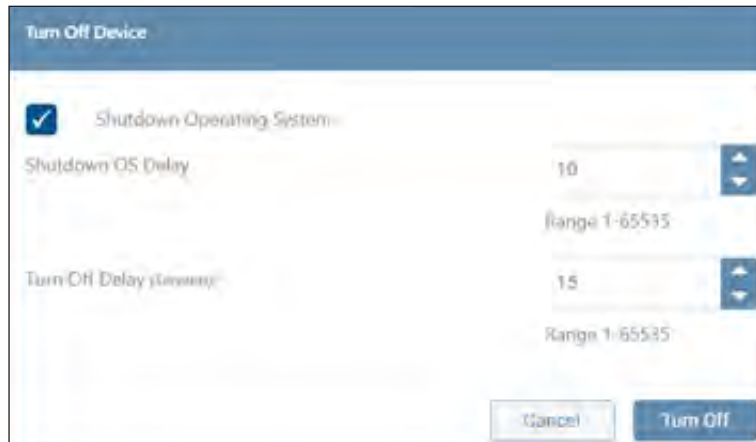


Figure 3-44: LED Configuration

### 3. PowerAlert Office

**Turn Off Device** – Click the “Shutdown Operating System” checkbox in order to gracefully shut down the OS prior to shutting down the device. Optionally, specify a Shutdown OS Delay Time. On clicking the **Turn Off** button, the OS Delay will begin counting down. On completion of the OS Shutdown, the device Turn Off Delay will begin counting down (Figure 3-45) after which the device will be turned off.



Turn Off Device

☒ Shutdown Operating System

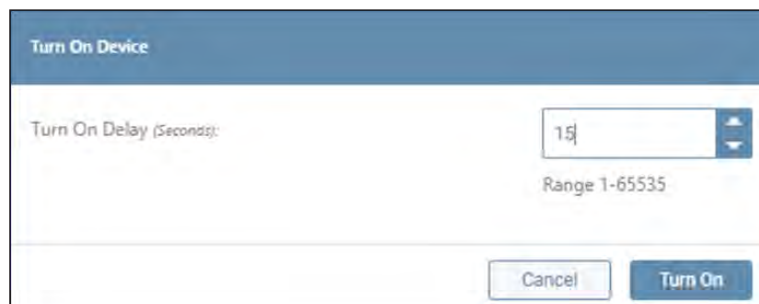
Shutdown OS Delay: 10  
Range 1-65535

Turn Off Delay (Seconds): 15  
Range 1-65535

Cancel Turn Off

Figure 3-45: Turn Off Device

**Turn On Device** – This item turns on the device after the specified delay (Figure 3-46).



Turn On Device

Turn On Delay (Seconds): 15  
Range 1-65535

Cancel Turn On

Figure 3-46: Turn On device

### 3. PowerAlert Office

#### Support

Click the Question icon to display a sub-menu of Support items (Figure 3-47). 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".

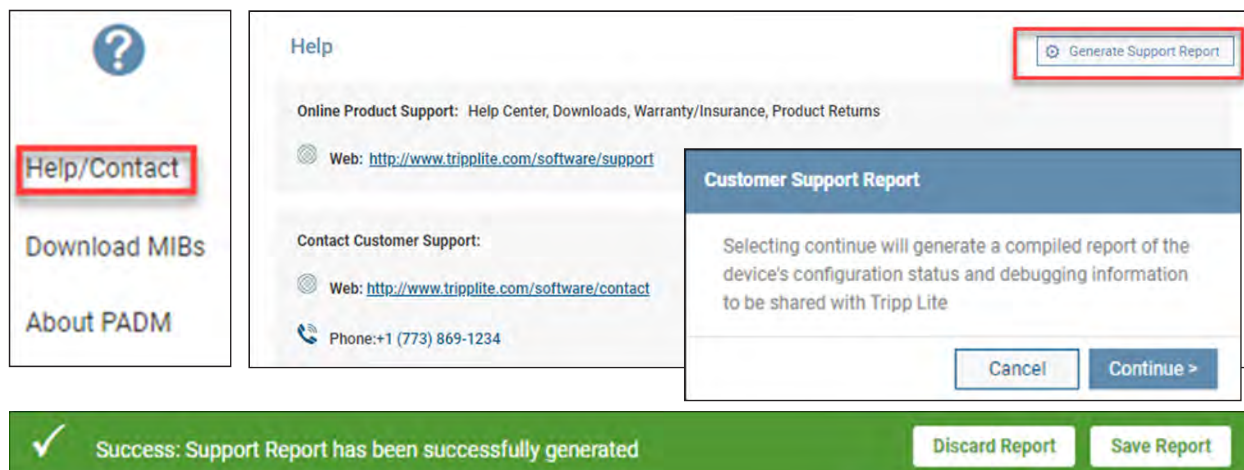


Figure 3-47: Help/Contact

### 3. PowerAlert Office

Click **Download MIBs** to automatically download the Tripp Lite MIB package to the computer's Downloads folder. Click **About PowerAlert** to display information related to the PowerAlert software (Figure 3-48).

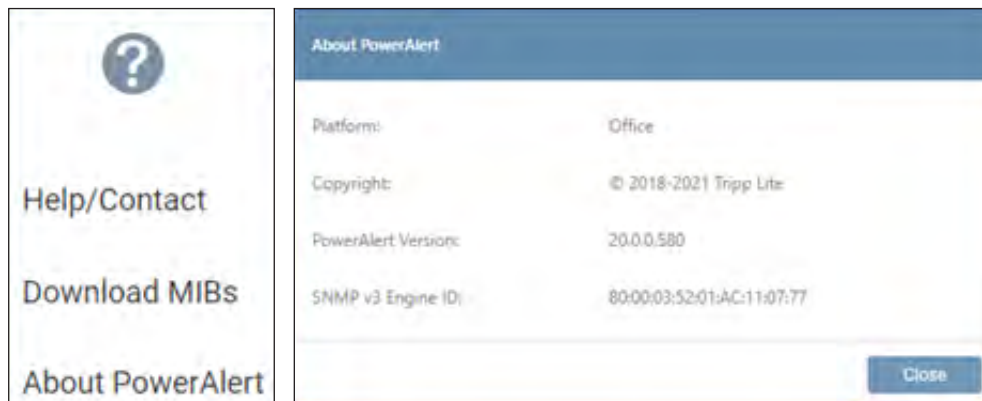


Figure 3-48: Download MIBs and About PowerAlert

#### 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 the 'eye' icon to view the plain text password entered. Click **Log Out** to terminate the current session (Figure 3-49).

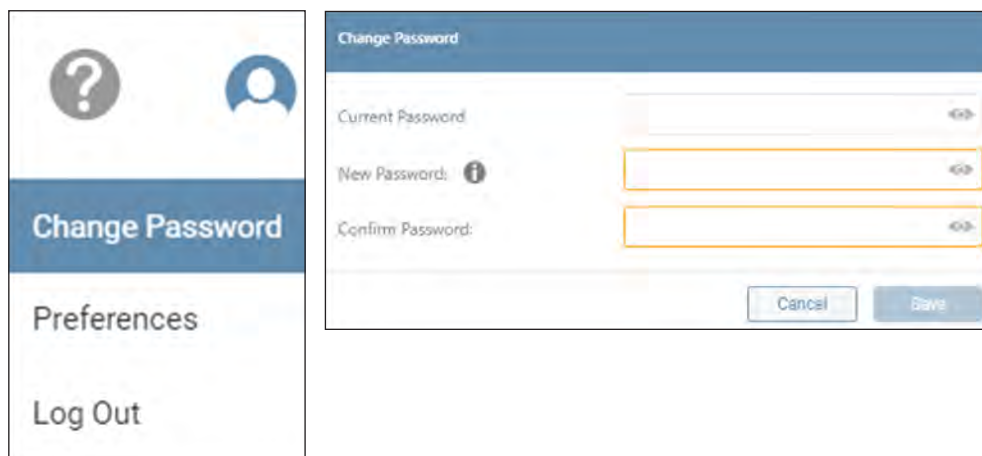


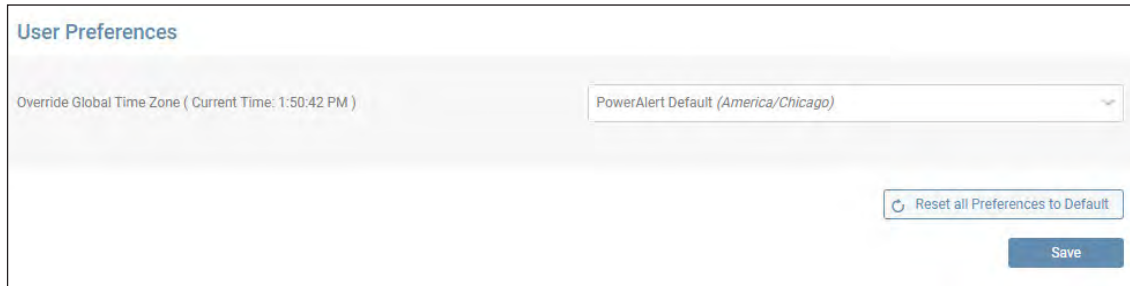
Figure 3-49: User Menu, Change Password and Logout

### 3. PowerAlert Office

Click **Preferences** to override the global settings for Time Zone (Figure 3-50).

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 Main Menu > Security.



The screenshot shows a 'User Preferences' window. At the top left, the title 'User Preferences' is displayed. Below it, there is a section for 'Override Global Time Zone ( Current Time: 1:50:42 PM )'. To the right of this text is a dropdown menu currently showing 'PowerAlert Default (America/Chicago)'. In the bottom right corner of the window, there are two buttons: 'Reset all Preferences to Default' and 'Save'.

Figure 3-50: 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.

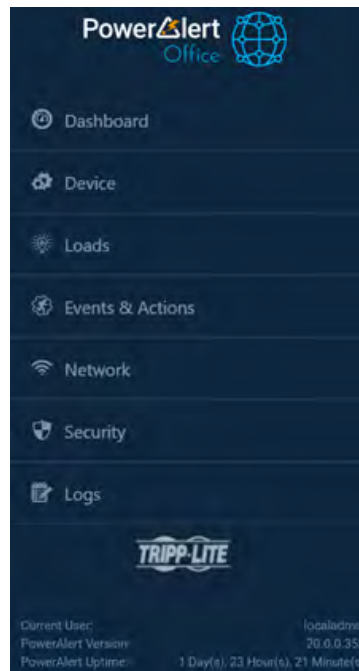


Figure 4-1: Main Menu

### 4.1 Dashboard

The Dashboard menu item displays a graphical summary of the device's operational status 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). To clear all selections, click **Clear Gauges**. Certain gauges are interactive – if the cursor changes when moving over the gauge, click 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.

The figure displays the 'Gauges' configuration interface. On the left is a dark sidebar with 'Add Graph' and 'Gauges' (selected). The main area shows a 'Device0209' section with four gauge options: 'Runtime Remaining (Minutes)', 'Battery Voltage (V)', 'Battery Age (Years)', and 'Battery Capacity (%)'. The 'Battery Capacity (%)' gauge is selected with a blue checkmark. Below this is a 'Thresholds and Bounds' table with columns for Name, Min (), Value (), and Max ().

Name	Min ()	Value ()	Max ()
Low Critical	0	51	44
High Critical	6	45	100
Alert Tolerance (margin before retriggering an event)			0

At the bottom right of the table are three buttons: 'Cancel', 'Apply Changes', and 'Save & Close'.

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 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).

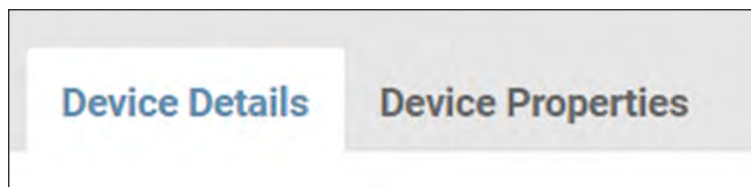


Figure 4-5: Device Details and Device Properties

# 4. Main Menu

## Device Details

This tab displays the metrics of the device and all connected peripherals (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.

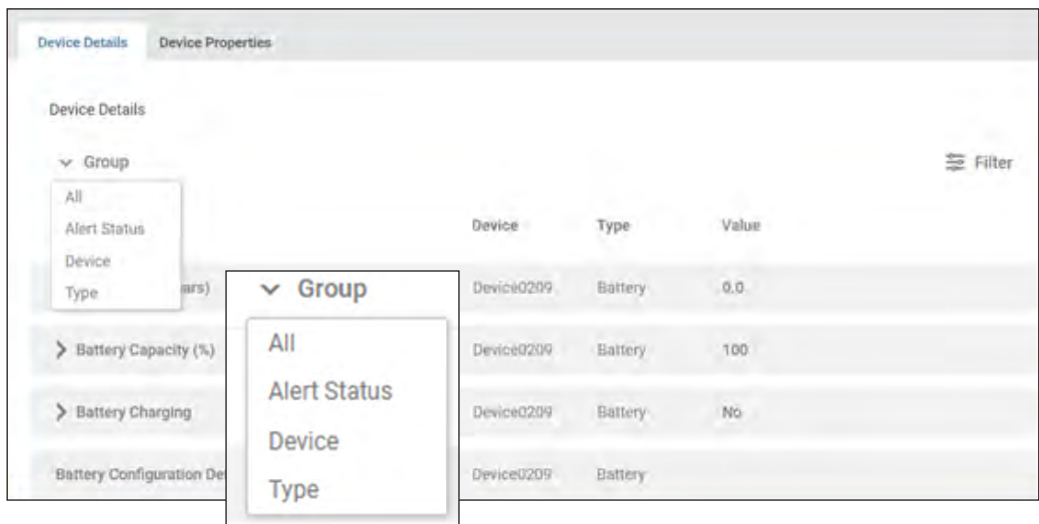
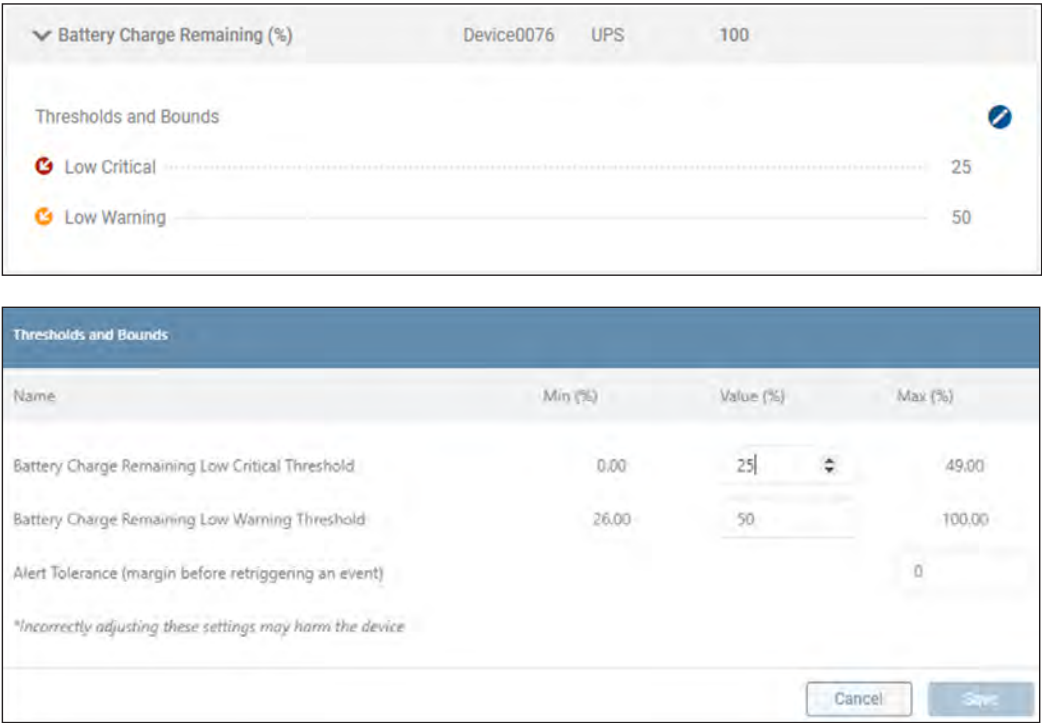


Figure 4-6: Device Details

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%.



## 4. Main Menu

### Device Properties

This tab displays information related to the identity of the device and all connected peripherals (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.

The screenshot shows the 'Device Properties' tab for 'Device0209'. At the top, there's a status bar with 'Device0209' and 'UPS'. Below it, a green message states 'There are currently no alerts for this device.' with a pencil icon. The main section lists device details: Manufacturer (TRIPP LITE), Model (SMART1500RM2U), Serial # (2911EY0SM820600209), Install Date (7/8/2021), Location, Region, and Protocol (3015).

Property	Value
Manufacturer	TRIPP LITE
Model	SMART1500RM2U
Serial #	2911EY0SM820600209
Install Date	7/8/2021
Location	
Region	
Protocol	3015

The 'Set Device Property' dialog box allows editing device information. It includes fields for Name (Device0209), Install Date (7/8/2021), Location, Region, Manufacturer (TRIPP LITE), Device ID (34567), and Asset Tag. 'Cancel' and 'Save' buttons are at the bottom.

Property	Value
Name	Device0209
Install Date	7/8/2021
Location	
Region	
Manufacturer	TRIPP LITE
Device ID	34567
Asset Tag	

Figure 4-8: Displaying and Editing Device Properties

# 4. Main Menu

## 4.3 Loads

The Loads menu item will appear only for devices that support loads (Figure 4-9). It is comprised of three tabs: Loads Overview, Loads Ramp/Shed and Load Groups.

**Note:** PowerAlert Office will display only the tabs that the device supports.

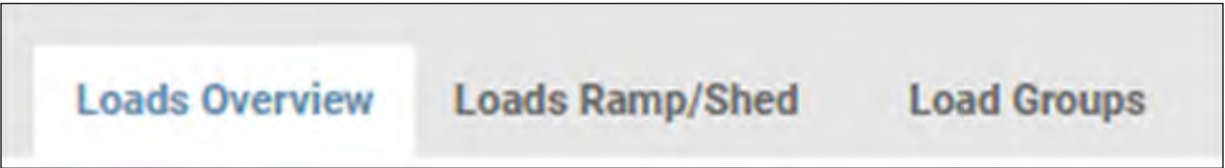


Figure 4-9: Loads Tabs

### Loads Overview

This tab displays a summary of the device’s loads, including status and outlet-level metrics, if applicable (Figure 4-10). 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.

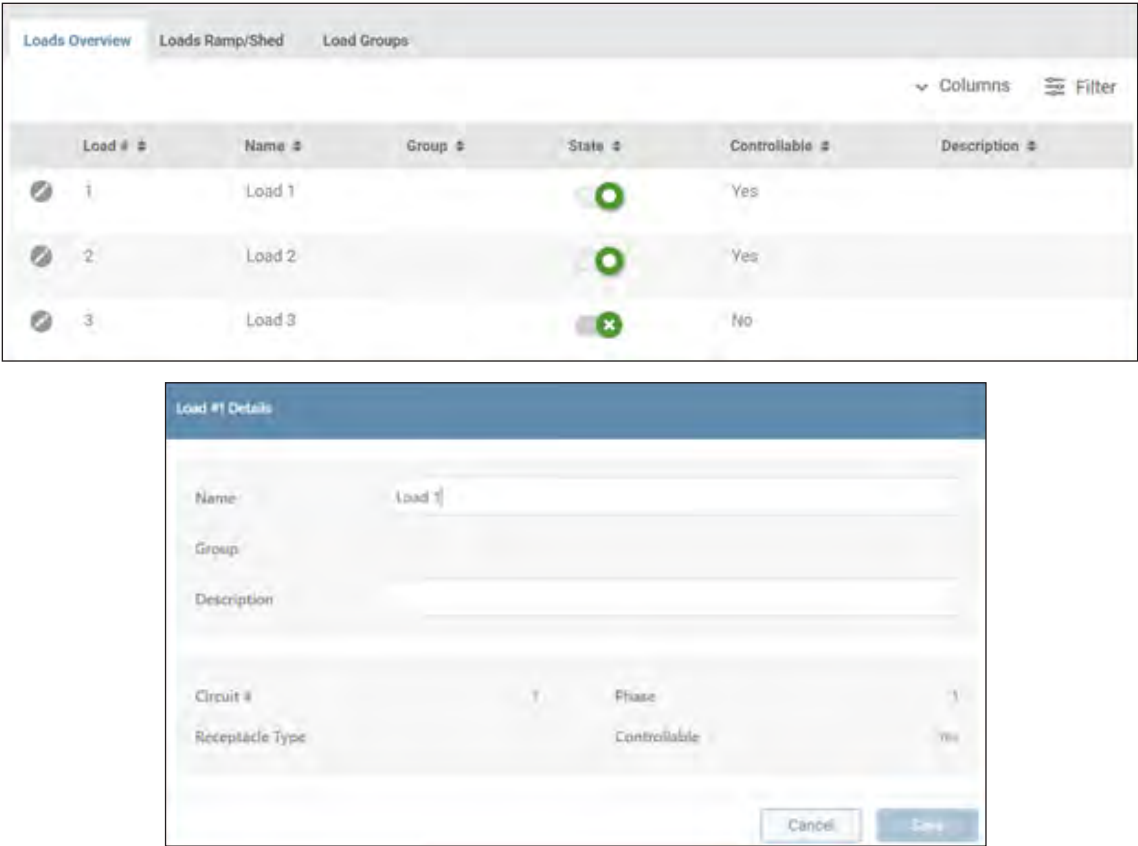


Figure 4-10: Loads Overview Tab and Editing Load Details

## 4. Main Menu

### Loads Ramp/Shed

Loads Ramp/Shed is supported only by UPS systems with two or more controllable loads. This tab displays a summary of Ramp and Shed settings across all Loads (Figure 4-11). 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.

Load #	Name	Group	Description	Ramp	Ramp Delay	Shed	Shed Delay
1	Load 1			<input checked="" type="checkbox"/>	0	<input checked="" type="checkbox"/>	0
2	Load 2			<input checked="" type="checkbox"/>	0	<input checked="" type="checkbox"/>	0
3	Load 3			<input checked="" type="checkbox"/>	0	<input checked="" type="checkbox"/>	0

☒ 0

☐ 0

☒ 3

☐ 0

Figure 4-11: Load Ramp/Shed

### Load Groups

Load Groups are supported only by UPS systems with two or more controllable loads. This tab displays a summary of configured Load Groups (Figure 4-12). 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 4-13). 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 4-13).

Status	Name	State	Description	# of Loads
<input checked="" type="checkbox"/> Enabled	Group A	<input checked="" type="checkbox"/>	Servers 1 - 3	3

Figure 4-12: Load Ramp/Shed

# 4. Main Menu

Load Group

Enabled

Name

Group A

Description

All Loads

All Loads


Unassociated

	Load #	Name	Group	Description	Receptacle T
<input type="checkbox"/>	1	Load 1			Unknown
<input type="checkbox"/>	2	Load 2			Unknown

Cancel

Save


Figure 4-13: Adding and Editing a Load Group


To delete one or more Load Groups, click the  icon to the left of each line item (Figure 4-14). On doing so, the **Delete Load Group(s)** button becomes active (turns red); click the button to complete the deletion.

Loads Overview

Loads Ramp/Shed

Load Groups

 Delete Load Group(s)

 Add Load Group




 Status	Name	State	Description	# of Loads
 Enabled	Group A			2

Figure 4-14: 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 4-15). Click the pencil icon to the right of the line item to edit the item. In the window that appears, click 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						
<div>Import a Battery Configuration File</div> <div>DeleteAdd</div>						
Battery Status		floating		Runtime Remaining:	455	Capacity:
Seconds on Battery:		0		Voltage:	269.0 V	100
	Name	External	Smart	Model	Installed On	Replace On
	Internal-1	No	No	12v9	6/24/2020	6/24/2020

### Battery

Name:

Internal-1

Installed On:

11/11/2020

Replace On:

11/11/2023

Battery Age High Warning Threshold (Years)

Min 0.0

Value

3.0

Max 4.9

Battery Age High Critical Threshold (Years)

Min 3.1

Value

5.0


Max 5.0

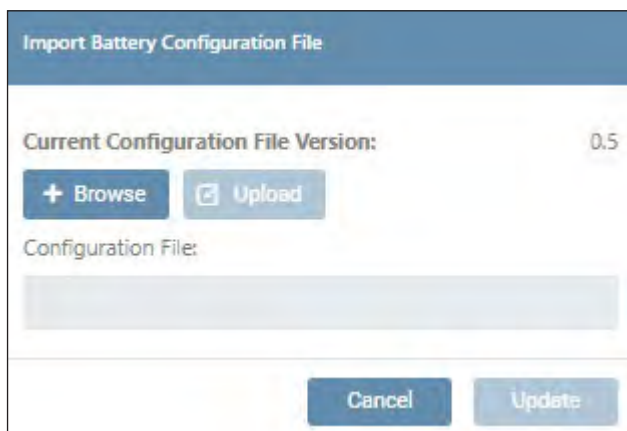
Cancel

Save

Figure 4-15: 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), PowerAlert Office 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 PowerAlert Office (Figure 4-16). 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  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.



The dialog box is titled "Import Battery Configuration File". It shows the "Current Configuration File Version" as 0.5. There are two buttons: "+ Browse" and "Upload". Below these is a text input field labeled "Configuration File:". At the bottom are "Cancel" and "Update" buttons.



The dialog box is titled "Add Battery". It shows the "Current Device" as Device0080. It indicates "Current number of internal batteries = 3" and "Current number of external batteries = 1". Instructions state: "Select one or more battery packs and their associated quantities from the pulldown below. You may then press 'Next' to have the usage calculations performed and saved to the unit." There is a table with two rows, each showing a quantity of 1 and a battery model BP36V14-2U. To the right is a dropdown menu showing a list of battery models: BP36V13, BP36V14-2U (highlighted), BP36V15-2U, BP36V27, and BP36V27-2US. There are "+Add" and "Apply" buttons.

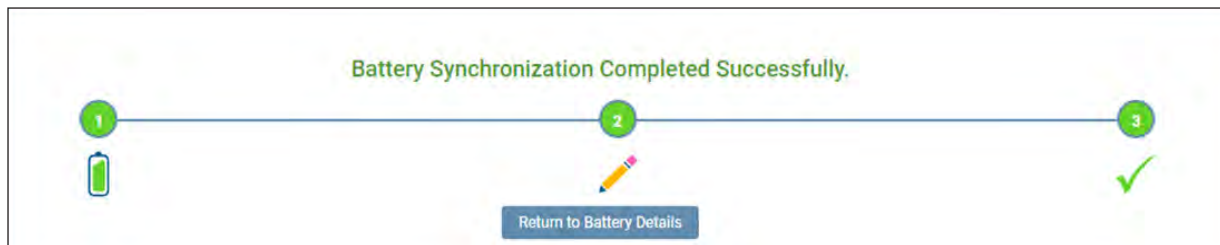



Figure 4-16: Adding an EBP and Configuring the Battery Profile

## 4. Main Menu

Once the process is complete, the newly added EBPs will appear in the summary list (Figure 4-17). 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, PowerAlert Office 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 PowerAlert Office does not need to be used.

- With smart internal batteries and up to six external smart battery packs installed, the UPS calculates the runtime. The embedded EBP utility should not be used.
- With smart internal batteries and more than six external smart battery packs installed, the embedded EBP utility should be used to calculate runtime. Note that PowerAlert Office (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 should be used to calculate runtime.







Batteries						
<div> Delete  Add</div>						
Status:	Normal		Charge Remaining:	100 %		Capacity:
Seconds on Battery:	0		Runtime Remaining:	516		0
Minutes Remaining:	0		Voltage:	41 V		
 Name	External	Smart	Manufacturer	Model#	Installed On	Replace On
Internal-1	No				2/5/2023	2/5/2020
 External-1-2	Yes				2/12/2020	2/11/2023

Figure 4-17: 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 4-18). To enable Auto-Acknowledgement and Logging for all events, select the appropriate check boxes at the top of the Events list.

Events									
Sort		All:	<input checked="" type="checkbox"/> Auto Acknowledge	<input checked="" type="checkbox"/> Logging	Filter				
>	Overload		Device	Value	Device2251	Critical	✓ Acknowledge	✓ Log	
>	Communications Lost		Device	Value	Device2251	Informational	✓ Acknowledge	✓ Log	
>	On Battery		Device	Value	Device2251	Warning	✓ Acknowledge	✓ Log	
>	Battery Low		Device	Value	Device2251	Critical	✓ Acknowledge	✓ Log	
>	Battery Self Test Failed		Device	Value	Device2251	Warning	✓ Acknowledge	✓ Log	
>	Output Off		Device	Value	Device2251	Critical	✓ Acknowledge	✓ Log	
>	Battery Bad		Device	Value	Device2251	Critical	✓ Acknowledge	✓ Log	


Figure 4-18: 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 4-19). 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		Enabled	
Label/Name:	Overload	Severity	Critical
Clear Event Name:	Load Okay	Auto Acknowledge	<input checked="" type="checkbox"/>
		Log	<input checked="" type="checkbox"/>
		Cancel	Save

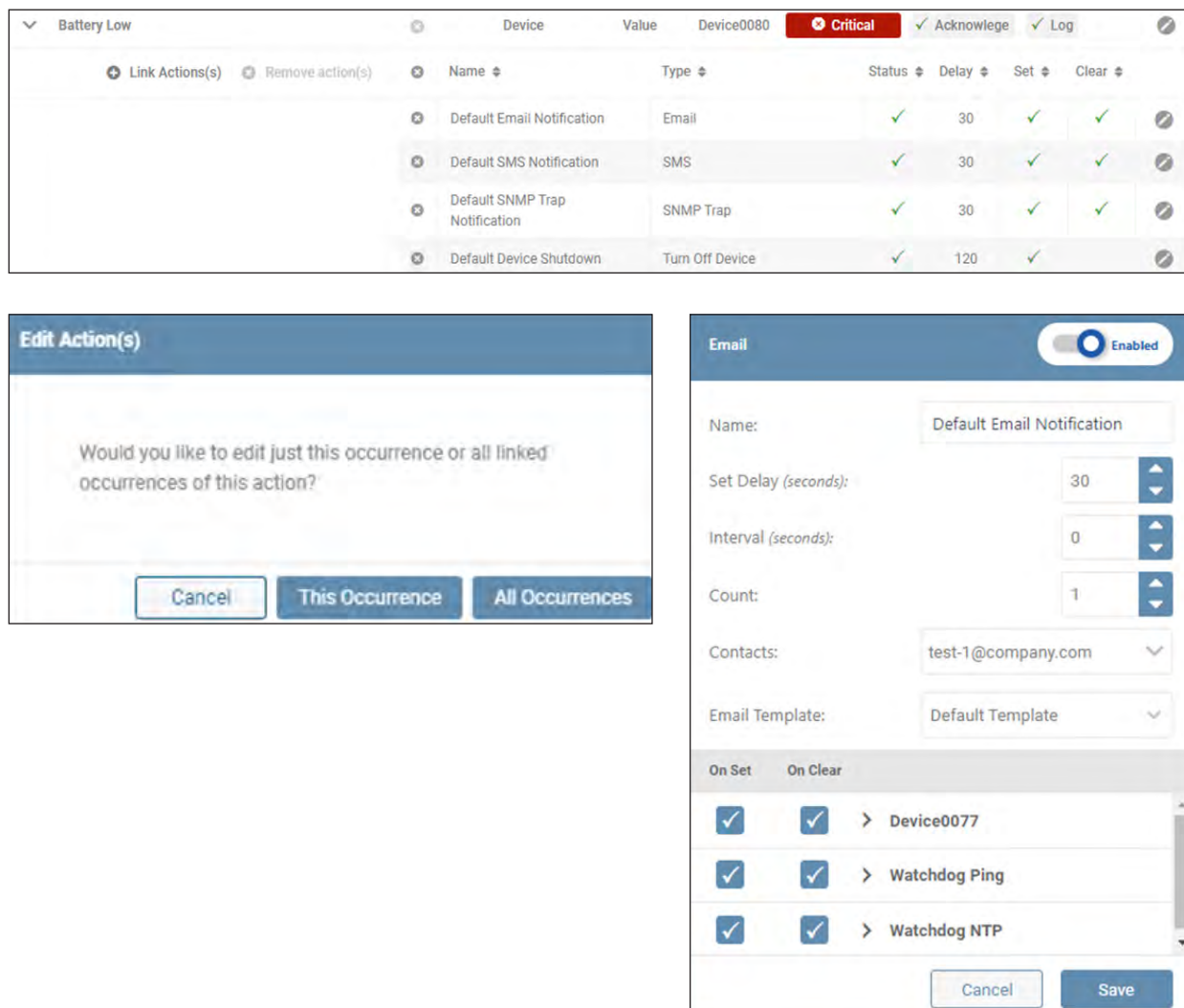
Figure 4-19: Editing an Event

## 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 4-20). 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.



The screenshot displays the 'Battery Low' event configuration interface. At the top, there's a header bar with 'Battery Low' on the left, a close icon, and several status indicators: 'Device', 'Value', 'Device0080', 'Critical' (in a red box), 'Acknowledge', and 'Log'. Below this is a table of actions. The table has columns for 'Name', 'Type', 'Status', 'Delay', 'Set', and 'Clear'. There are also buttons for 'Link Actions(s)' and 'Remove action(s)'. The actions listed are 'Default Email Notification' (Email, 30s delay), 'Default SMS Notification' (SMS, 30s delay), 'Default SNMP Trap Notification' (SNMP Trap, 30s delay), and 'Default Device Shutdown' (Turn Off Device, 120s delay). Each row has a pencil icon for editing and an 'X' icon for removal.

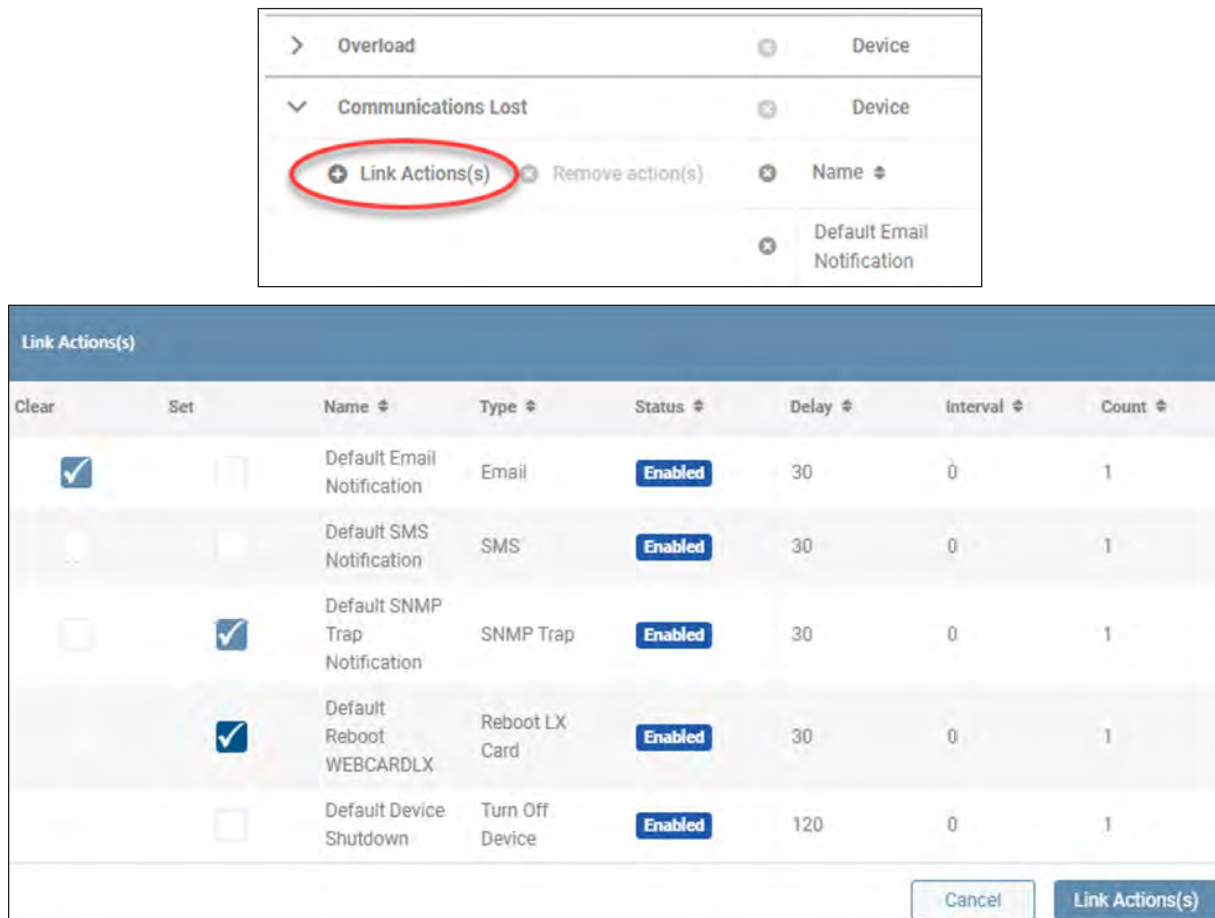
Below the table, there are two modal windows. The first is titled 'Edit Action(s)' and asks: 'Would you like to edit just this occurrence or all linked occurrences of this action?'. It has three buttons: 'Cancel', 'This Occurrence', and 'All Occurrences'. The second modal is titled 'Email' and is for editing the 'Default Email Notification' action. It has a toggle switch for 'Enabled'. The fields include: 'Name' (Default Email Notification), 'Set Delay (seconds)' (30), 'Interval (seconds)' (0), 'Count' (1), 'Contacts' (test-1@company.com), and 'Email Template' (Default Template). At the bottom, there's a section for 'On Set' and 'On Clear' actions, each with checkboxes and a list of actions: 'Device0077', 'Watchdog Ping', and 'Watchdog NTP'. The 'Save' button is at the bottom right.

Name	Type	Status	Delay	Set	Clear
Default Email Notification	Email	✓	30	✓	✓
Default SMS Notification	SMS	✓	30	✓	✓
Default SNMP Trap Notification	SNMP Trap	✓	30	✓	✓
Default Device Shutdown	Turn Off Device	✓	120	✓	

Figure 4-20: Editing Event Actions

## 4. Main Menu

Click **Link Action(s)** to select which Actions are to be triggered by the Event (Figure 4-21). 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.



The screenshot shows a configuration window for linking actions to an event. The event is 'Overload' on a 'Device'. The 'Link Actions(s)' button is highlighted with a red circle. Below the dialog is a table showing the linked actions.

Clear	Set	Name	Type	Status	Delay	Interval	Count
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Default Email Notification	Email	Enabled	30	0	1
<input type="checkbox"/>	<input type="checkbox"/>	Default SMS Notification	SMS	Enabled	30	0	1
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Default SNMP Trap Notification	SNMP Trap	Enabled	30	0	1
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Default Reboot WEBCARDLX	Reboot LX Card	Enabled	30	0	1
<input type="checkbox"/>	<input type="checkbox"/>	Default Device Shutdown	Turn Off Device	Enabled	120	0	1

Buttons: Cancel, Link Actions(s)

Figure 4-21: 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 4-22).

Alert Contacts						
			Delete Contact(s)		Add an Alert Contact	
Status	Label/Name	Contact Details	Type	Trap Port	Set Port	
Enabled	John Doe	johndoe@company.com	Email	n/a	n/a	
Enabled	SNMPuser1	192.168.10.10	SNMPv1	162	161	
Enabled	SNMPalert2	192.168.22.22	SNMPv2c	162	161	
Enabled	Jane Doe	1-888-123-4567	SMS	n/a	n/a	

Figure 4-22: 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 4-23. 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 two screenshots of the 'Add an Alert Contact' dialog box. The left screenshot shows the 'Email Alert Contact' dialog with fields for Label/Name (John Doe), Email (johndoe@company.com), and a 'Send Test' button. The right screenshot shows the 'SNMPv1 Alert Contact' dialog with fields for Label/Name (SNMPuser1), Host (192.168.10.10), Community (\*\*\*\*\*), Enable Trap (checked), Trap Type (Trap), Port (162), and a 'Test Trap' button. Both dialogs have 'Cancel' and 'Save' buttons at the bottom.


Figure 4-23: Adding an Alert Contact – SNMPv1 and Email Examples

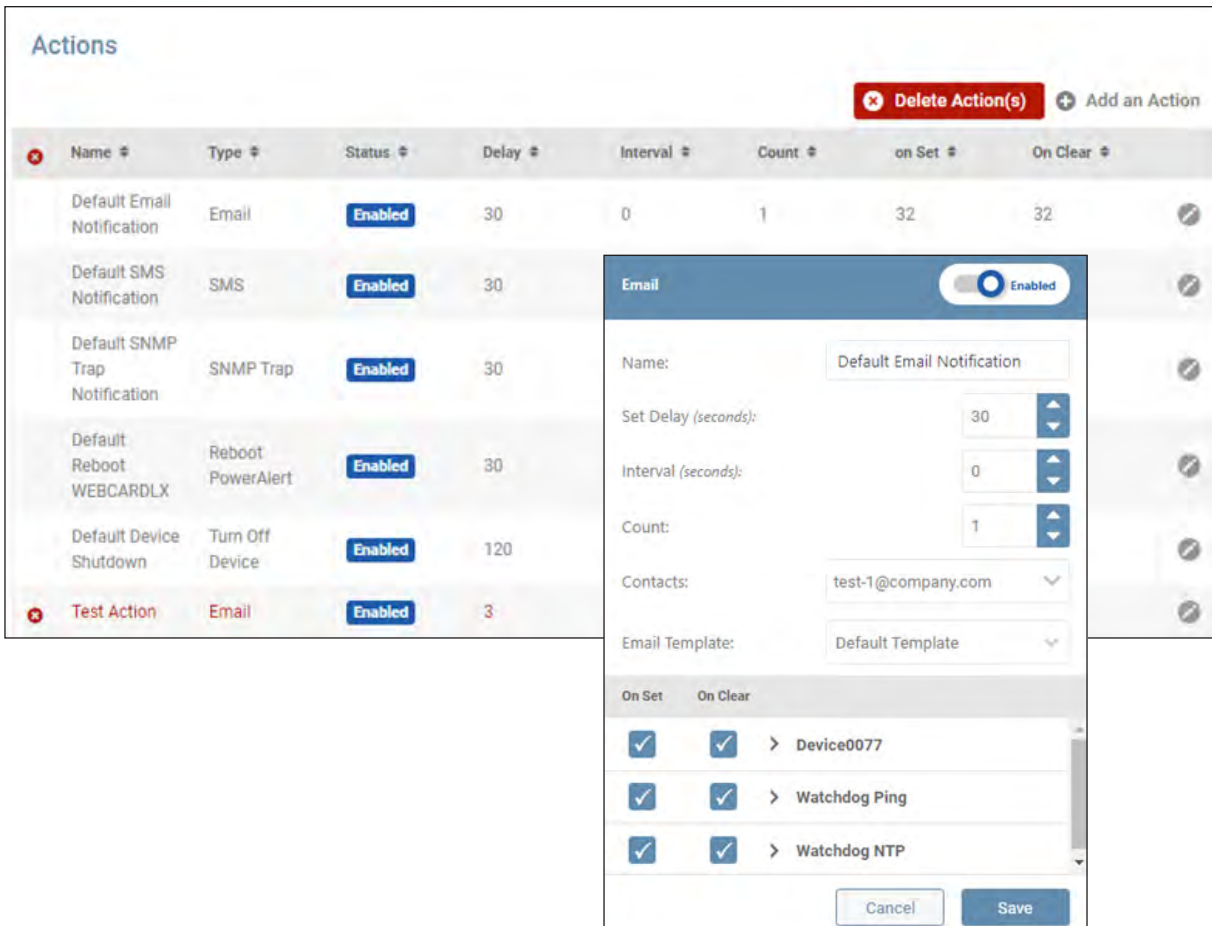
To edit a contact, click the pencil icon to the right of an entry. Once all edits have been completed, click the **Save** button. To delete one or more contact, click the **✕** icon to the left of each line item. On doing so, the **Delete Contact(s)** button becomes active (turns red); click the button 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 4-24). 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.



The screenshot displays the 'Actions' management interface. At the top, there is a red 'Delete Action(s)' button and a green 'Add an Action' button. Below is a table with columns: Name, Type, Status, Delay, Interval, Count, On Set, and On Clear. The table lists several default actions, all of which are 'Enabled'. A 'Test Action' is also listed at the bottom. To the right of the table, a configuration modal for the 'Default Email Notification' action is open. This modal includes fields for Name, Set Delay (seconds), Interval (seconds), Count, and Contacts. It also features a section for 'On Set' and 'On Clear' events, each with checkboxes and a list of target devices (Device0077, Watchdog Ping, Watchdog NTP). The modal has 'Cancel' and 'Save' buttons at the bottom.

Name	Type	Status	Delay	Interval	Count	On Set	On Clear
Default Email Notification	Email	Enabled	30	0	1	32	32
Default SMS Notification	SMS	Enabled	30				
Default SNMP Trap Notification	SNMP Trap	Enabled	30				
Default Reboot WEBCARDLX	Reboot PowerAlert	Enabled	30				
Default Device Shutdown	Turn Off Device	Enabled	120				
Test Action	Email	Enabled	3				

Figure 4-24: Actions Summary and Editing an Action

To create a new action, click **Add an Action** and select one of the action types (Figure 4-25). 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

To create a new schedule, click Add Schedule and select the action type from the menu (Figure 4-27). 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 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 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 time. Doing so will automatically add a 10- or 20-minute extension to the desired Run-On, depending on how the Scheduled Action is saved.


The figure consists of three screenshots of a mobile application interface for configuring a scheduled action. The title bar for all screens is "Scheduled Action: Initiate Battery Self-Test" with an "Enabled" toggle switch.

- Top Screenshot (Action Tab):** The "Name" field contains "Bi-monthly self-test". Below the tabs, the "Initiate Battery Self-Test" action is selected. The "Target Device" dropdown menu shows "Device0843". At the bottom are "Cancel" and "Next >" buttons.
- Bottom-Left Screenshot (Frequency Tab):** The "Frequency" tab is active. The "Monthly" dropdown is selected. Below it, a radio button is selected for "1 of every 1 Month(s)". Further down, another radio button is selected for "First Sunday" with a dropdown menu showing "Sunday". Below that, "Of Every 2 Month(s)" is displayed. At the bottom are "Cancel", "< Back", and "Next >" buttons.
- Bottom-Right Screenshot (Range Tab):** The "Range" tab is active. The "Run On" field shows a calendar icon and the date/time "9/9/2021 7:55:28 AM". Below it, the "Repeat Forever" radio button is selected. Further down, the "Repeat" radio button is selected with a value of "0" and a "Time(s)" dropdown. At the bottom, the "Repeat Until" radio button is selected with a calendar icon and the date/time "9/9/2021 7:55:28 AM". At the bottom are "Cancel", "< Back", and "Save" buttons.

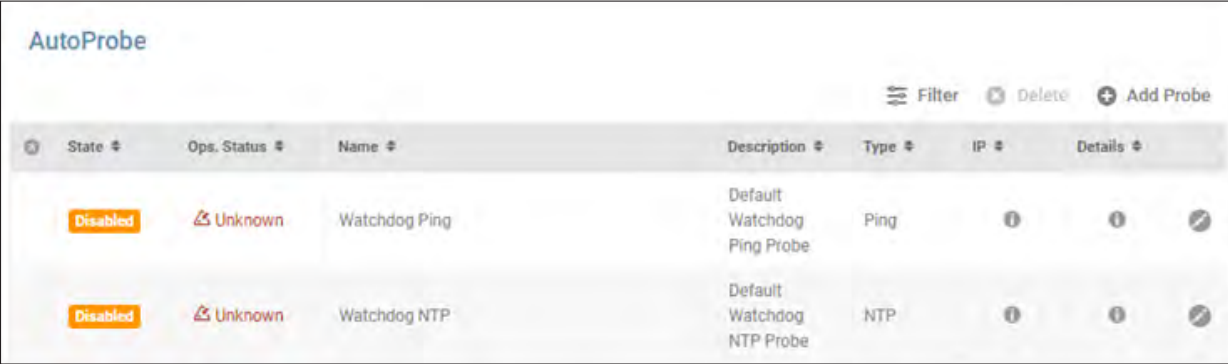
Figure 4-27: Creating a Scheduled Action

## 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 4-28). 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	Ops. 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 4-28: 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 4-29). 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.

The figure shows the process of creating an Auto-Probe. On the left is a vertical menu titled 'Add Probe' with three options: 'Ping Probe', 'NTP Probe', and 'SNMP GET'. The 'SNMP GET' option is selected. To the right are two screenshots of the 'SNMP GET Probe' configuration window. The top screenshot shows the 'Details' tab with fields for 'Label/Name' (test), 'Description' (get model), 'Interval (minutes)' (2), 'Retry (# of Times)' (3), 'Primary Address' (192.168.0.0), 'Port' (162), 'OID' (1.3.6.1.2.1.33.1.1.2.0), 'Secondary Address' (Secondary Address), and 'Port' (161). The bottom screenshot shows the 'Security' tab with fields for 'SNMP Type' (SNMPV3), 'User Name' (adminuser1), 'Privacy Mode' (AuthPriv), 'Auth. Protocol' (MD5), 'Auth. Passphrase' (masked), 'Privacy Protocol' (DES), and 'Privacy Passphrase' (masked). Both screenshots have 'Cancel' and 'Save' buttons at the bottom right.

Figure 4-29: 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 adding a System Contact, as well as Binding IP Addresses (Figure 4-30). In the pulldown menu, use the open field to add individual IP addresses. Use the check boxes to select which addresses are to be subject to the binding.

**Note:** Setting the loopback address (i.e. 127.0.0.1) as the Binding IP Address will lock access to localhost. As a result, PowerAlert Network Shutdown Agent (PANSA) will not be able to discover or communicate with PowerAlert Office. To ensure that PANSA can connect with PowerAlert Office, use a routable (not loopback) Binding IP Address.

Figure 4-30: Internet Settings

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 4-31). To avoid multiple reboots, make all required network configuration changes prior to executing **Apply Now**.

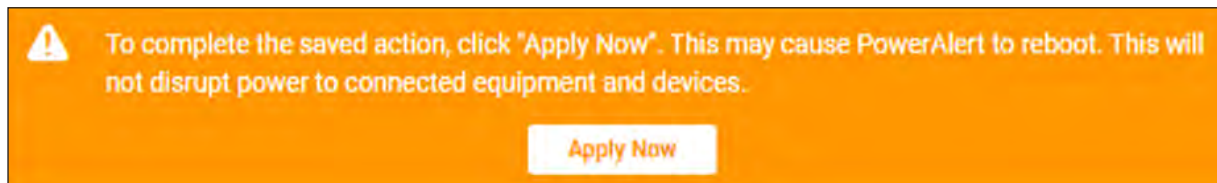


Figure 4-31: “Apply Now” message

## 4. Main Menu

### 4.6.2 Services

This sub-menu allows for configuration of the network services identified below (Figure 4-32). Use the slider to the right of a service to enable/disable it. Click the **Save** button once all edits have been made.

#### SNMP

- SNMPv1, SNMPv2c and SNMPv3 are all enabled, by default.

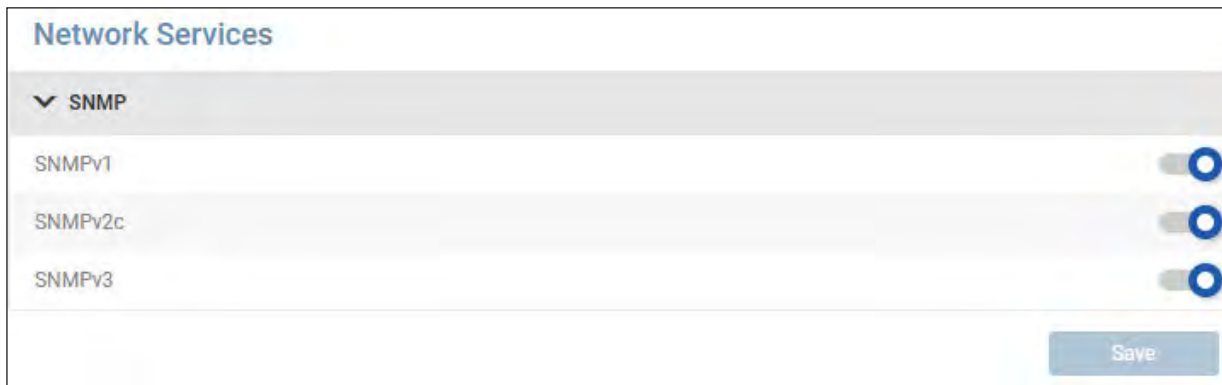


Figure 4-32: Network Services Configuration

### 4.6.3 SMTP

This sub-menu allows for configuration of Simple Mail Transfer Protocol (SMTP) parameters and Email format settings (Figure 4-33). Click the **Save** button once all edits have been made (Figure 4-33).

#### 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

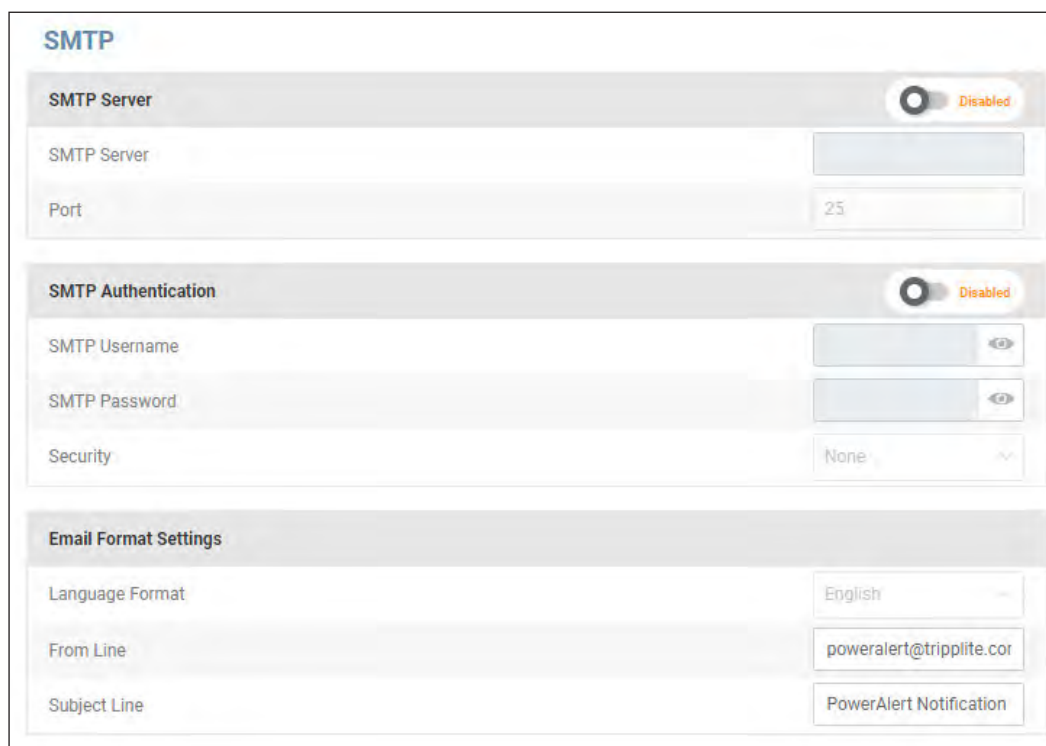
- Move the slider to enable or disable SMTP Authentication; default = disabled.
- If enabled, enter valid values for SMTP User Name and SMTP Password.
- Select the applicable Security Type from the pulldown menu.

### 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.

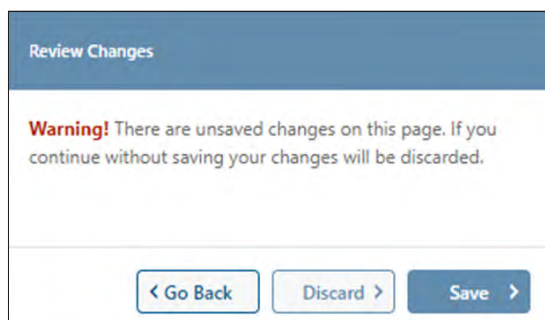
- In the “Subject Line” field, enter the information that will appear in the subject line of notification messages.



The screenshot shows the 'SMTP Configuration' form. It is divided into three main sections: 'SMTP Server', 'SMTP Authentication', and 'Email Format Settings'. The 'SMTP Server' section has a 'Disabled' toggle, an empty 'SMTP Server' text field, and a 'Port' field with the value '25'. The 'SMTP Authentication' section also has a 'Disabled' toggle, 'SMTP Username' and 'SMTP Password' text fields with eye icons, and a 'Security' dropdown menu set to 'None'. The 'Email Format Settings' section includes a 'Language Format' dropdown set to 'English', a 'From Line' text field containing 'poweralert@tripplite.cor', and a 'Subject Line' text field containing 'PowerAlert Notification'.

Figure 4-33: 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 4-34).



The screenshot shows a 'Review Changes' dialog box. It has a blue header with the text 'Review Changes'. Below the header, a warning message is displayed: 'Warning! There are unsaved changes on this page. If you continue without saving your changes will be discarded.' At the bottom of the dialog, there are three buttons: '< Go Back', 'Discard >', and 'Save >'.

Figure 4-34: 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 4-35).



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 for the user 'localadmin'.

Username	Name	Type	Location	Logged On	Session Length
localadmin		WEB	172.18.127.35	1/17/2020 2:55:51 PM	3m
localadmin		CONSOLE	172.18.127.35	1/17/2020 2:58:31 PM	1m

Figure 4-35: Session Management

The system supports the ability to terminate one or more sessions. Click the  icon to the left of each line item (Figure 4-36). On doing so, the **End Session(s)** button becomes active (turns red); click the button to complete the termination.



This screenshot is similar to Figure 4-35, but the 'End Session(s)' button at the top right is now red and contains an 'X' icon. Additionally, the 'X' icon in the first column of the table (next to the second 'localadmin' row) is also red.

Username	Name	Type	Location	Logged On	Session Length
localadmin		WEB	172.18.127.35	1/17/2020 2:55:51 PM	3m
localadmin		CONSOLE	172.18.127.35	1/17/2020 2:58:31 PM	1m

Figure 4-36: 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 (Figure 4-37). Click each tab to view its contents.

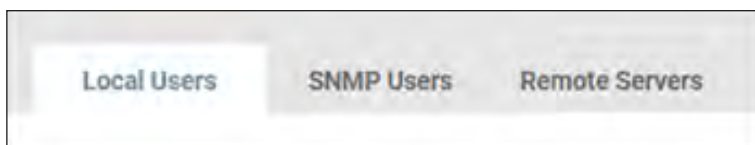


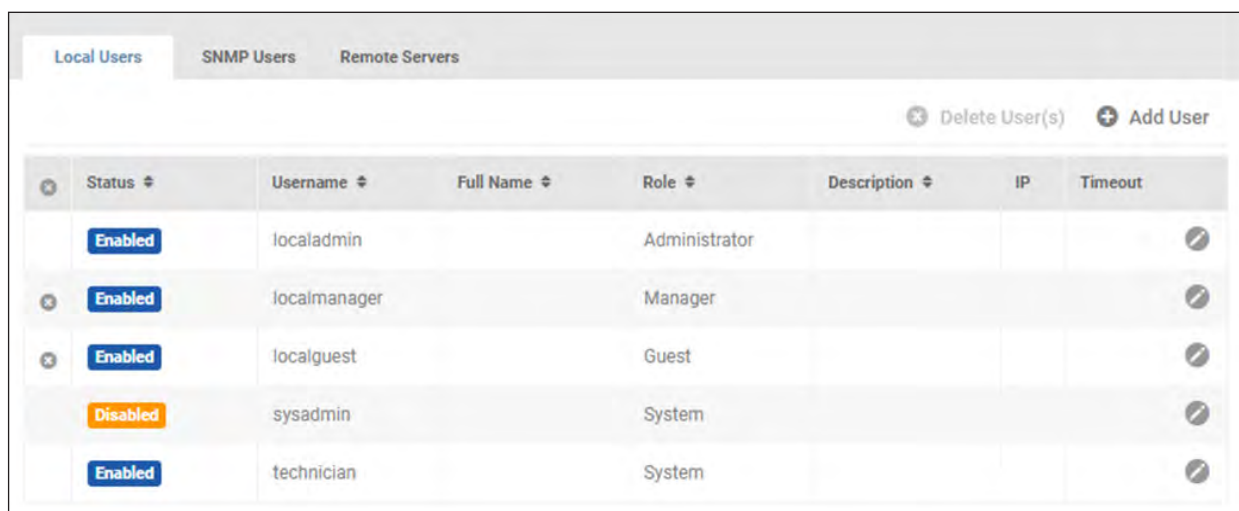
Figure 4-37: User Account tabs



## 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 4-38). Three preconfigured Local Users are provided by default: *localadmin*, *localmanager*, *localguest*. 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* user cannot be deleted.



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

Figure 4-38: 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 4-39). 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 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 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. PowerAlert Office 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

Local User

Enabled

UserSessionIP Filter

Username

ITadmin123

Full Name

Joe Admin

Role

Administrator

Description

Contact Info

Password

Confirm Password

Override Global Password Age

Enabled

Minimum Age

1

Day(s)

Maximum Age

30

Day(s)

Cancel

Save

Local User

Enabled

UserSessionIP Filter

Override Global Session Timeout

Enabled

360

Minute(s)

Override Global Idle Timeout

Enabled

60

Minute(s)

Cancel

Save

Local User

Enabled

UserSessionIP Filter

Address


Subnet Mask

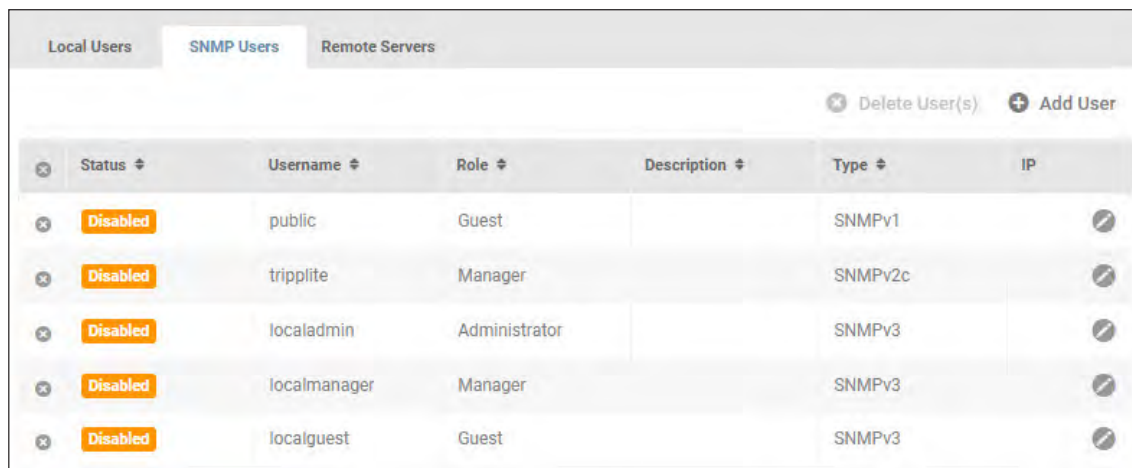
Cancel

Save

Figure 4-39: 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 4-40). These entities are commonly used by network management systems and SNMP utilities for inbound SNMP Sets, SNMP Gets, and SNMP Walks to PowerAlert Office. For outbound SNMP Traps, Informs, or SNMP Sets from PowerAlert Office 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. Note that all SNMP Users are disabled, by default; to enable an entry, move the slider to the right (Figure 4-41). 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	public	Guest		SNMPv1	
	Disabled	triplite	Manager		SNMPv2c	
	Disabled	localadmin	Administrator		SNMPv3	
	Disabled	localmanager	Manager		SNMPv3	
	Disabled	localguest	Guest		SNMPv3	

Figure 4-40: SNMP Users

To create a new SNMP User, click **Add User** and select one of the SNMP versions; a corresponding dialog box opens (Figure 4-41). Enter the required information, denoted by the boxes outlined in color. Note: Usernames cannot contain spaces.

For SNMPv1 and SNMPv2c Users, click 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.

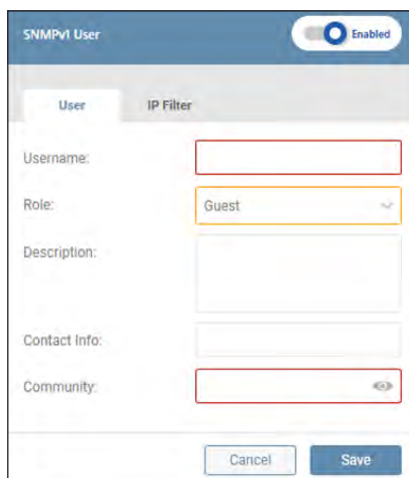
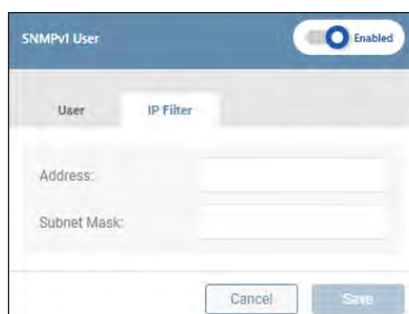
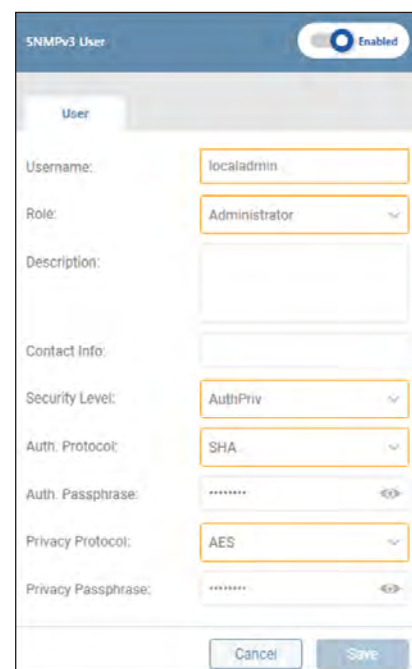

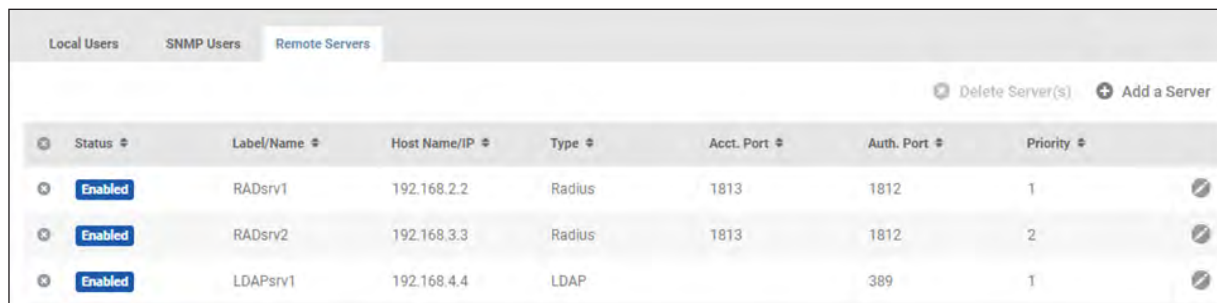




Figure 4-41: Creating an SNMP User – v1 and v3 Examples

## 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.



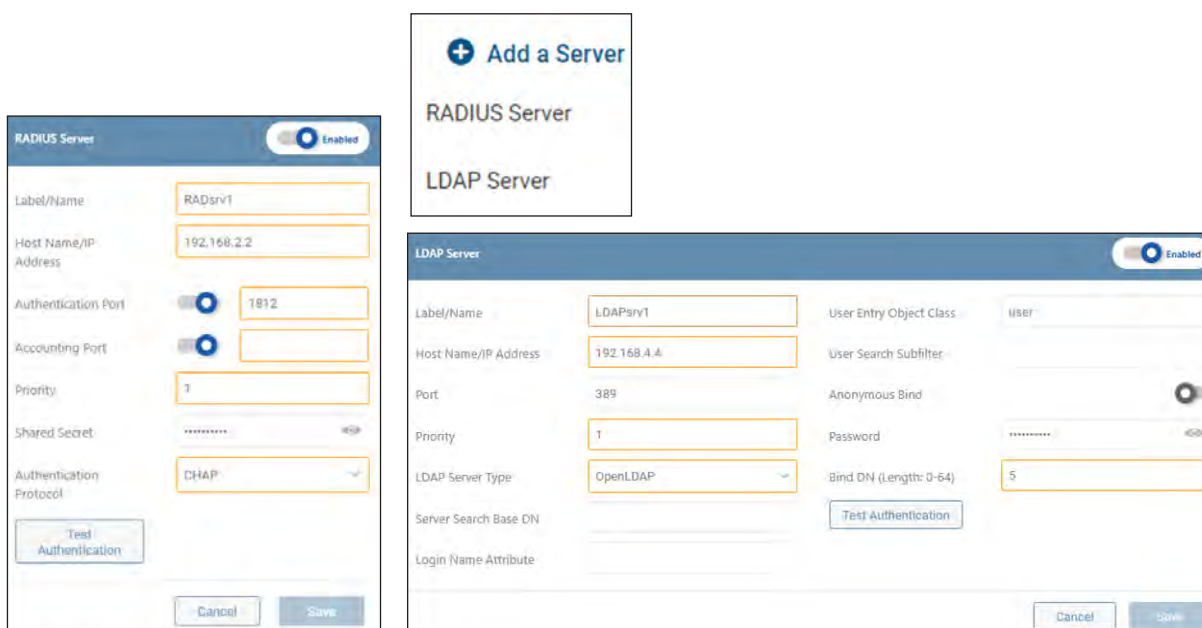
Status	Label/Name	Host Name/IP	Type	Acct. Port	Auth. Port	Priority
Enabled	RADsrv1	192.168.2.2	Radius	1813	1812	1
Enabled	RADsrv2	192.168.3.3	Radius	1813	1812	2
Enabled	LDAPsrv1	192.168.4.4	LDAP		389	1

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 PowerAlert Office based on the privileges assigned to the “UPSadmin” role created in PowerAlert Office.



**+ Add a Server**

**RADIUS Server**

**LDAP Server**

**RADIUS Server** Enabled

Label/Name: RADsrv1

Host Name/IP Address: 192.168.2.2

Authentication Port: 1812

Accounting Port:

Priority: 1

Shared Secret:

Authentication Protocol: CHAP

Test Authentication

Cancel Save

**LDAP Server** Enabled

Label/Name: LDAPsrv1

Host Name/IP Address: 192.168.4.4

Port: 389

Priority: 1

LDAP Server Type: OpenLDAP

User Entry Object Class: user

User Search Subfilter:

Anonymous Bind:

Password:

Bind DN (Length: 0-64): 5

Server Search Base DN:

Login Name Attribute:

Test Authentication

Cancel Save

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 4-44). 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.

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 the Privileges tab. Navigate through the left menu to view applicable privileges; Privileges will vary based on device type and model. Use the sliders to assign privileges to the role. By default, an Administrator has all Privileges; at the top of the dialog box, move the **Administrator** slider to the right in order to assign all Privileges to the role. 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.

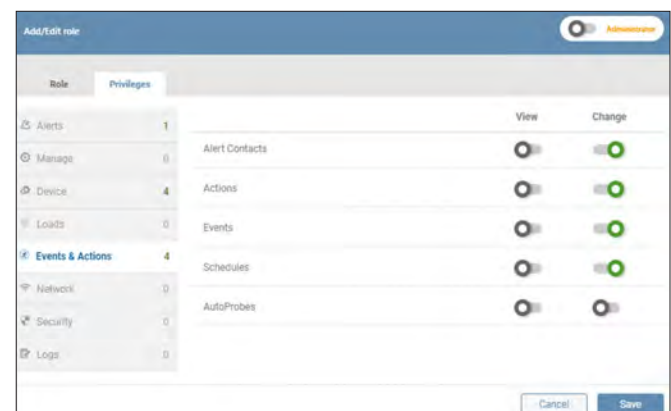
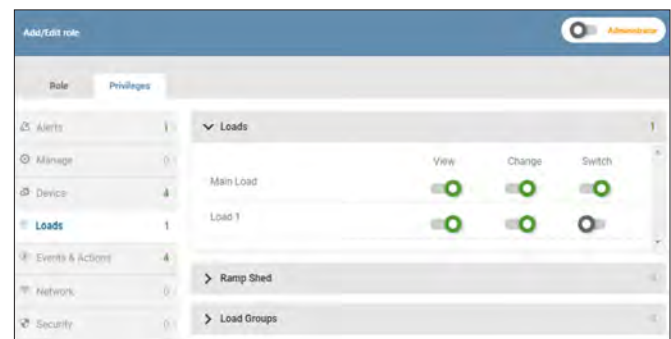
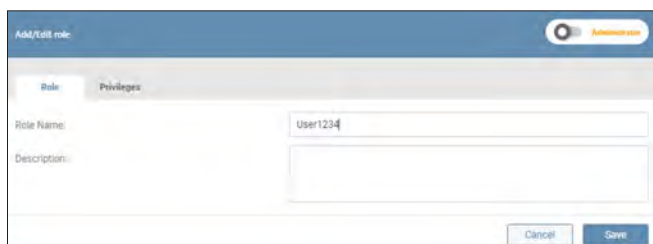


Figure 4-45: Adding a Role



## 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 input fields with up/down arrows: 'Global Session Timeout (Minutes)' set to 360 and 'Global Idle Timeout (Minutes)' set to 60. The 'Password Requirements' section features a 'Password Age Requirements' toggle switch that is turned on. Below this, there are three input fields with up/down arrows: 'Minimum Age (Days)' set to 7, 'Maximum Age (Days)' set to 30, and 'Min. # of Characters' set to 8. At the bottom, there are three checkboxes: 'Min. One Capital Letter', 'Min. One Number', and 'Min. One Special Character', all of which are currently unchecked.

Figure 4-46: Setting Timeouts and Password Requirements

## 4. Main Menu

To set the preferred Authorization and Accounting Schemes, select the desired setting from the respective pulldown menus (Figure 4-47). Note that “Local Accounting Only” will be the only available choice if no Remote Servers are configured (see User Accounts).

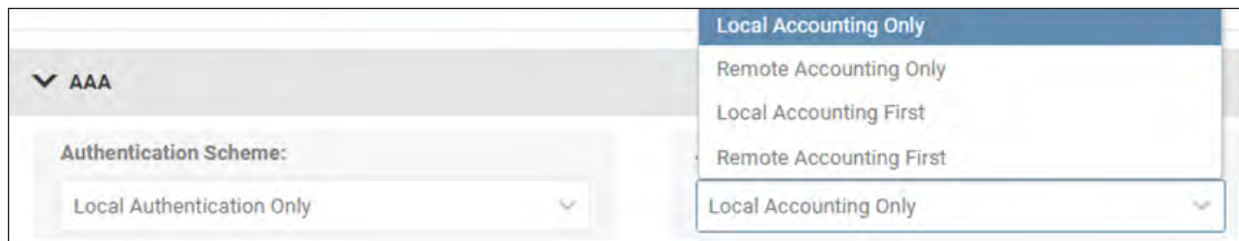


Figure 4-47: AAA Settings

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

### 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 the Application Log (Figure 4-48).

**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).

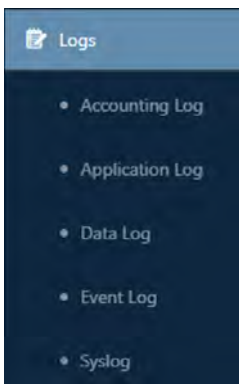


Figure 4-48: Logs Menu Item

## 4. Main Menu

### 4.8.1 Accounting Log

The Accounting Log documents events related to access of the PowerAlert interface, displaying the most recent events at the top of the log (Figure 4-49). 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.

The screenshot displays the 'Accounting Logs' section of a web application. It features a table with columns for Date/Time, User, Origin, Category, and Description. The table lists several events, including logins, logouts, SMTP settings, load group creation, and preference updates. Above the table are buttons for Refresh, Export, and Filter. Below the table is an 'Export Logs' dialog box with options for Export Format (CSV, XML) and Export To (Download, Email). The 'Download' option is selected for both.

Date/Time	User	Origin	Category	Description
6/19/2020 12:56:12 PM	localadmin	172.17.7.166	Login	login
6/19/2020 12:55:57 PM	localadmin	172.17.7.166	Login	logout
6/19/2020 12:48:12 PM	localadmin	172.17.7.166	SMTP Settings	Resource: network_smtp, Attributes: status=false,host=Mail123,port=25,user=username,password=****,security=SECURITY_NONE,auth_required=false,subject=PowerAlert Device Manager
6/19/2020 11:31:39 AM	localadmin	172.17.7.166	Login	login
6/19/2020 10:15:40 AM	localadmin	172.17.7.166	Load Groups	Operation: create, Resource: loads_group, ID: 1, Name: Group A, Attributes: name,description,enabled,device_id,current_load_id
6/19/2020 10:08:59 AM	localadmin	172.17.7.166	Preferences	Operation: update, Resource: preferences_user, Name: localadmin, Attributes: ui_settings
6/19/2020 9:49:03 AM	localadmin	172.17.7.166	Login	login

**Export Logs**

Export Format: ☒ CSV ☐ XML

Export To: ☒ Download ☐ Email

Figure 4-49: Accounting Log Summary and Export



## 4. Main Menu

To configure log size and automatic log exporting, click the Log Settings tab (Figure 4-50). 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.

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

The screenshot shows a web interface with two tabs: "Accounting Log" and "Log Settings". The "Log Settings" tab is active. Below the tabs, there is a label "Maximum number of stored log entries:" followed by a text input field containing "10000" and a small blue up/down arrow button. Below this input, there is a smaller line of text: "Minimum 1,000 to Maximum 10,000 entries". At the bottom right of the form is a blue "Save" button.

Figure 4-50: Accounting Log Settings

### 4.8.2 Application Log

The Application Log is not locally displayed. To view it, click the **Export Application Log Now** button. This will generate a syslog.txt file that can be retrieved from the Downloads folder. Use a standard text editor application to view the exported file (Figure 4-51).

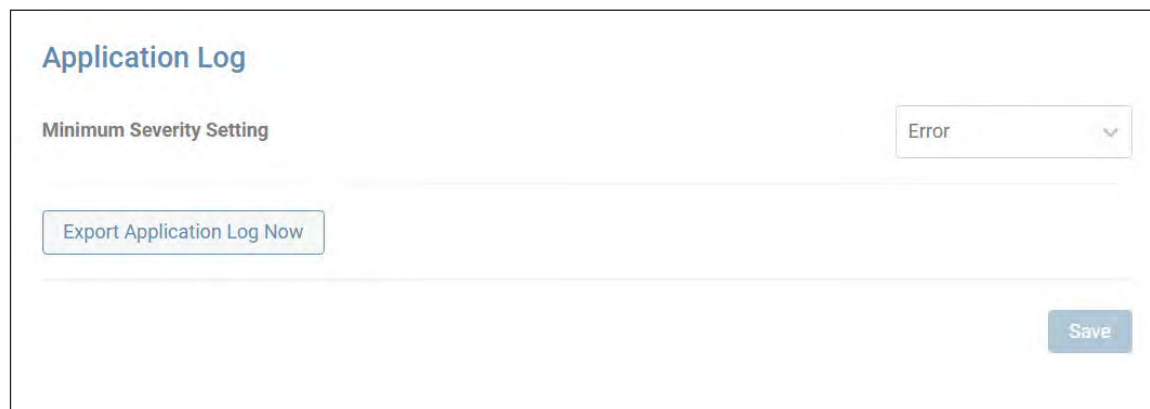
The screenshot shows a web interface titled "Application Log". Below the title, there is a label "Minimum Severity Setting" followed by a dropdown menu currently showing "Error". Below this is a blue button labeled "Export Application Log Now". At the bottom right of the form is a blue "Save" button.

Figure 4-51: Application Log

## 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 4-52).

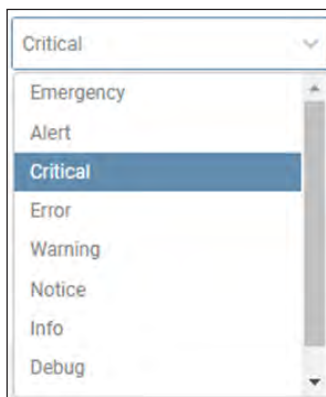


Figure 4-52: Minimum Severity Setting

### 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 (default setting), with the most recent readings appearing at the top of the log (Figure 4-53).

Data Logs    Data Log Rollups    Log Settings											
View   Refresh   Export   Filter											
Device Name	Device0076										
Date/Time	Battery					Input		Output			
	Runtime Remaining (Min)	Battery Charge Remaining	Battery Voltage	Battery Temperature (C)	Battery Temperature (F)	Input Frequency	Input Voltage	Output Frequency	Output Current	Output Utilization	Temper (F)
		%	V	C	F	Hz	V	Hz	A	%	F
1/20/2020 10:09:00 AM	437	100.0	27.3	34.0	93.2	59.7	120.1	59.7	0.0	0.0	
1/20/2020 10:08:00 AM	437	100.0	27.3	34.0	93.2	59.8	120.6	59.7	0.0	0.0	
1/20/2020 10:07:00 AM	437	100.0	27.3	34.0	93.2	59.7	120.1	59.7	0.0	0.0	
1/20/2020 10:06:00 AM	437	100.0	27.3	34.0	93.2	59.8	120.9	59.8	0.0	0.0	

Figure 4-53: Data Log, Time Series View.

## 4. Main Menu

Click the **View** button to select which data variable are to be displayed (Figure 4-54). 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 the **Alert Contacts** section of the **Events & Actions** menu item for details on creating email recipients. Data logs can be exported only in CSV format.

The figure consists of three screenshots of a web application interface, arranged vertically. The first screenshot is a 'View' dialog box with a blue header. It contains a 'Select All' checkbox which is checked. Below it are two rows, each with a right-pointing chevron, a checkmark, and the text 'Device0076' and 'Sensor4952' respectively. At the bottom are 'Cancel' and 'Save' buttons. The second screenshot is a 'Filter' dialog box with a light blue header. It has 'Apply Filters' and '+ Clear Filters' buttons on the left, and a 'Close >' button on the right. Below these are two date/time pickers. The first is labeled 'Start' with a calendar icon, showing '1/20/2020 12:00:00 AM'. The second is labeled 'End', showing '1/20/2020 11:59:00 PM'. The third screenshot is an 'Export Logs' dialog box with a blue header. It has 'Export To:' with two radio buttons: 'Download' (unselected) and 'Email' (selected). Below this is a table with two columns: 'Name' and 'Email'. The table has two rows. The first row has a radio button (unselected), 'JohnDoe', and 'johndoe@company.com'. The second row has a radio button (selected), 'JaneDoe', and 'janedoe@company.com'. At the bottom are 'Cancel' and 'Continue' buttons.

**View**

☒ Select All

> ☒ Device0076

> ☒ Sensor4952

Cancel Save

**Filter**

Apply Filters + Clear Filters Close >

Start 1/20/2020 12:00:00 AM End 1/20/2020 11:59:00 PM

**Export Logs**

Export To: ☐ Download ☒ Email

	Name	Email
<input type="radio"/>	JohnDoe	johndoe@company.com
<input checked="" type="radio"/>	JaneDoe	janedoe@company.com

Cancel Continue

Figure 4-54: 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 4-55).

Data Logs    Data Log Rollups    Log Settings													
View   Refresh   Export													
Device Name													
Date/Time	Input Frequency 2			Input Frequency 3			Input Frequency 1			Input Voltage L1-L2			
	Low	High	Average	Low	High	Average	Low	High	Average	Low	High	Average	
	Hz	Hz	Hz	Hz	Hz	Hz	Hz	Hz	Hz	V	V	V	
hourly	59.9	60.0	59.9	59.9	60.0	60.0	59.9	60.0	59.9	213.8	215.8	214.6	214.6
daily	59.9	60.0	59.9	59.9	60.0	59.9	59.9	60.0	59.9	212.7	221.5	216.4	216.4
weekly	59.9	60.0	59.9	59.9	60.0	59.9	59.9	60.0	59.9	212.8	222.4	217.9	217.9
monthly													
yearly													

Figure 4-55: Data Log, Roll-up View

To configure log recording parameters and automatic log exporting, click 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 4-56).

**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 4-56: Data Log Settings Message

By default, all metrics of the device and all connected sensors are selected. Click the pencil icon and use the pulldown menus to select which variables are to be logged (Figure 4-57).

**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

The screenshot displays the 'Data Log Settings' interface. At the top, there are three tabs: 'Data Log', 'Data Log Rollups', and 'Log Settings', with 'Log Settings' being the active tab. Below the tabs, the 'Export Criteria' section includes a label 'Intervals in seconds to record data' and a numeric input field set to '60'. A table below this shows 'Device' as 'Device0843' and '# of Variables' as '11'. A note states: 'Based on the time intervals selected 6 day(s) of Data records 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.' A 'Save' button is located in the top right corner of the settings area.

Below the main settings area, a modal window titled 'Select Variables to Log' is open. It features a search bar labeled 'Variable' and a list of variables. The variables are grouped into expandable sections: 'Device0076' (expanded), 'Device' (expanded), 'Battery' (expanded), 'Input' (expanded), 'Output' (expanded), 'Sensor4952' (collapsed), and 'Envirosense' (collapsed). Each variable has a checkbox and a checkmark indicating it is selected. The 'Cancel' and 'Save' buttons are at the bottom of the modal.

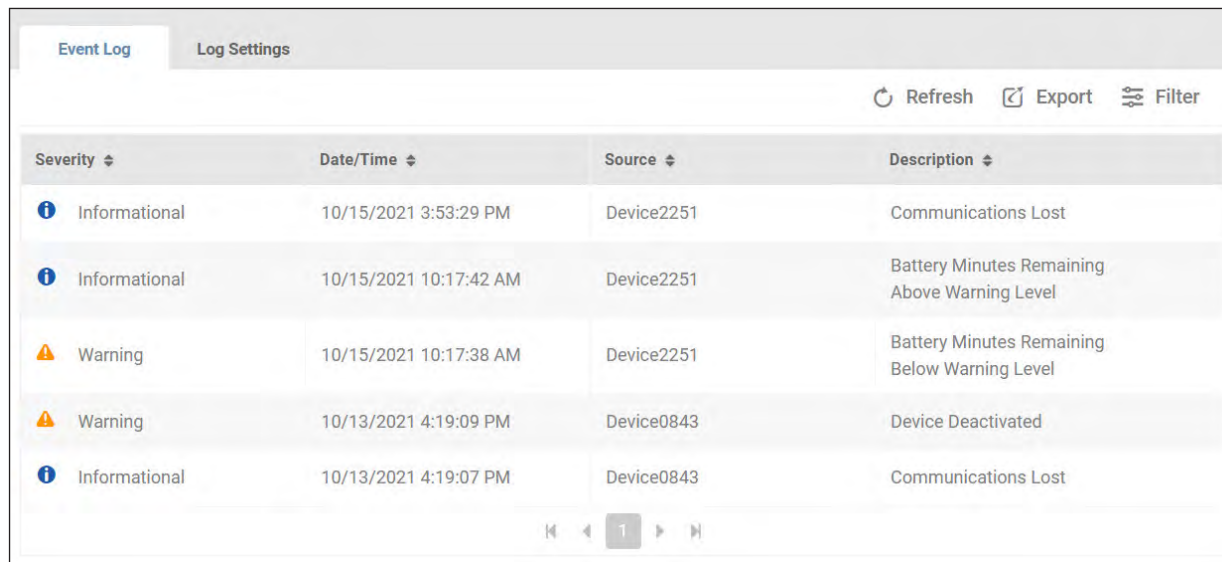
Variable	Selected
Device0076	✓
Device	✓
Battery	✓
Runtime Remaining (Min)	✓
Battery Charge Remaining	✓
Battery Voltage	✓
Battery Temperature (C)	✓
Battery Temperature (F)	✓
Input	✓
Output	✓
Sensor4952	
Envirosense	

Figure 4-57: 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 4-58). 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.



Event Log		Log Settings			
				Refresh	Export
				Filter	
Severity	Date/Time	Source	Description		
Informational	10/15/2021 3:53:29 PM	Device2251	Communications Lost		
Informational	10/15/2021 10:17:42 AM	Device2251	Battery Minutes Remaining Above Warning Level		
Warning	10/15/2021 10:17:38 AM	Device2251	Battery Minutes Remaining Below Warning Level		
Warning	10/13/2021 4:19:09 PM	Device0843	Device Deactivated		
Informational	10/13/2021 4:19:07 PM	Device0843	Communications Lost		

Figure 4-58: Event Log

To configure log recording parameters, click the **Log Settings** tab (Figure 4-59). 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. Click the **Save** button once all edits have been made.





Event Log		Log Settings	
Maximum number of stored log entries:		10000	
Minimum 1,000 to Maximum 10,000 entries			
		Save	

Figure 4-59: 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.












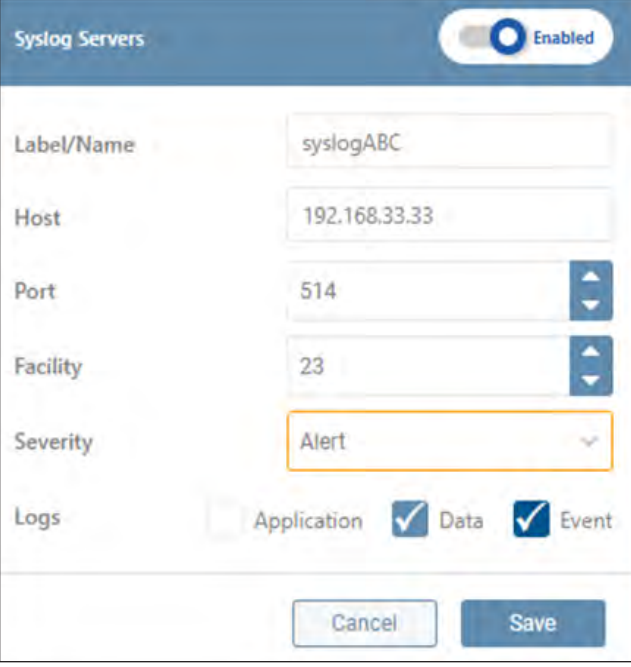

							 Delete Syslog Server	 Add a Syslog Server
 Status	Label/Name	Host	Port	Facility	Severity	Logs		
 <b>Enabled</b>	syslogABC	192.168.33.33	514	23	Alert	 		
 <b>Enabled</b>	syslog123	192.168.44.55	515	22	Debug	 		

Figure 4-60: 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** 

Label/Name



syslogABC

Host

192.168.33.33



Port

514




Facility

23



Severity

Alert



Logs

☐ Application ☒ Data ☒ Event

Cancel

Save



## 5. Technical Support

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

Phone: 773.869.1234 (7am – 6pm CST).

Web: [tripplite.com/support](http://tripplite.com/support)

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

## Appendix A – Features by Package

PowerAlert Software		PowerAlert Package		
Category	Feature	Office	Home	Medical
ACTIONS	Device Shutdown	Yes	Yes	Yes
	OS Shutdown & Restart	Yes	Yes	Yes
	Script Execution	Yes		
	Manage Scheduled Actions	Yes		
	Manage AutoProbes	Yes		
ALERTS	Alert Rollup	Yes	Yes	Yes
	Alert Acknowledgment	Yes		Yes
CONFIGURATION	Remote Configuration	Yes	Yes	Yes
	Mass Configuration Utility	Yes	Yes	Yes
	Manage Battery Packs	Yes		
EVENTS	Display Events	Yes	Yes	Yes
	Edit Events	Yes		Yes
	Event Actions	Yes		
LOADS	Display Individual Loads	Yes	Yes	Yes
	Edit Load Attributes	Yes		Yes
	Display Status	Yes	Yes	Yes
	Display Metrics	Yes		Yes
	Load Control	Yes	Yes	
	Manage Load Groups	Yes		
LOGGING	Accounting Log	Yes		Yes
	Application Log	Yes	Yes	Yes
	Data Log	Yes		Yes
	Event Log	Yes	Yes	Yes
	Manage Syslog Servers	Yes		
MAINTENANCE	Version Check	Yes	Yes	Yes
	Update and Downgrade	Yes	Yes	Yes
NOTIFICATIONS	Email	Yes	Yes	
	SMS	Yes		
	SNMP	Yes		
PROTOCOLS	HTTP & HTTPS	Yes	Yes	Yes
	SNMP	Yes		
SECURITY	Authorization, Accounting & Authentication	Yes		
	Password Policies	Yes		
	Manage Users	Yes		Yes
	Manage Roles & Privileges	Yes		
	Manage User Sessions	Yes		
	Idle & Session Timeouts	Yes	Yes	Yes
OTHER	Watchdog Compatibility	Yes	Yes	Yes
	IP Binding	Yes	Yes	Yes
	System Tray	Yes	Yes	Yes
	SNMP Access	Yes		

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

