

User's Guide

LX Platform Devices

Table of Contents

1. Introduction	2	4. Telnet/SSH Console	28	4.3 Network Configuration	68
1.1 System Requirements	2	4.1 Device Menu	29	4.3.1 IP Configuration	68
2. Installation and Configuration	3	4.1.1 Status	30	4.3.1.1 Host Name	69
2.1 Saving Configuration Changes	3	4.1.2 Identification	31	4.3.1.2 Domain Data Entry Menu	69
2.2 Default UPS System Shutdown Settings	3	4.1.3 Controls	32	4.3.1.3 IPV4 Settings	69
2.3 SNMP Configuration	3	4.1.3.1 Control Data	32	4.3.1.4 IPV6 Settings	70
3. The Web Interface	4	4.1.4 Events	33	4.3.2 User Access Interfaces	70
3.1 Accessing the Web Interface	4	4.1.5 Loads	35	4.3.2.1 Telnet/SSH	70
3.2 Status	5	4.1.5.1 Load Configuration	35	4.3.2.2 Web	71
3.2.1 Status/Overview	5	4.1.5.2 Load Groups	36	4.3.2.3 SNMP Settings	72
3.2.2 Status/Details	6	4.1.5.3 Ramp/Shed Settings	37	4.3.2.4 FTP/SFTP	72
3.2.3 Status/Alarms	6	4.1.6 Preferences and Thresholds	38	4.3.3 Remote Services	73
3.3 Control	6	4.1.7 Device Alarms	38	4.3.3.1 Email Settings	74
3.3.1 Control/Device	7	4.1.8 Logs	38	4.3.3.2 Remote Syslog Servers	75
3.3.2 Control/Loads	8	4.2 System Configuration	38	4.3.3.3 Auto Probes	78
3.3.3 Control/Load Groups	9	4.2.1 Address Book	39	4.4 Alarms and Logging	88
3.3.4 Control/Events	10	4.2.1.1 Email Contacts	39	4.4.1 Alarms	88
3.4 Configuration	11	4.2.1.2 SNMP Contacts	40	4.4.1.1 Alarm Details	89
3.4.1 Configuration/System Settings	11	4.2.1.3 HTTP Contacts	42	4.4.2 View Logs	89
3.4.2 Configuration/Device Settings	12	4.2.2 Global Actions	43	4.4.2.1 Data Log	90
3.4.3 Configuration/Contacts	13	4.2.2.1 Action Profiles	43	4.4.2.2 Event Log	92
3.4.3.1 Email	13	4.2.2.2 Schedules	55	4.4.3 Logging Settings	95
3.4.3.2 SNMP V1	14	4.2.3 Security	59	4.4.3.1 Accounting Log Settings	95
3.4.3.3 SNMP V2c	14	4.2.3.1 Authentication Method	59	4.4.3.2 Application Log Settings	95
3.4.3.4 SNMP V3	15	4.2.3.2 Local Users	60	4.4.3.3 Data Log Settings	96
3.4.3.5 HTTP	15	4.2.3.3 RADIUS Servers	63	4.4.3.4 Event Log Settings	97
3.4.3.6 HTTPS	16	4.2.3.4 Change Password	64	4.4.3.5 Format Settings	98
3.4.3.7 Configuration/Network	16	4.2.4 Date/Time	64	4.5 About	98
3.4.3.8 Configuration/Network/Services	17	4.2.4.1 Time Source Data Entry Menu	64	5. Command Line Interface	99
3.4.3.9 Configuration/Network/SMTP	17	4.2.4.2 Time Zone	65	5.1 Syntax Conventions	99
3.4.3.10 Configuration/Network/Internet	18	4.2.4.3 NTP Settings	65	5.2 Manual Pages	100
3.4.3.11 Configuration/Network/Domain	18	4.2.4.4 Time Settings	66	5.3 Output Conventions	100
3.4.4 Configuration/Actions	19	4.2.5 Local Device Discovery	66	5.4 Getting Started with the PowerAlert CLI	100
3.4.4.1 Defining Action Types	19	4.2.6 Restart PowerAlert Device Manager	67	6. Troubleshooting	102
3.4.5 Configuration/Scheduling	21			7. Technical Support	102
3.4.6 Security	22			8. Appendix	103
3.4.7 Configuration/Log Settings	23				
3.5 Logs	24				
3.5.1 Logs/Events Log	25				
3.5.2 Logs/Data Log	25				
3.5.3 Logs/Accounting Log	26				
3.6 About	27				

Documentation Notice: This User's Guide is a supplement to the printed manual that came with your Tripp Lite LX Platform device. Refer to the printed manual for instructions on hardware installation and basic configuration, including IP address assignment. If you have misplaced your printed manual, you can download an electronic version at www.tripplite.com/support and entering the model number of your product in the search box.

PROTECT YOUR INVESTMENT!

Register your product for quicker service and ultimate peace of mind.

You could also win an ISOBAR6ULTRA surge protector—a \$100 value!

www.tripplite.com/warranty



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

Copyright © 2018 Tripp Lite. All trademarks are the sole property of their respective owners.

1. Introduction

Tripp Lite LX Platform devices contain an Ethernet network interface that enables remote monitoring, control and condition reporting. These functions can be performed using Tripp Lite Management Software, SNMP Network Management Software, a Web browser or Telnet/SSH. This User's Guide focuses on configuration and management offered through the web interface and Telnet/SSH. The web interface for LX Platform devices is known as the PowerAlert® Device Manager, or PADM, for short.

1.1 System Requirements

- Tripp Lite LX Platform Device, such as WEBCARDLX, PDU3E-series PDUs, PDU3XE-series PDUs, LX suffix PDUs and LX-compatible Cooling products
- Ethernet network that supports the TCP/IP protocol
- One of the following options for remote monitoring and control:
 - Tripp Lite Management Software
 - SNMP-based Network Management Software
 - Web browser (Chrome, Firefox, Internet Explorer or Safari)
 - VT-100 Telnet and/or SSH Client
- For “Terminal Mode” configuration only:
 - Terminal emulation software program (such as TeraTerm Pro by Ayera Technologies)

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

2. Installation and Configuration

For instructions on hardware installation and basic configuration, refer to the printed manual included with your Tripp Lite LX Platform device. For instructions on loading a firmware or device driver upgrade, refer to the applicable release notes. The manual and release notes can be downloaded by going to www.tripplite.com and typing the model name of the LX Platform device in the search bar.

2.1 Saving Configuration Changes

Most configuration changes made in PowerAlert Device Manager will take effect immediately. PADM and Telnet/SSH will typically advise you if your configuration changes require a restart to take effect.

Regardless, to ensure that configuration changes persist, it is recommended that you restart PowerAlert Device Manager. Most configuration changes will auto-save after about 30 minutes of idle time; changes to the network settings will not.

Restarting PADM will not disrupt power to equipment powered through your UPS or PDU and has no effect on the general operation of your Tripp Lite device.

2.2 Default UPS System Shutdown Settings

When used with a Tripp Lite UPS during a power failure, WEBCARDLX is pre-configured to shut down the UPS system two minutes after receiving a low battery signal. This allows the UPS system to provide the maximum available runtime to connected equipment. To change the default setting, select Device Shutdown from the Action Type dropdown menu (refer to **3.4.4 Configurations/Actions** or **4.2.2.1 Action Profiles for Telnet/SSH**).

2.3 SNMP Configuration

LX Platform devices function as SNMP-managed devices on your network, using the SNMP agent and Management Information Base (MIB). The SNMP agent resides in the LX Platform device firmware and responds to standard SNMP commands (Get, Get Next and Set). It can also generate SNMP traps (messages). The MIB determines which parameters can be monitored and controlled. Three MIB files—TRIPPLITE.MIB, TRIPPLITE-PRODUCTS.MIB and RFC-1628-UPS.MIB—must be loaded on each Network Management Station that will monitor the managed device. (The files can be downloaded from www.tripplite.com/support. Consult your Network Management Station software documentation for instructions on how to import MIB files.)

Note: *SNMP Users are configured in the Configuration > Security > User section of PADM.*

SNMPv3 Definitions

<i>Username</i>	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. A username can have up to 32 ASCII characters (alphanumeric and the following special characters: !@#\$%^*(){}[]~_-).
<i>Authentication Passphrase</i>	A phrase of 8 to 32 ASCII characters (alphanumeric and the following special characters: !@#\$%^*(){}[]~_-) that verifies that the Network Management System (NMS) communicating with this device through SNMPv3 is the NMS it claims to be, that the message has not been changed during transmission, and that the message was communicated in a timely manner, indicating that it was not delayed and that it was not copied and sent again later at an inappropriate time.
<i>Privacy Passphrase</i>	A phrase of 8 to 32 ASCII characters (alphanumeric and the following special characters: !@#\$%^*(){}[]~_-) that ensures the privacy of the data (by means of encryption) that a Network Management System (NMS) is sending to this device or receiving from this device through SNMPv3.
<i>Authentication Protocol</i>	The Tripp Lite implementation of SNMPv3 supports only SHA (as of 15.04.0) authentication.
<i>Privacy Protocol</i>	The Tripp Lite implementation of SNMPv3 supports only AES (as of 15.04.0) as the protocol for encrypting and decrypting data.
<i>Public Value</i>	A field provided to enter a username/password hint for SNMPv3 Admin users. This SNMPv3 value is part of the SNMPv3 USM User Table.

3. The Web Interface

3.1 Accessing the Web Interface

- 1. Open your browser.
- 2. Enter the IP address assigned to the LX Platform device in the address bar.
- 3. The login page will appear with prompts for Username and Password (Figure 3-1). The default administrator username is **localadmin** and the default password is **localadmin**. The Username and Password fields are case sensitive. After entering the login credentials, click the [Login] button.



Figure 3-1: Login Page

- 4. After logging in, the Overview page on the Status Menu will display. (Figure 3-2a). Additional navigation elements are shown in Figure 3-2b.

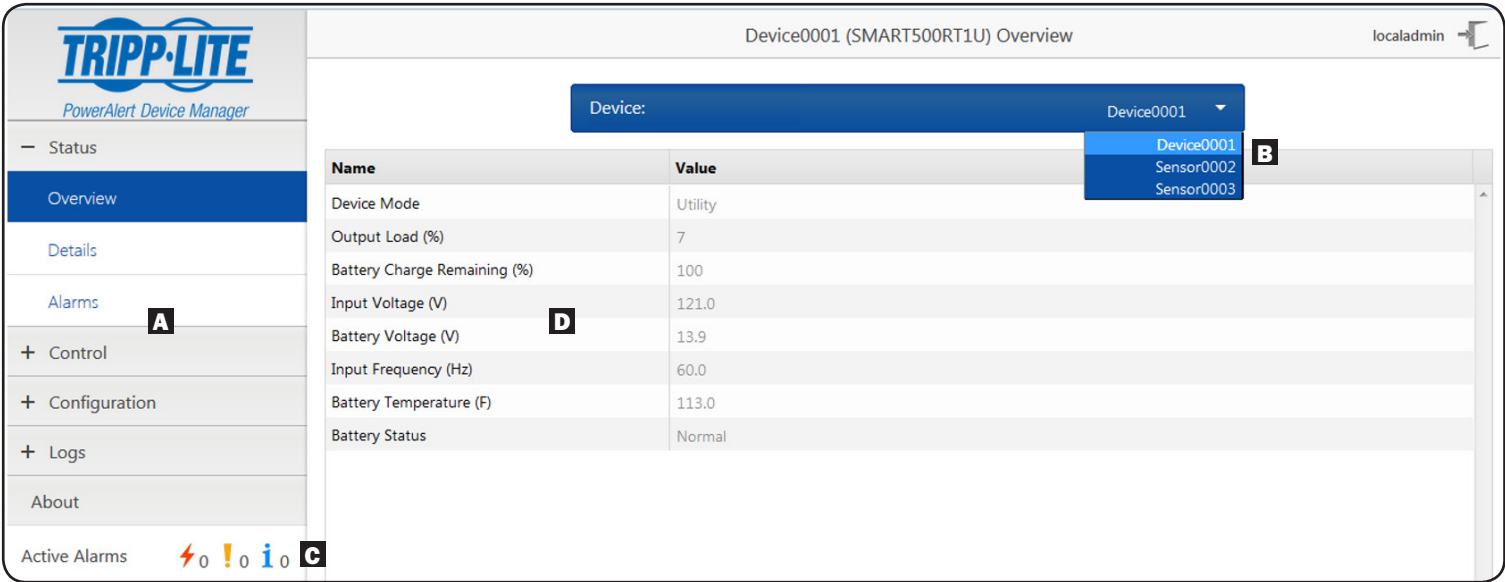


Figure 3-2a: Power Alert Device Manager Navigation

- A Menus:** Click the + next to a menu item to expand the menu group and expose the submenus.
- B Dropdown Menu:** Click to select a submenu. The first submenu item is typically the main device, followed by any peripherals attached to it, (e.g. environmental sensors).
- C Active Alarm Count:** Click active alarms for a shortcut to bring up the alarm page.
- D Page Data:** Menu-driven information displays here.

3. The Web Interface

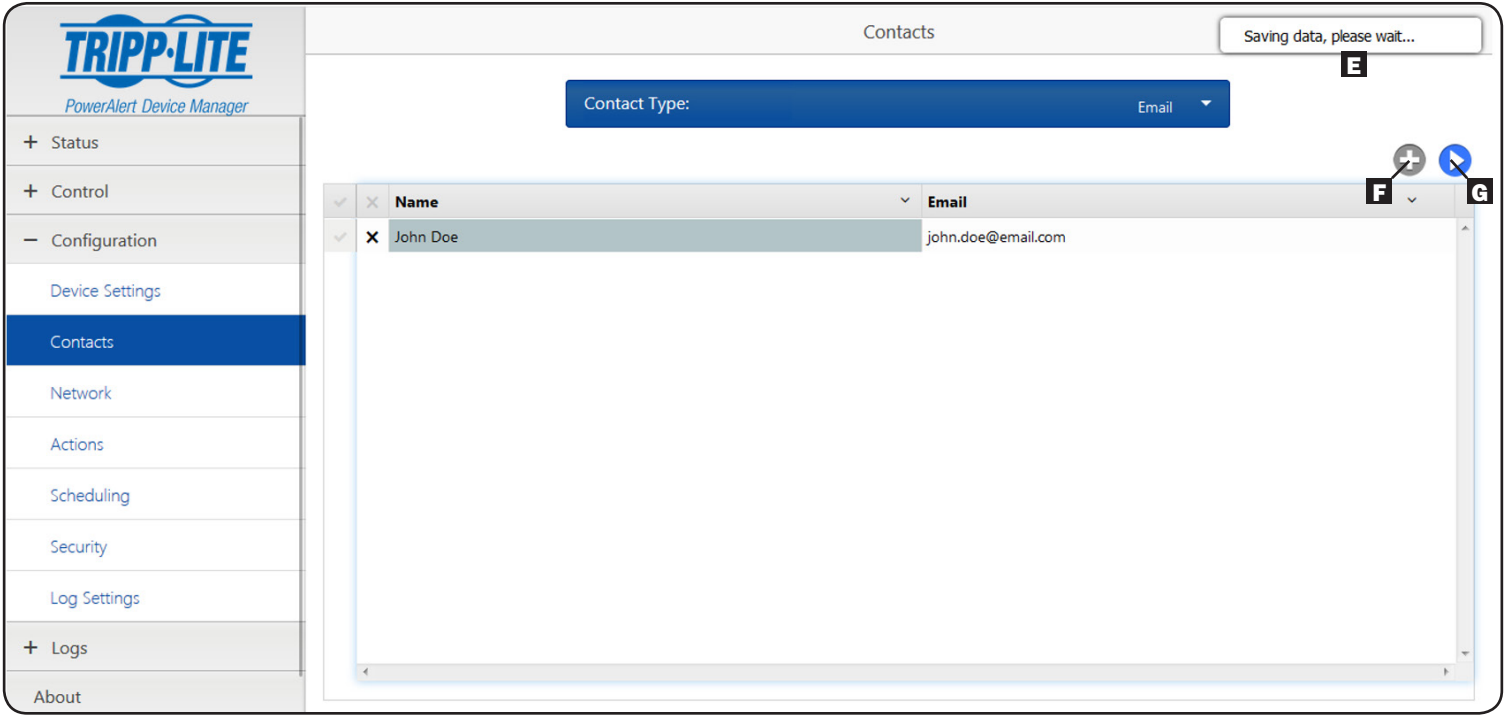


Figure 3-2b: Power Alert Device Manager Navigation

E Message Display: User feedback messages appear in this area.

F Plus button: Click to add a new item.

G Save button: Click to save the settings.

3.2 Status

The Status menu group contains three submenus: Overview, Details and Alarms.

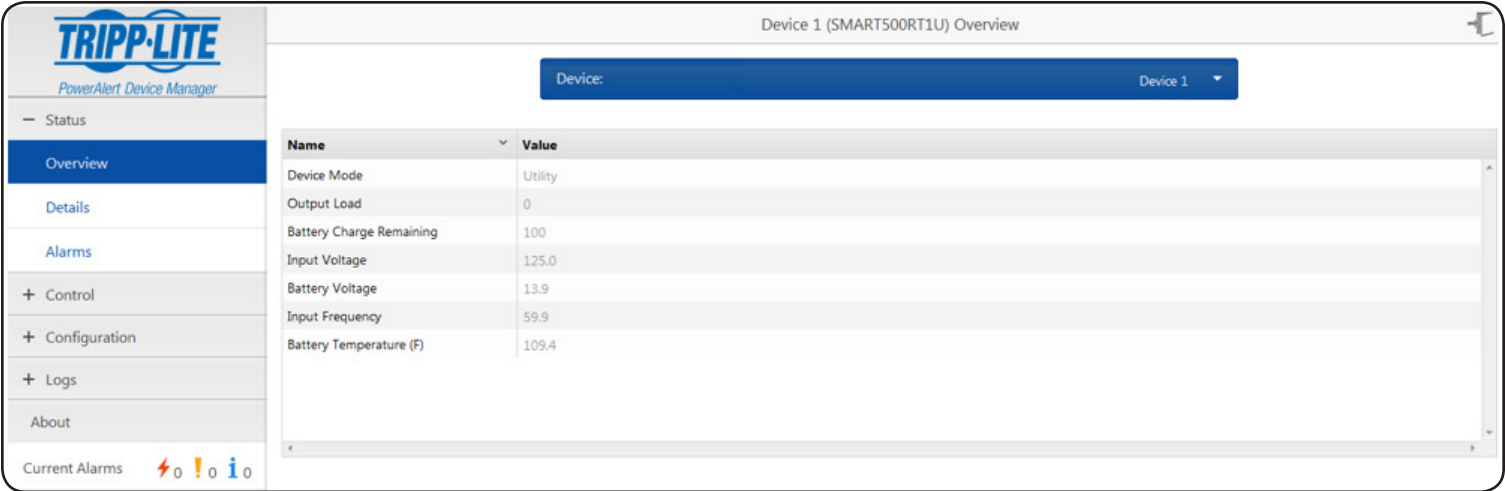


Figure 3-3: Status Menu and Overview Page

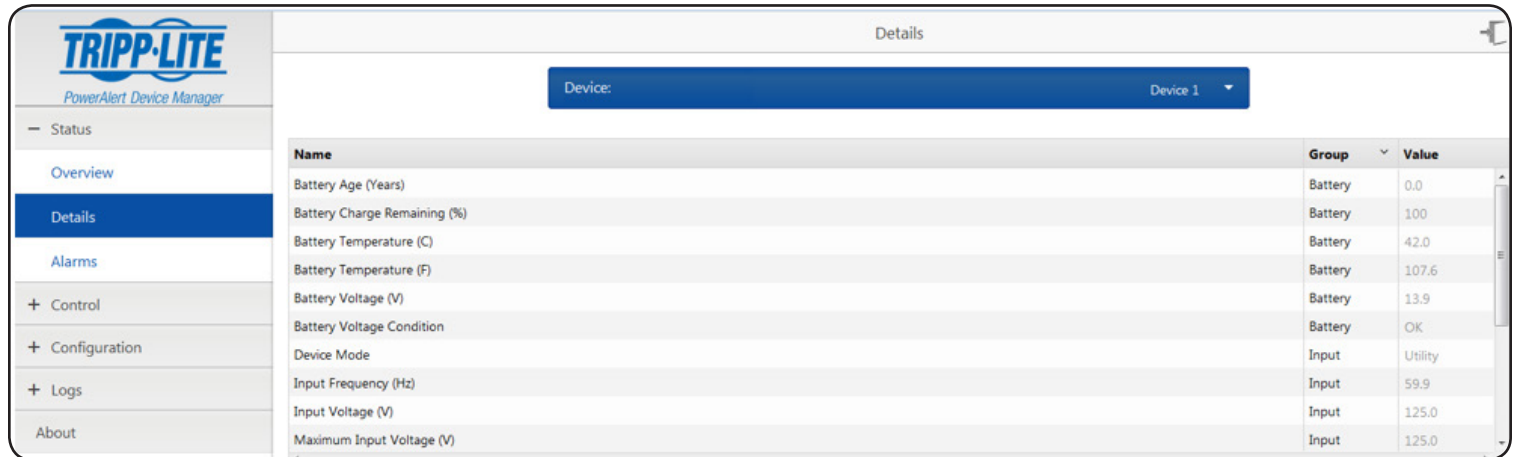
3.2.1 Status/Overview

The Overview page displays a subset of data for the selected device type that users reference most often.

3. The Web Interface

3.2.2 Status/Details

The Details page (Figure 3-4) displays the full list of device status information for the selected device, including the information displayed in the Overview page. To navigate between the device and any connected EnviroSense2 sensor modules, select the desired device from the device dropdown menu.



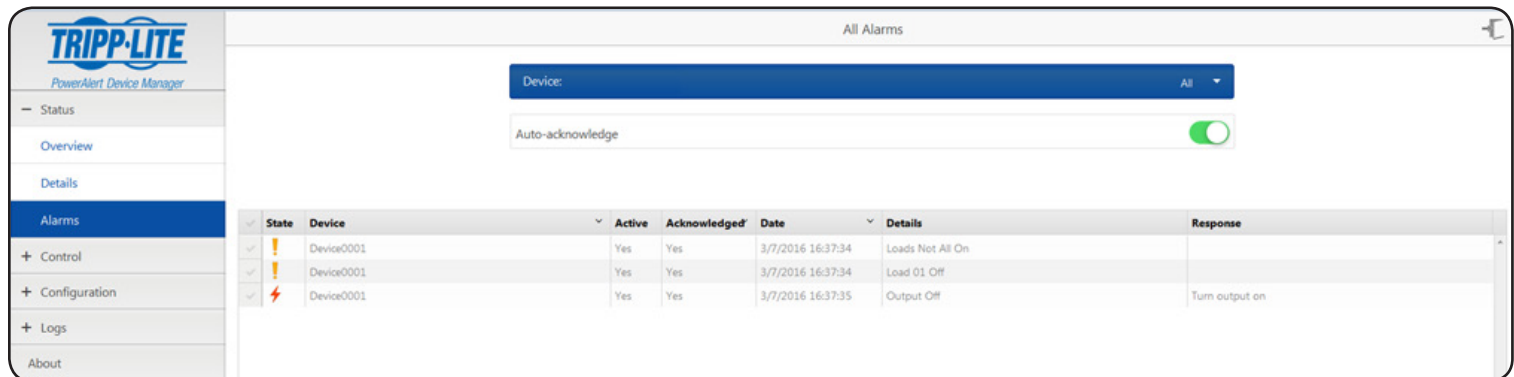
Name	Group	Value
Battery Age (Years)	Battery	0.0
Battery Charge Remaining (%)	Battery	100
Battery Temperature (C)	Battery	42.0
Battery Temperature (F)	Battery	107.6
Battery Voltage (V)	Battery	13.9
Battery Voltage Condition	Battery	OK
Device Mode	Input	Utility
Input Frequency (Hz)	Input	59.9
Input Voltage (V)	Input	125.0
Maximum Input Voltage (V)	Input	125.0

Figure 3-4: Details Page

3.2.3 Status/Alarms

The Alarms page (Figure 3-5) will display the alarms for the selected device. Along with the time stamp and alarm details, alarms indicate their current state (active or inactive) and the acknowledge status (yes or no). An alarm that is inactive, meaning the alarm condition has cleared, and acknowledged will be removed from the list. An alarm can be acknowledged in one of two ways: the system can be set to auto-acknowledge alarms as they are received, or the user can disable auto-acknowledge and manually acknowledge alarms by selecting the checkbox (or checkboxes) of the alarms to be acknowledged and clicking the Acknowledge button. By default, Auto-acknowledge is enabled (as shown in Figure 3-5) and, as a result, the Acknowledge button is not displayed. Turn off the Auto-acknowledge switch to see the Acknowledge button (🔴).

Note: This setting should be enabled if using with Tripp Lite management software or PowerAlert Network Shutdown Agent (PANSA).

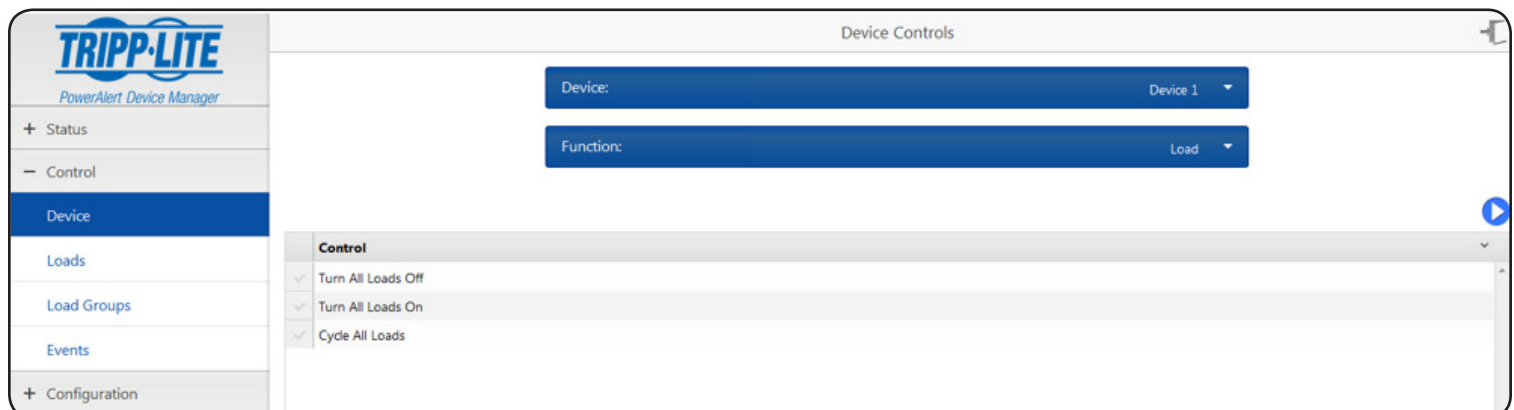


State	Device	Active	Acknowledged	Date	Details	Response
🔴	Device0001	Yes	Yes	3/7/2016 16:37:34	Loads Not All On	
🔴	Device0001	Yes	Yes	3/7/2016 16:37:34	Load 01 Off	
🔴	Device0001	Yes	Yes	3/7/2016 16:37:35	Output Off	Turn output on

Figure 3-5: Alarms Page

3.3 Control

The Control menu group contains four submenus: Device, Loads, Load Groups and Events. The available controls will vary by device.



Control
✓ Turn All Loads Off
✓ Turn All Loads On
✓ Cycle All Loads

Figure 3-6: Control Menu Group

3. The Web Interface

3.3.1 Control/Device

The Device page includes system maintenance controls that can be performed on the LX Platform device as well as access to the controls supported on the individual devices to which the LX Platform device is communicating. The system maintenance controls include “Restart SNMP Card”, “Restart with Factory Defaults (Preserve Network Settings)”, “Restart with Factory Defaults (Do NOT Preserve Network Settings)” and “Firmware Update”. The three restart methods do not require any user parameters. Simply check the desired Control, and click the [Save] button to execute. The system will prompt you that your session will close and allow you to **Continue** or **Cancel**.

Restarts can also be performed by pressing the Reset button on the Tripp Lite device. A short press (~ 1 second) will restart the webcard. A long press (press and hold for 15-20 seconds) will result in a restart with factory defaults, preserving the network settings.

Note: Executing any of these resets will not interrupt device operation. For example, an LX Platform PDU will continue distributing power through its outlets during a restart.

In some cases, controls may have parameters may appear lower on the web page; be sure to scroll down to access these parameters.

The “Firmware Update” control requires the selection of a firmware file. Select Choose File to browse to the location of the required .tar file (see next paragraph). Select the file to upload and click the [Save] button to execute (Figure 3-7). The Firmware Update process will prompt you that it will take several minutes. You will be logged out while the update is performed. Once you click OK, the update will start by uploading the specified file to the LX Platform device, where it will be decompressed and installed. During the update, the Status LED on the device interface will alternate between green and orange. After the update finishes installing, the device interface will reboot. A solid green Status LED indicates the update is complete. When the device interface is back online following the reboot, the PowerAlert Device Manager version can be checked via the Device/About page (refer to section **3.6 About** for details).

The file or files required for firmware update are located within "LX" firmware packages which are downloadable from the Tripp Lite website. These packages contain detailed instructions on performing the update, whether individually through PADM or using the PowerAlert Mass Updater Utility (also included in the LX firmware package). Another option for updating firmware is uploading the files via SFTP (enabled by default) and using the swupdate command in CLI.

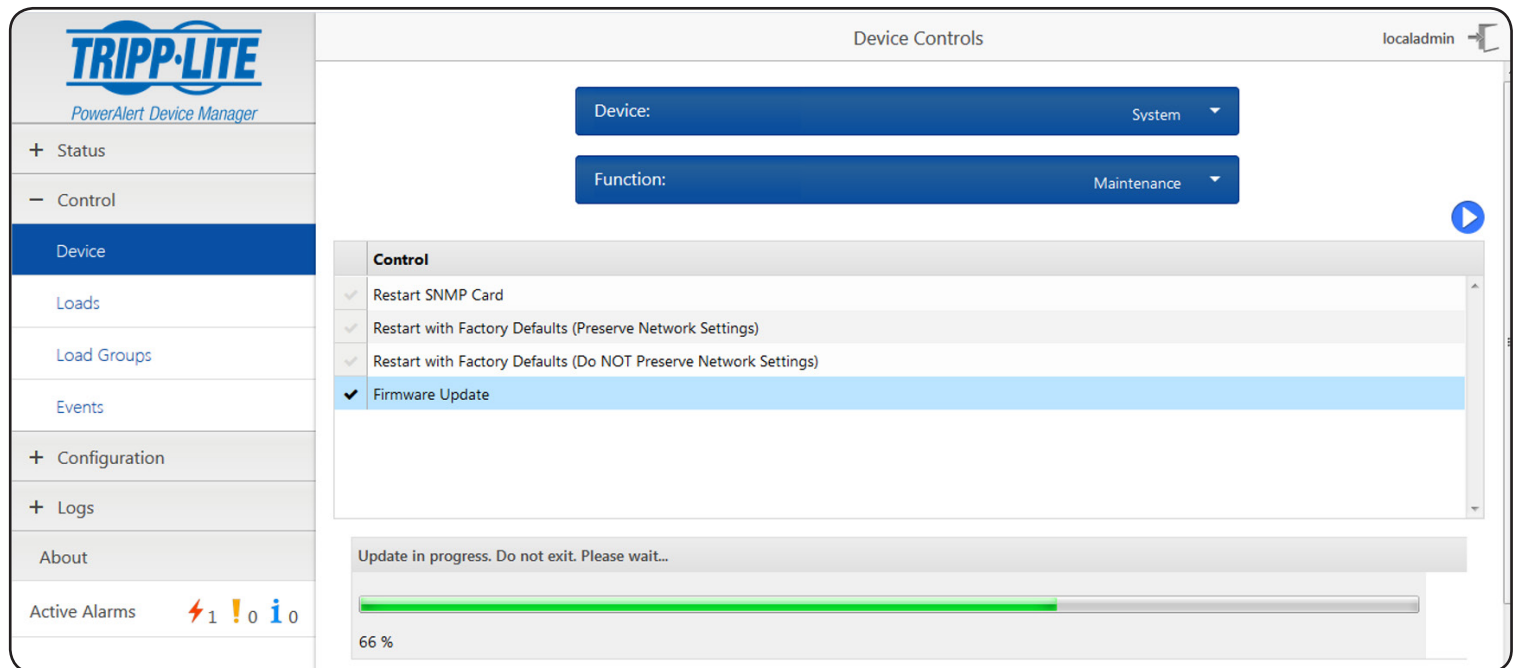


Figure 3-7: System Maintenance Controls

3. The Web Interface

In addition to the System Maintenance controls, individual device controls can be accessed by first selecting the specific device and then selecting the function. The options will vary by device; examples are “Test”, “Shutdown” and “Load” (Figure 3-8). For devices with controllable loads, the Load function group includes “Cycle All Loads”, “Turn All Loads Off” and “Turn All Loads On”. Example Shutdown controls include “Device Shutdown”, if supported. Click the [Save] button to execute the function.

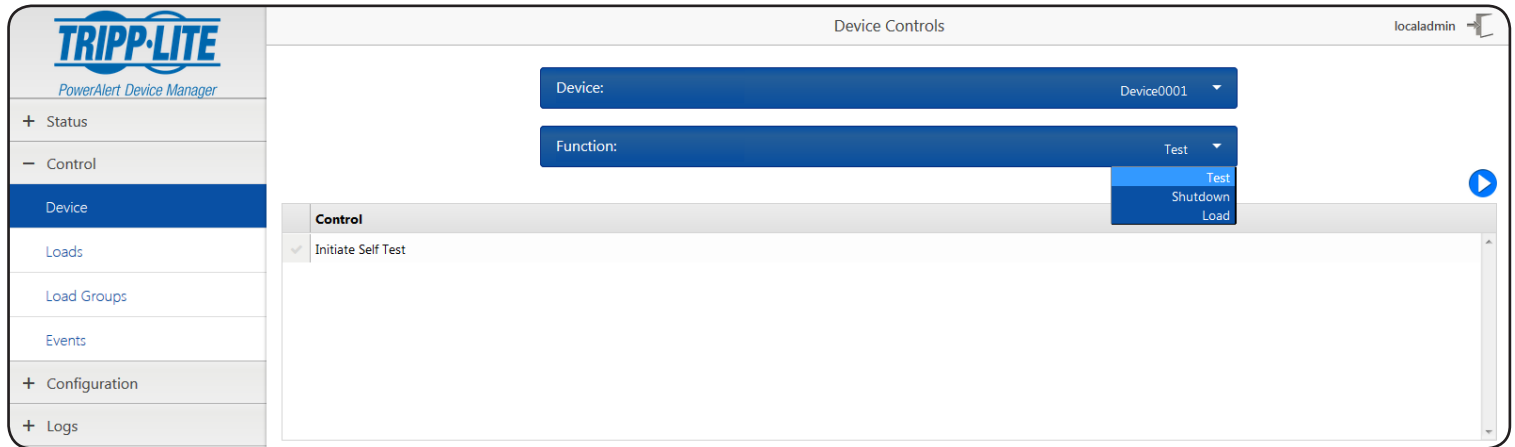


Figure 3-8: Individual Device Controls

3.3.2 Control/Loads

If the selected device has loads, the state of the load can be viewed on the Loads page (Figure 3-9). For devices that support controllable loads, the load state can be changed by choosing the load and then choosing the desired state: **On** if the load is off, **Off** if the load is on, or **Cycle** to turn the load off and then back on. Ramp and Shed behaviors can be set, each with adjustable delay times, for controllable loads that support ramp/shed. Select the desired behavior and timing for each load and click the [Save] button. Loads or Outlet Banks can be given a Description for easy identification. Simply enter the desired description and click the [Save] button. Ramp or Shed controls configured in this fashion can be manually executed in the Control > Device page, selecting Load in the Function sub-menu. For autonomous execution of Ramp and Shed, see section 3.4.4 Configurations/Actions.

The Loads page also allows the Main Load to be turned on, off or cycled on devices that support Main Load control. The on/off state of non-controllable loads is displayed, but the controls are not selectable.

For devices that support per-outlet or per-bank Current or Power measurement, those values will be displayed on the Loads page. Remember that load fluctuates with the power demands of the connected equipment. It is prudent to limit the total connected load to no more than 80% of the device's maximum capacity to accommodate higher start-up power demands and other increased power needs. Each load may optionally be assigned to a realm, which allows or restricts a user's Read Only or Read/Write access to the outlets in that realm (as set in Configuration>Security>User).

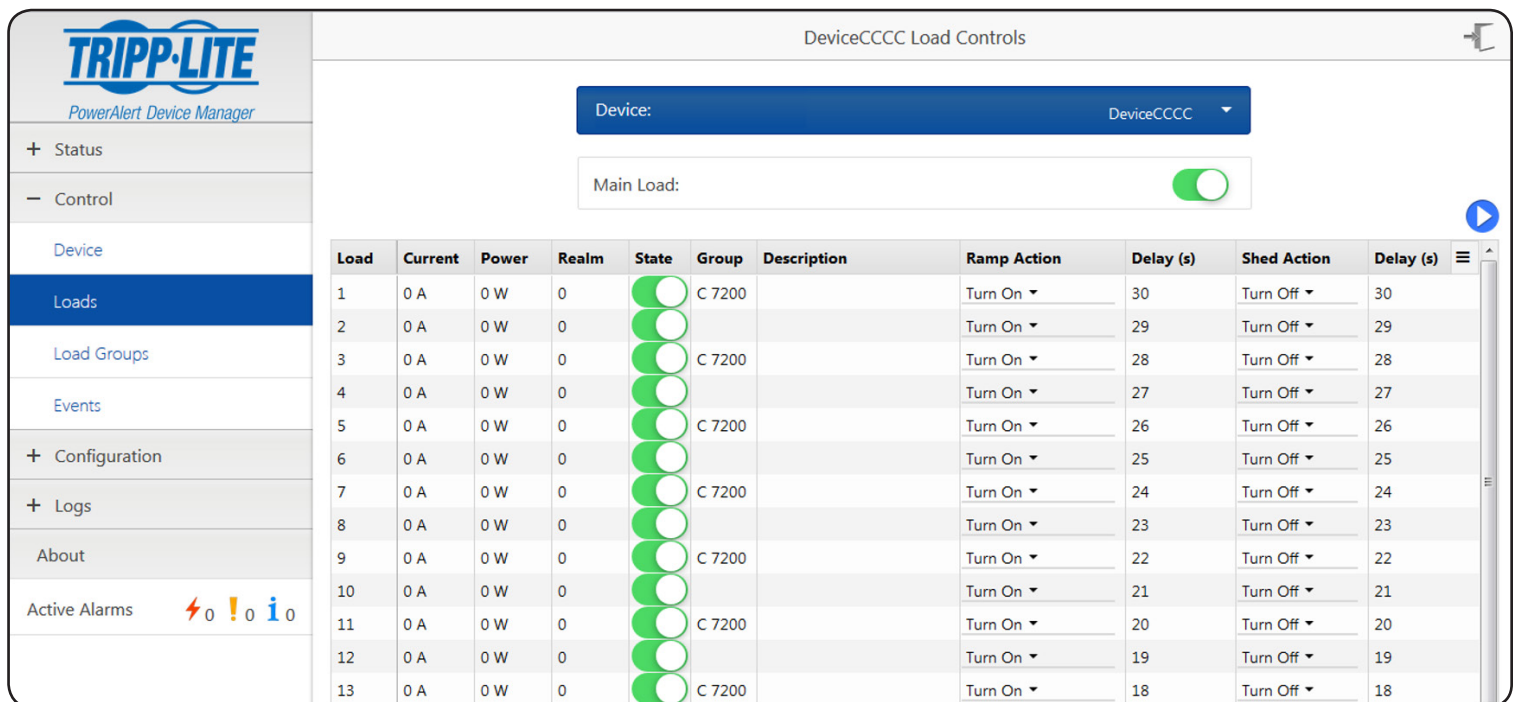


Figure 3-9: Loads Page

3. The Web Interface

3.3.3 Control/Load Groups

The Load Groups page (Figure 3-10) is used to create and control groups of outlets on select devices that have two or more controllable loads. Click the [+] button to create a new load group, configure it accordingly, then click the [Save] button to store it. Click the [x] to delete an existing load group and click the [Save] button to remove it permanently.

Note: An individual load can only be a member of a single Load Group.

As on the Loads page, the loads in a Load Group can be turned On, Off, or set to Cycle as a group. Refer to the Loads page for additional information on Load Group control. The state switch will change to blue and the switch position will be in the center if the loads in the group are not all in the same state. Refer to Figure 3-11 to see two loads in the “Even Loads” group “Off” state and Figure 3-12 to see how this is represented in the Load Groups page.

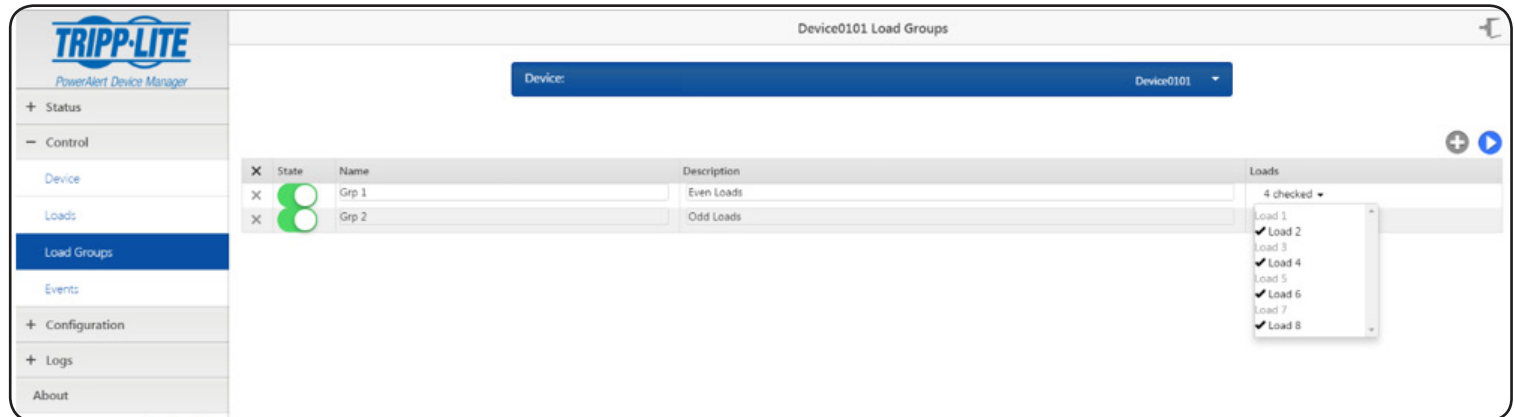


Figure 3-10: Load Groups Page

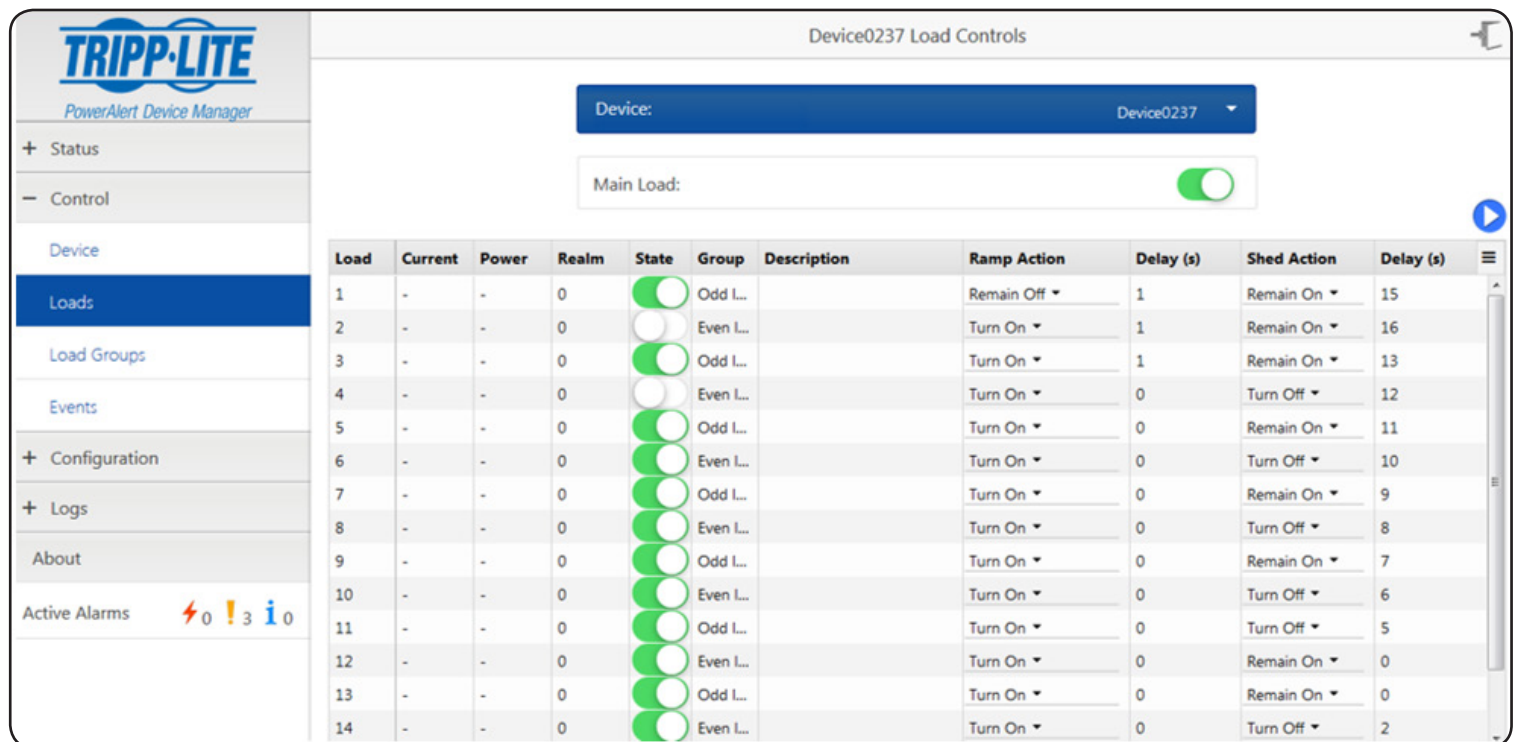


Figure 3-11: Loads in Mixed States

3. The Web Interface

Device0237 Load Groups

Device: Device0237

State	Name	Description	Loads
checked	Odd loads	odds	8 checked
checked	Even loads	evens	8 checked

Figure 3-12: Load Group with Loads in Mixed States

3.3.4 Control/Events

The Events page displays events supported by the selected device (Figure 3-13 and Figure 3-14). This list will vary by device model. Use the sliders to enable or disable notifications for each of the event types. Use the dropdown menu in the Category column to set the priority: Information, Warning or Critical. Click the [Save] button at any time to apply your changes.

Device0001 Events

Device: Device0001

Enabled	Category	Name
☒	Information	Battery Age Above Threshold
☒	Warning	Battery Capacity Below Warning Level
☒	Critical	Battery Low
☒	Information	Communications Lost
☒	Warning	Load 01 Off
☒	Warning	Load Level Above Threshold
☒	Warning	Loads Not All On
☒	Warning	NTP Watchdog NTP Probe Failed
☒	Warning	On Battery
☒	Critical	Output Off
☒	Critical	Overload
☒	Warning	Ping Watchdog Ping Probe Failed
☒	Warning	Self Test Failed
☒	Warning	Temperature High

Active Alarms: 0 Critical, 0 Warning, 0 Information

Figure 3-13: Events Page

Sensor0012 Events

Device: Sensor0012

Enabled	Category	Name
☒	Critical	Temperature Beyond Limits
☒	Critical	Contact Input 2 In Alarm
☒	Critical	Contact Input 1 In Alarm
☒	Choose...	Communications Lost

Choose...
Information
Warning
Critical

Figure 3-14: Setting Event Severity

3. The Web Interface

3.4 Configuration

The Configuration menu group contains seven submenus: Device Settings, Contacts, Network, Actions, Scheduling, Security and Log Settings (Figure 3-15). The available configuration options will vary by device.

3.4.1 Configuration / System Settings

System-level settings will include Watchdog configuration options, selection of the default time source and time zone offset.

The screenshot displays the 'System Device Settings' interface. On the left is a sidebar with navigation links: Status, Control, Configuration (expanded), Device Settings (selected), Contacts, Network, Actions, Scheduling, Security, Log Settings, Logs, and About. Below the sidebar, 'Active Alarms' are shown with 1 warning, 2 info, and 0 error icons.

The main content area is titled 'System Device Settings' and includes two dropdown menus: 'Device:' set to 'System' and 'Function:' set to 'Device Properties'. Below these are three sections:

- Watchdog Probe**: A section for configuring the Watchdog Probe.
- NTP Probe**: A table for NTP Probe settings.
- Ping Probe**: A table for Ping Probe settings.

At the bottom is a table for Date/Time settings.

Date/Time	Value
Current UTC Time	2016-03-07 23:16:40
Current Local Time	2016-03-07 17:16:40
Time Source	Network ▼
NTP Source (Primary)	0.pool.ntp.org
NTP Source (Secondary)	1.pool.ntp.org
UTC Time	23:16:40
UTC Date	2016-03-07
Time Zone Offset	Etc/UTC ▼

Figure 3-15: Configuration Menu

The Watchdog Probe function allows the network interface of the LX Platform device to reboot itself if it loses network communication. This reboot will not affect functionality of the LX device; for example, a PDU will continue distributing power through its outlets while the interface reboots.

- **Active** – Enables or disables the probe.
- **Period** -- The number of minutes between probe attempts. The range of valid values is 3 to 1440.
- **Attempts** -- The number of consecutive probes after which, if unsuccessful, the interface reboot will be triggered. The range of valid values is 3 to 10.
- **Primary address** – The IPv4 address of the primary probe target or the Fully Qualified Domain Names (FQDN). For the NTP Probe, the IPv4 address or FQDN of the NTP server should be entered.
- **Primary port** – The port number of the primary probe target (NTP server).
- **Secondary address** – The IPv4 address or the FQDN of the secondary probe target. This can be optionally set as a means to double-check if network connectivity was lost. If probes to the primary address fail, but probes to the secondary address are successful, the reboot will not be triggered.

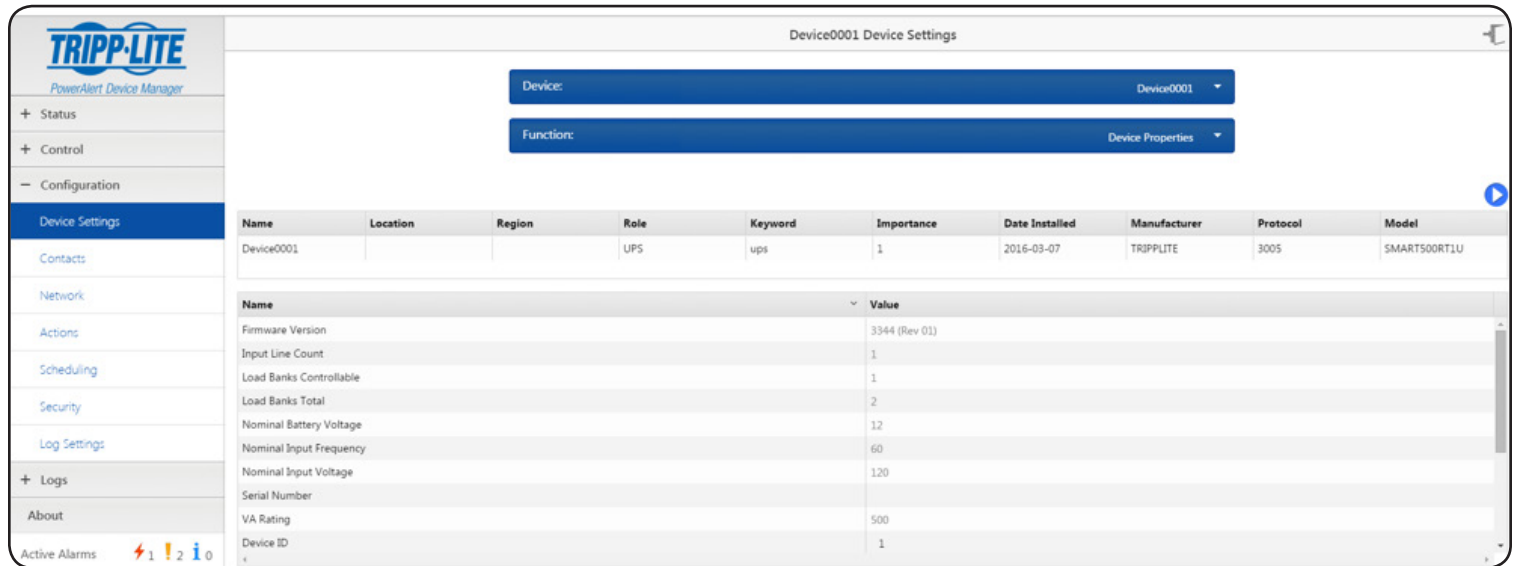
The Time Source choices are Network and RTC. If Network is chosen, enter the Primary NTP Source (and Secondary NTP Source, if desired) in the appropriate fields. The default Time Zone Offset is UTC; to change this, select the desired selection from the pulldown menu. Ensure that you click on the [Save] icon after entering or editing these fields.

The default Ping and NTP watchdog probe events are configured to log to the event log and reboot the card 30 seconds after the event is detected. Probes will become active once they complete a successful handshake with the remote host. An unsuccessful handshake will be captured in the event log, as well as the Telnet/SSH for Auto Probes status.

3. The Web Interface

3.4.2 Configuration/Device Settings

The Device Settings page displays the settings of the selected device. Select the device to configure and choose Device Properties (Figure 3-16) or Device Thresholds (Figure 3-17) from the Function dropdown menu. Click the [Save] button at any time to apply the selected settings. To configure a UPS for operation with external battery packs, use the External Battery Pack Configuration Utility (downloadable from the Tripp Lite website).

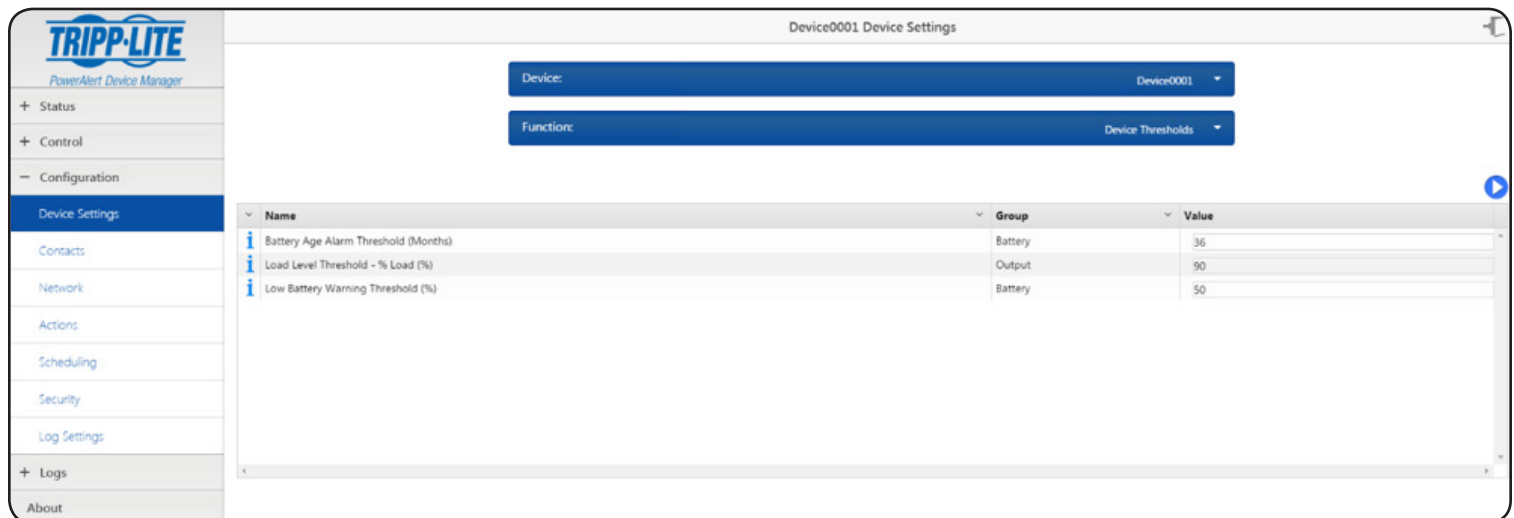


The screenshot shows the 'Device0001 Device Settings' page. On the left is a navigation menu with options: Status, Control, Configuration, Device Settings (selected), Contacts, Network, Actions, Scheduling, Security, Log Settings, Logs, and About. The main content area has two dropdown menus: 'Device:' set to 'Device0001' and 'Function:' set to 'Device Properties'. Below these is a table with device information.

Name	Location	Region	Role	Keyword	Importance	Date Installed	Manufacturer	Protocol	Model
Device0001			UPS	ups	1	2016-03-07	TRIPPLITE	3005	SMART500RTIU

Name	Value
Firmware Version	3344 (Rev 01)
Input Line Count	1
Load Banks Controllable	1
Load Banks Total	2
Nominal Battery Voltage	12
Nominal Input Frequency	60
Nominal Input Voltage	120
Serial Number	
VA Rating	500
Device ID	1

Figure 3-16: Device Properties



The screenshot shows the 'Device0001 Device Settings' page with the 'Function:' dropdown set to 'Device Thresholds'. The main content area displays a table of thresholds.

Name	Group	Value
Battery Age Alarm Threshold (Months)	Battery	36
Load Level Threshold - % Load (%)	Output	90
Low Battery Warning Threshold (%)	Battery	50

Figure 3-17: Device Thresholds

3. The Web Interface

3.4.3 Configuration/Contacts

The Contacts page is used to configure Email, SNMP V1, SNMP V2c, SNMP V3, HTTP and HTTPS contacts (Figure 3-18).

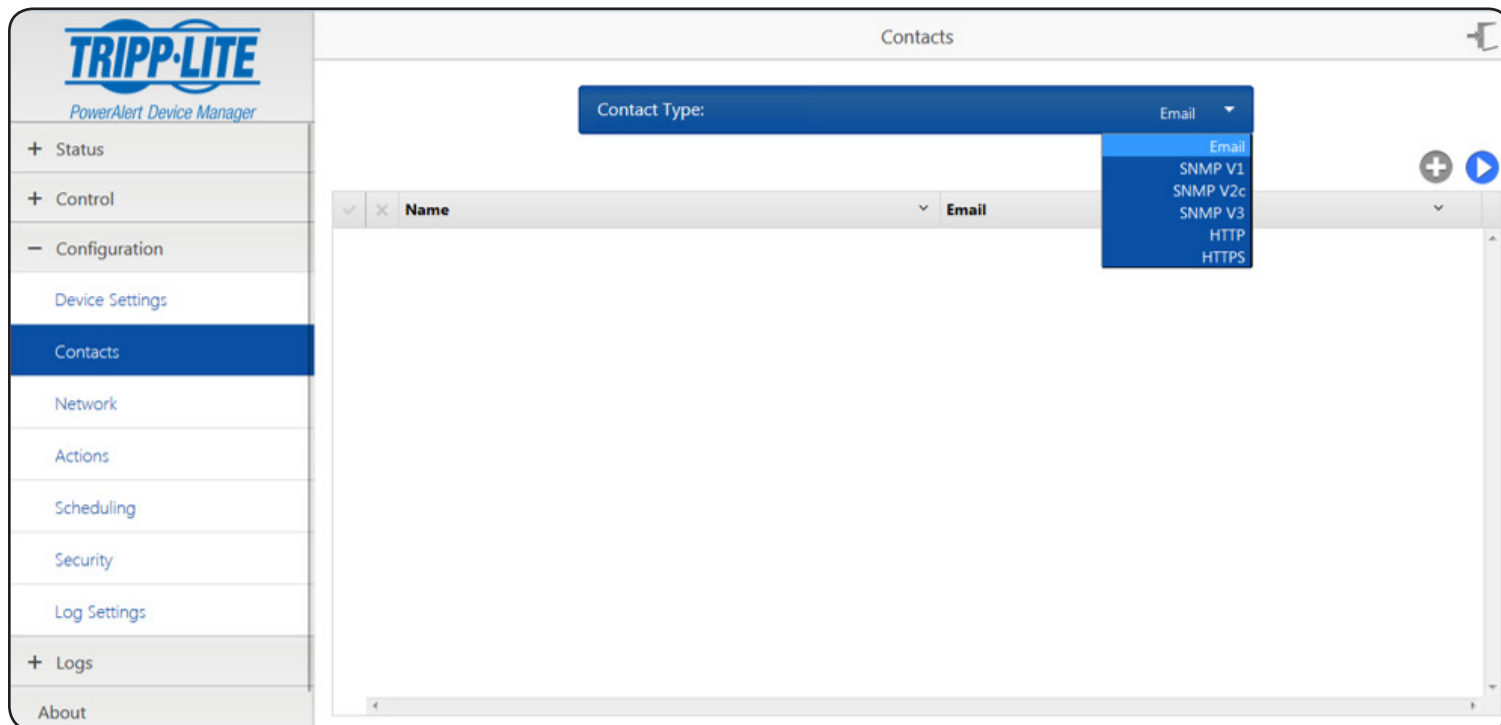


Figure 3-18: Contacts Page

3.4.3.1 Email

Before PowerAlert Device Manager can send email notifications with rotated log contents, email actions and other system data, there must be at least one email contact. To create a new email contact, select Email from the dropdown menu and click the [+] button. Enter a unique name for the contact name field; enter a unique contact email address in the email field. Click the [Save] button at any time to apply the settings. The same procedure can be used to edit an existing contact. Start by selecting the row you wish to edit by clicking the [✓]. To remove an existing contact, click the [✗] to the left of the Contact Name (Figure 3-19). Common email services such as Gmail, Yahoo! Mail and Hotmail are supported. Test emails can be sent to each email contact through the Telnet/SSH interface. Refer to **Section 4.2.1.1** for details.

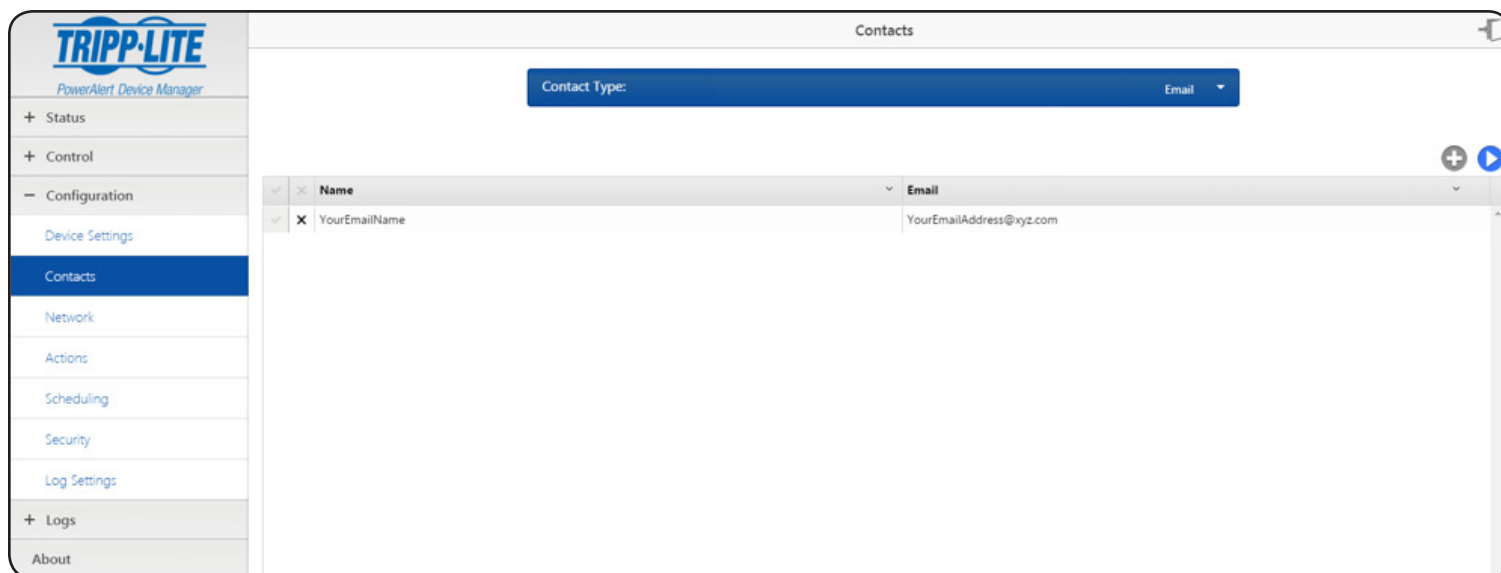
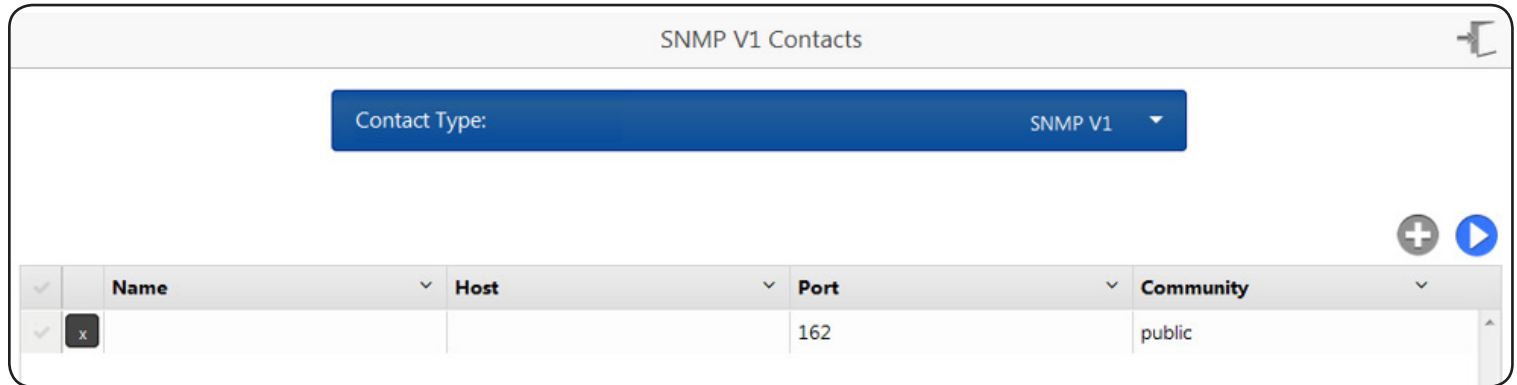


Figure 3-19: Creating a New Email Contact

3. The Web Interface

3.4.3.2 SNMP V1

The SNMP V1 page displays a list of SNMP V1 contacts. Before PowerAlert Device Manager can send an SNMP trap or an SNMP set to an IP address, there must be at least one SNMP contact. To create a new SNMP V1 contact, select SNMP V1 from the dropdown menu and click the [+] button (Figure 3-20). Enter a name for the contact in the Name field; enter the host in the host IP address field. The Port and Community fields will default to Port 162 and Community “public”. To make a change to either of the defaults, click the field and edit the contents. Click the [Save] button at any time to apply the settings. The same procedure can be used to edit an existing contact. Start by selecting the row you wish to edit by clicking on the [✓]. To remove an existing contact, click the [X] to the left of the Contact Name. By default, adding an SNMP contact will automatically make it a recipient of alarm traps, which are sent 30 seconds after the alarm is detected.

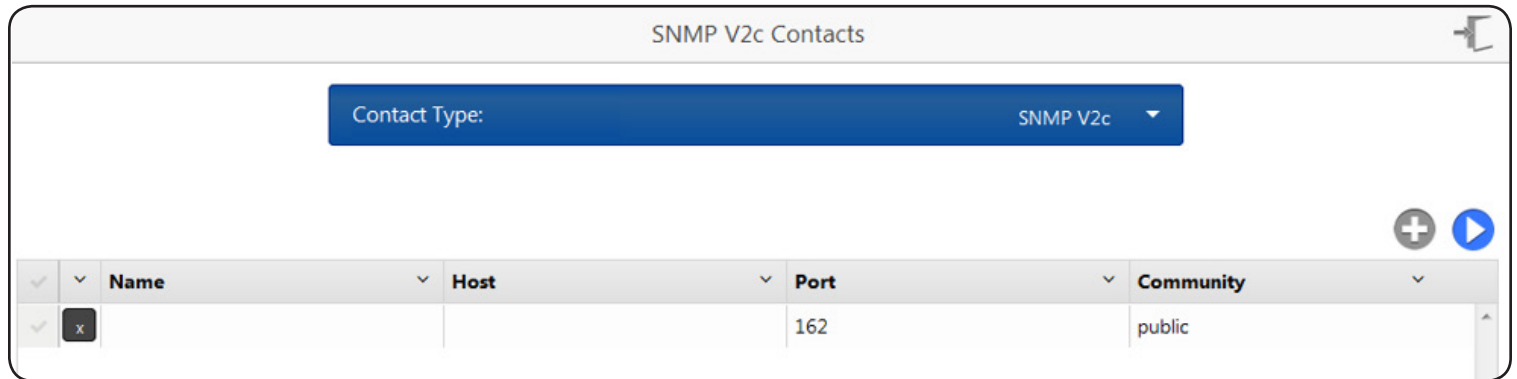


	Name	Host	Port	Community
x			162	public

Figure 3-20: Creating an SNMP V1 Contact

3.4.3.3 SNMP V2c

The SNMP V2c page displays the list of SNMP V2c contacts. To create a new SNMP V2c contact, select SNMP V2c from the dropdown menu and click the [+] button (Figure 3-21). Enter a name for the contact in the Name field; enter the host in the host IP address field. The Port and Community fields will default to Port 162 and Community “public”. To make a change to either of the defaults, click the field and edit the contents. Click [Save] at any time to apply the settings. The same procedure can be used to edit an existing contact. Start by selecting the row you wish to edit by clicking on the [✓]. To remove an existing contact, click the [X] to the left of the Contact Name.



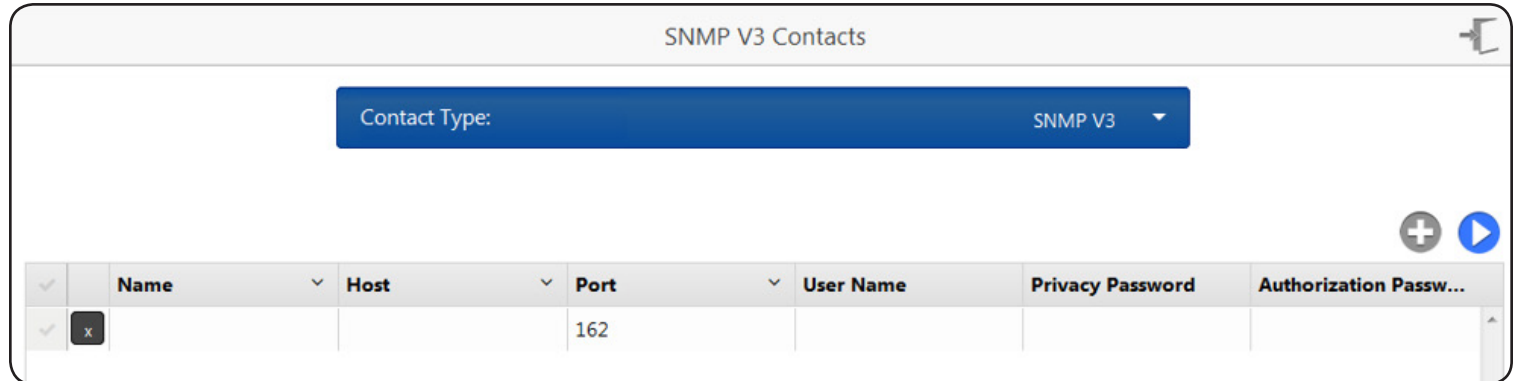
	Name	Host	Port	Community
x			162	public

Figure 3-21 Creating an SNMP V2c Contact

3. The Web Interface

3.4.3.4 SNMP V3

The SNMP V3 page displays a list of SNMP V3 contacts. To create a new SNMP V3 contact, select SNMP V3 from the dropdown menu and click the [+] button (Figure 3-22). Click on the name field to enter the contact name. Click on the Host field and enter the host IP address for the contact. The Port contents will default to 162. To make a change, click on the field to edit the contents. User Name, Privacy Password and Authorization Password can be modified by clicking and typing the field for each option. Click the [Save] button at any time to apply the settings. To edit an existing SNMP V3 contact, click on the field for name, host, port, User Name, Privacy Password and Authorization Password to make changes. To remove an existing SNMP V3 contact, click the [X] on the left hand side of the table.

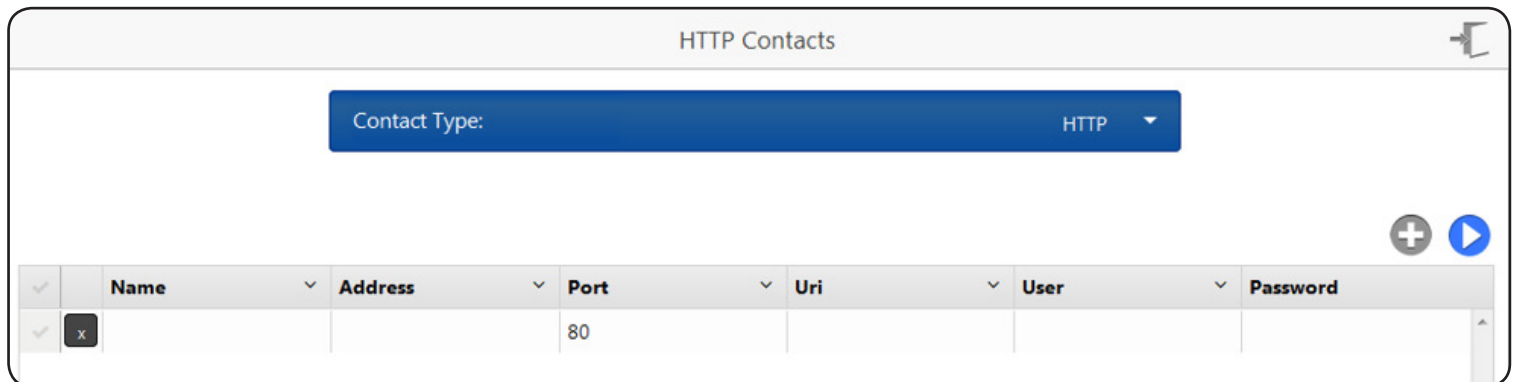


	Name	Host	Port	User Name	Privacy Password	Authorization Passw...
☒			162			

Figure 3-22: Creating an SNMP V3 Contact

3.4.3.5 HTTP

The HTTP page displays a list of the HTTP contacts. To create a new HTTP contact, select HTTP from the dropdown menu and click the [+] button (Figure 3-23). Click on the name field to enter the contact name. Click on the Address field and enter the Address for the contact. The Port contents will default to 80. To make a change, click on the field to edit the contents. Uri, User and Password can be modified by clicking the field for each option. Click the [Save] button at any time to apply the settings. To edit an existing HTTP contact, click on the textbox to make changes. To remove an existing HTTP contact, click the [X] on the left hand side of the table.



	Name	Address	Port	Uri	User	Password
☒			80			

Figure 3-23: Creating an HTTP Contact

3. The Web Interface

3.4.3.6 HTTPS

The HTTPS page displays a list of HTTPS contacts. To create a new HTTPS contact, select HTTPS from the dropdown menu and click the [+] button (Figure 3-24). Click on the name field to enter the contact name. Click on the Address field and enter the Address for the contact. The Port contents will default to 443. To make a change, click on either field to edit the contents. Uri, User and Password can be modified by clicking the field for each option. Click the [Save] button at any time to apply the settings. To edit an existing HTTPS contact, click on the field to make changes. To remove an existing HTTPS contact, click the [X] on the left hand side of the table.

	Name	Address	Port	Uri	User	Password
☒			443			

Figure 3-24: Creating an HTTPS Contact

3.4.3.7 Configuration/Network

Configuration of the LX Platform device Network Services, SMTP, Internet and Domain are accessed through the Network Page (Figure 3-25).

TRIPP-LITE
PowerAlert Device Manager

Network

Network: Services

Services
SMTP
Internet
Domain

SNMP Settings

AutoStart ☒

Port 161

V1 ☒

V2 ☒

V3 ☒

HTTP/HTTPS Settings

HTTP Auto Start ☒

HTTP Port 80

HTTPS Auto Start ☒

HTTPS Port 443

SSH Settings

Figure 3-25: Network Page

3. The Web Interface

3.4.3.8 Configuration/Network/Services

The Services option displays SNMP Settings, HTTP/HTTPS Settings, SSH Settings and Telnet settings. Use the sliders to enable or disable each available option. Click the Port field to add/edit the port number. Click the [Save] button to apply settings at any time (Figure 3-26).

The screenshot shows the 'Network' configuration page in the Tripp-Lite PowerAlert Device Manager. The left sidebar contains navigation links: Status, Control, Configuration (expanded), Device Settings, Contacts, Network (selected), Actions, Scheduling, Security, Log Settings, Logs, and About. The main content area is titled 'Network' and features a dropdown menu set to 'Services'. Below this, there are four sections of settings, each with a toggle switch and a port number field:

- SNMP Settings:** AutoStart (enabled), Port (161), V1 (enabled), V2 (enabled), V3 (enabled).
- HTTP/HTTPS Settings:** HTTP Auto Start (enabled), HTTP Port (80), HTTPS Auto Start (enabled), HTTPS Port (443).
- SSH Settings:** Auto Start (enabled), Port (22).
- Telnet Settings:** Auto Start (enabled), Port (23).

At the bottom left, there is a status bar showing 'Active Alarms' with icons for fire, lightning, and information.

Figure 3-26: Network Services Settings

3.4.3.9 Configuration/Network/SMTP

The SMTP settings page displays SMTP and Authentication Settings. To use a specific on-premise SMTP server or 3rd party SMTP server (Gmail, Yahoo! Mail, etc.), enter the appropriate SMTP settings for that server. To add or modify the SMTP settings, click on each available field. Use the sliders to enable the options available in Authentication settings. Click the [Save] button to apply settings at any time (Figure 3-27).

The screenshot shows the 'SMTP Network Settings' configuration page in the Tripp-Lite PowerAlert Device Manager. The left sidebar is identical to the previous figure, with 'Network' selected. The main content area is titled 'SMTP Network Settings' and features a dropdown menu set to 'SMTP'. Below this, there are two sections of settings:

- SMTP Settings:** Relay Address (text field), Relay Port (25), Relay User (text field), Relay Password (text field), From (poweralert@tripplite.com), Subject (PowerAlert Notification).
- Authentication Settings:** CRAM-MD5 (enabled), DIGEST-MD5 (enabled), Login (enabled), Plain (enabled).

At the bottom left, there is a status bar showing 'Active Alarms' with icons for fire, lightning, and information.

Figure 3-27: SMTP Settings

3. The Web Interface

3.4.3.10 Configuration/Network/Internet

The Internet Network Settings page displays both IPv4 and IPv6 settings (Figure 3-28). Select DHCP, static or stateless (IPv6 only) from the dropdown menu for Method and enter the address information for the other options. Click the [Save] button at any time to apply the current settings.

The screenshot shows the 'Internet Network Settings' page. On the left is a sidebar with the Tripp-Lite logo and a menu: Status, Control, Configuration (expanded), Device Settings, Contacts, Network (selected), Actions, Scheduling, Security, Log Settings, Logs, and About. At the bottom of the sidebar, it shows 'Active Alarms' with 0 icons. The main content area has a title bar 'Internet Network Settings' and a dropdown menu 'Network: Internet'. Below this are two sections: 'IPv4 Settings' and 'IPv6 Settings'. Each section has a 'Method' dropdown set to 'Dhcp'. The IPv4 settings include fields for Address (10.22.0.123), Subnet (255.224.0.0), Gateway (10.0.0.1), Manual DNS (disabled), Primary DNS (10.0.0.11), and Secondary DNS (10.0.0.8). The IPv6 settings include fields for Address (::0), Prefix (0), Gateway (::0), Manual DNS (disabled), Primary DNS (fc00::2), and Secondary DNS (::0). A blue play button is in the top right corner.

Figure 3-28: Internet Settings

3.4.3.11 Configuration/Network/Domain

The Domain page displays both host and domain information. Click on the field for each option to change the settings (Figure 3-29). Click the [Save] button at any time to apply the current settings.

The screenshot shows the 'Domain Network Settings' page. It has a title bar 'Domain Network Settings' and a dropdown menu 'Network: Domain'. Below this is a 'Domain Settings' section with two rows: 'Host' and 'Domain', each with an input field. A blue play button is in the top right corner.

Figure 3-29: Domain Settings

3. The Web Interface

3.4.4 Configuration/Actions

The system allows the user to define actions to be executed when events occur or are cleared. The actions may be to send email, send an SNMP trap, set a value via SNMP, execute a control, execute a load control, start a ramp or shed action, or shutdown a device. The actions available vary by device. Refer to Figure 3-30 for an overview of the Action Types.

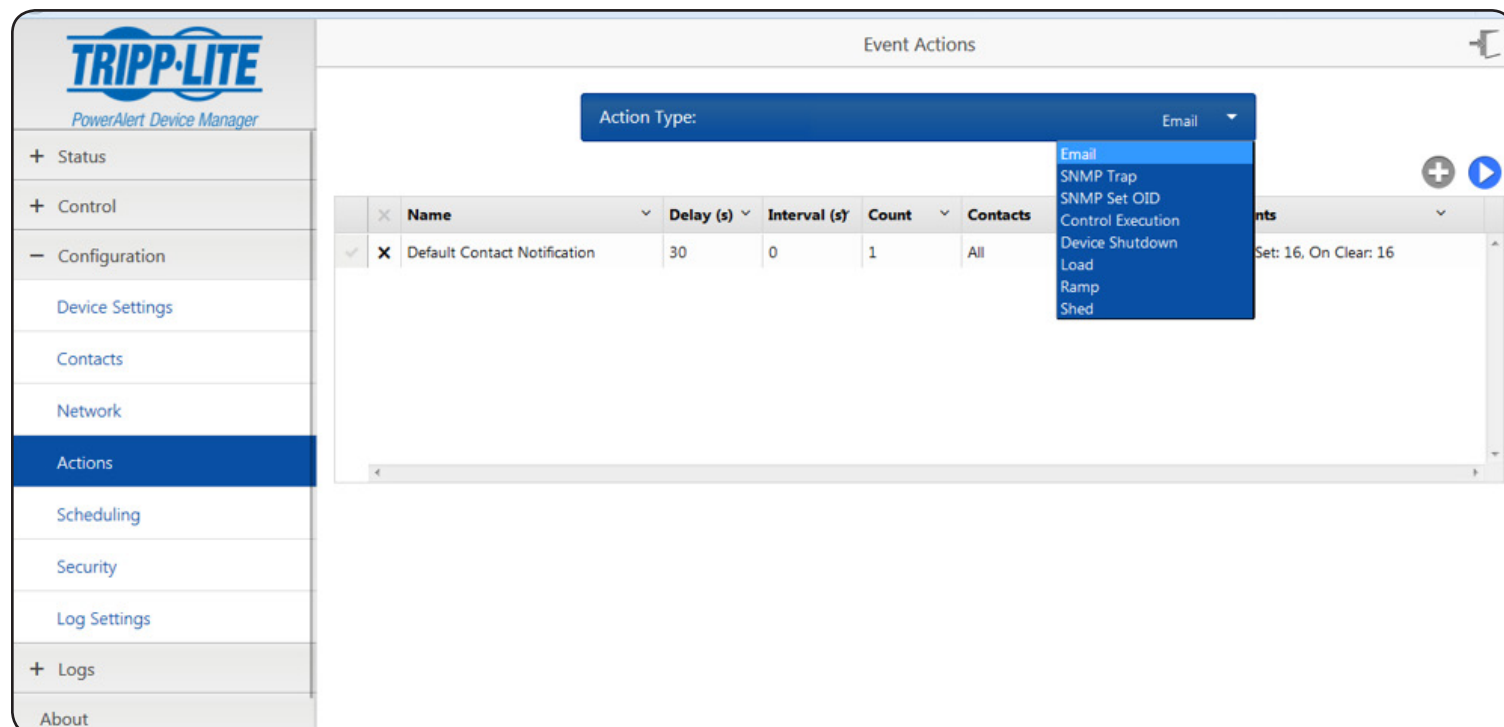


Figure 3-30: Configuring Event Actions

3.4.4.1 Defining Action Types

The following data items are common across many action types:

1. **Name:** Name of the action. This name must be unique across all action types.
2. **Delay:** The amount of time after the triggering event occurs before the action is performed. If the event clears before the delay time has elapsed, the action will not be performed.
3. **Interval:** Some action types allow the action to be performed repeatedly. For those action types, this attribute defines the amount of time to wait before the action is performed again. When the action is to be performed only once, this value is 0.
4. **Count:** This defines the number of times the action will be performed. When the interval is 0, the Count must be 1. A value of 0 means that the action will be repeated until the event is cleared.
5. **Events:** The events that will trigger the action to be performed. This can be when the event occurs or when the event clears.

3. The Web Interface

3.4.4.1.1 Configuration/Action/Email

This action type will send an email when the event occurs or clears. Before defining an Email Action, Email Contacts to receive the email message must already exist. Refer to section 3.4.3 for details. Choose the “All” option in the Contacts column to send the email to all contacts when the event occurs.

Email actions support a repeat option. You can choose the interval and count options to repeat sending the email until the event clears. Repeat does not apply when the action is triggered by the event clearing.

The Actions page displays the event actions for each device. The event action types are SNMP Set OID, SNMP Trap and Email (Figure 3-31).

The screenshot shows the 'Event Actions' configuration page in the Tripp-Lite PowerAlert Device Manager. The left sidebar contains a navigation menu with options: Status, Control, Configuration, Device Settings, Contacts, Network, Actions (highlighted), Scheduling, Security, Log Settings, Logs, and About. The main content area has two dropdown menus: 'Device:' set to 'System' and 'Action Type:' set to 'Email'. Below these is a table with the following columns: Name, Delay, Interval, Count, Contacts, and Events. A single row is visible with the following data: Name: Default Contact Notification, Delay: 30, Interval: 0, Count: 1, Contacts: All, Events: On Set: 29, On Clear: 29. There are '+' and '-' icons in the top right corner of the table area.

Name	Delay	Interval	Count	Contacts	Events
Default Contact Notification	30	0	1	All	On Set: 29, On Clear: 29

Figure 3-31: Email Actions

3.4.4.1.2 Configuration/Action/SNMP Set OID

The SNMP Set OID page displays the current SNMP Set OID event actions. To add a new event action, click the [+] button and select the event parameters. Click the [Save] button to save the current settings at any time (Figure 3-32).

Note: Only SNMPv1 contacts are supported for SNMP Set OID actions.

The screenshot shows the 'Event Actions' configuration page in the Tripp-Lite PowerAlert Device Manager. The left sidebar contains a navigation menu with options: Status, Control, Configuration, Device Settings, Contacts, Network, Actions (highlighted), Scheduling, Security, Log Settings, Logs, and About. The main content area has two dropdown menus: 'Device:' set to 'System' and 'Action Type:' set to 'SNMP Set OID'. Below these is a table with the following columns: Name, Delay, Interval, Count, Oid, Value, Contacts, and Events. The table is currently empty. There are '+' and '-' icons in the top right corner of the table area.

Name	Delay	Interval	Count	Oid	Value	Contacts	Events
------	-------	----------	-------	-----	-------	----------	--------

Figure 3-32: SNMP Set OID Event Actions

3. The Web Interface

3.4.4.1.3 Configuration/Action/SNMP Trap

The SNMP Trap page displays the current SNMP Trap event actions. To add a new event action, click the [+] button and select the event parameters. Click the [Save] button to save the current settings at any time (Figure 3-33).

Name	Delay	Interval	Count	Contacts	Events
Default Trap Notification	30	0	1	All	On Set: 29, On Clear: 29

Figure 3-33: SNMP Trap Event Actions

3.4.5 Configuration/Scheduling

The Scheduling page is used to schedule tasks for a selected device. Start by selecting the device and the desired task from the list of tasks supported by your device (Figure 3-34). Select the frequency of execution and configure how long the schedule should repeat, if desired (Figure 3-35). Click the [Save] button to save the current settings at any time.

An existing schedule cannot be edited, but if you select the schedule you wish to modify, make the desired changes, and save it, a new schedule will be created, and the existing one can simply be deleted. To remove an existing schedule, click the [x] on the left-hand side of the table. The selected schedule will be removed. It is not necessary to click the [Save] button.

Task	Start Date	End Date	End After	Frequency
Turn All Loads On	3/17/2016 13:40	3/17/2016 19:00		Daily
Initiate Self Test	3/20/2016 14:00			Weekly

Figure 3-34: Scheduling Tasks

3. The Web Interface

Device0001 Scheduling

Task: Initiate Self Test

☐ Once
 ☐ Daily
 ☒ Weekly
 ☐ Monthly
 ☐ Yearly

Repeat every 1 week(s) on:

☒ Sun
 ☐ Mon
 ☐ Tue
 ☐ Wed
 ☐ Thu
 ☐ Fri
 ☐ Sat

Begin at 14:00 on March 20 2016

☒ Repeat forever
 ☐ Repeat 1 Time(s)
 ☐ Repeat until March 18 2016

Figure 3-35: Setting Task Frequency and Repeat Rate

3.4.6 Security

The Security page displays options to assign users [set up SNMP access/default communities], change the password, change AAA settings and change Radius server settings (Figure 3-36). Community names are entered in the “Name” column.

Note: The default “tripplite” community is also used by Tripp Lite’s PowerAlert Network Shutdown Agent (PANSA)—any change to its name or inactivating it may cause issues when using PANSA.

All users can access the password page. Only administrator-level users can access the other menu options. For names and passwords, alphanumeric and the following special characters are allowed: !@#\$\$%^*(){}~_-. Names must be a minimum of 6 characters; passwords must be a minimum of 8 characters. Click the [Save] button to save the current settings at any time.

Security

Settings: User

×	Status	Protocol	Name	Password	Auth Password	IP Address	IP Mask	Role	Realms	Expiration	Idle Timeout
×	Active	V3	localadmin	*****	*****	::	::	administrator		0	0
×	Active	V3	localmanager	*****	*****	::	::	manager		0	0
×	Active	V3	localguest	*****	*****	::	::	read-only		0	0
×	Active	V1	public			::	::	read-only		0	0
×	Active	V2c	tripplite			::	::	manager		0	0
×	Inactive	None				::	::	read-only		0	0
×	Inactive	None				::	::	read-only		0	0
×	Inactive	None				::	::	read-only		0	0
×	Inactive	None				::	::	read-only		0	0
×	Inactive	None				::	::	read-only		0	0
×	Inactive	None				::	::	read-only		0	0
×	Inactive	None				::	::	read-only		0	0

Figure 3-36: Security Page

3. The Web Interface

3.4.7 Configuration/Log Settings

The Log Settings page is used to configure the log rotation options for the supported log types: Accounting, Data and Events (Figure 3-37). A maximum of 1024 lines will be stored in any of the logs before the log automatically rotates. The size of the log can be adjusted; the minimum is 64 lines and the maximum is 1024 lines. The log format can be chosen; options are xml and csv. Use the [+] button to assign an existing HTTP or Email contact to receive the rotated logs (Figure 3-38). Click the [Save] button to save the settings at any time. In addition to log rotation settings, Syslog and Application log settings can be configured. The only setting for the Application log is the minimum severity level system message that should be logged (Figure 3-39). All higher-level messages will be logged automatically.

The screenshot shows the 'Accounting Log Settings' page. On the left is a navigation menu with the Tripp-Lite logo and the following items: Status, Control, Configuration (expanded), Device Settings, Contacts, Network, Actions, Scheduling, Security, Log Settings (selected), Logs, and About. The main content area has a title bar 'Accounting Log Settings'. Below it are three settings: 'Log:' with a dropdown menu showing 'Accounting' selected, 'Log Format:' with a dropdown menu showing 'Accounting' selected, and 'Log Size (Lines):' with a text input field containing '1024' and a small icon. At the bottom, there is a table with the header 'Contact To Receive Log Rotation Notifications' and a single row with 'Protocol' and 'Contact To Receive Log Rotation Notifications' columns. The table is empty. There are '+' and '-' buttons in the top right corner of the main content area.

Figure 3-37: Log Settings Page

The screenshot shows the 'Data Log Settings' page. On the left is a navigation menu with the Tripp-Lite logo and the following items: Status, Control, Configuration (expanded), Device Settings, Contacts, Network, Actions, Scheduling, Security, Log Settings (selected), Logs, and About. The main content area has a title bar 'Data Log Settings'. Below it are three settings: 'Log:' with a dropdown menu showing 'Data' selected, 'Log Format:' with a dropdown menu showing 'XML' selected, and 'Log Size (Lines):' with a text input field containing '1024' and a small icon. At the bottom, there is a table with the header 'Contact To Receive Log Rotation Notifications' and a single row with 'Protocol' and 'Contact To Receive Log Rotation Notifications' columns. The table contains one entry: 'Email' in the Protocol column and 'YourEmailName' in the Contact To Receive Log Rotation Notifications column. There are '+' and '-' buttons in the top right corner of the main content area.

Figure 3-38: Assigning a Contact to Receive Logs

3. The Web Interface

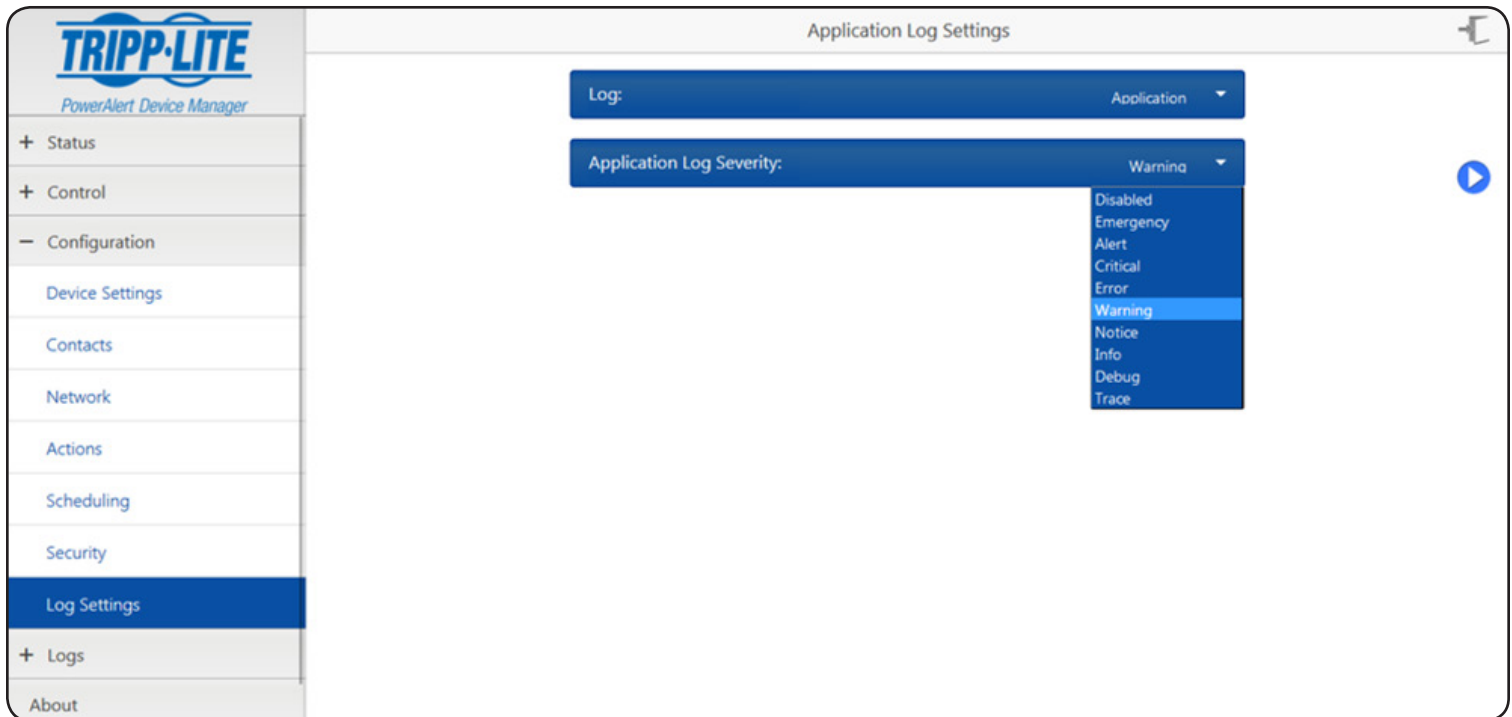


Figure 3-39: Setting Minimum Severity Level for Logging

3.5 Logs

The Logs menu group includes the Events, Data and Accounting Logs. The logs are loaded on demand and do not refresh automatically, so that the data you are looking at does not shift position as new information is added to the log. Refresh the page to see the most recent log entries. Each log can display up to a maximum of 1024 entries before it will automatically rotate the logs.

Click the Refresh icon  to update the selected log. Click the Rotate icon  to manually send the log via email or HTTP.

Note: Doing so clears the entries in the log.

Note: If there are no Contacts configured to receive rotated log files and the log fills up or you click on Rotate, the log data will be cleared. Once it is cleared it cannot be retrieved, so be sure to configure log rotation contacts prior to rotating the log if the historical system data is important to you.

Use the Device dropdown to filter the log to include only data from the selected device.

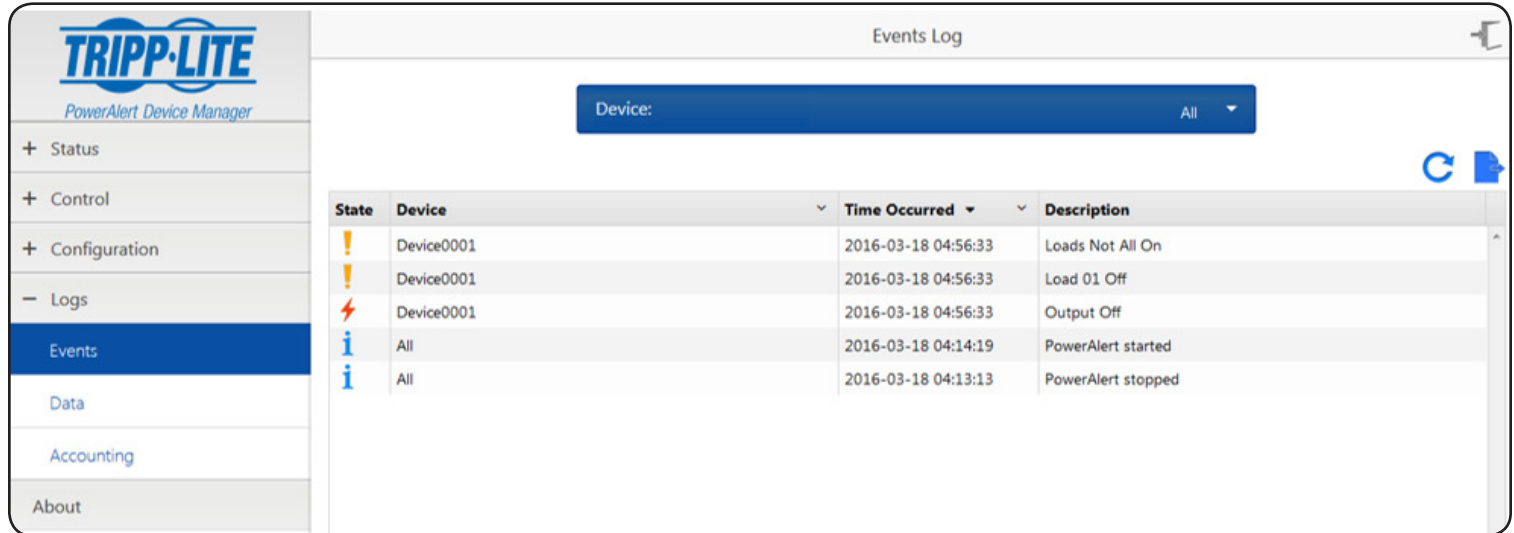
3. The Web Interface

3.5.1 Logs/Events Log

The Events Log displays the historical record of events that have occurred in the system. Select a device from the device dropdown menu to filter the log on the specific device (Figure 3-40).

By default, Events are displayed in reverse chronological order. Click the column header to change the sort criteria. The event state, the device it occurred on, and a description of the event are also displayed. To view more events, simply continue scrolling down through the log.

Note: Changes to sorting and filtering will not persist if you leave the log and return.



The screenshot shows the 'Events Log' window of the Tripp-Lite PowerAlert Device Manager. On the left is a sidebar with navigation links: Status, Control, Configuration, Logs (expanded), Events (selected), Data, Accounting, and About. The main area has a 'Device:' dropdown set to 'All'. Below this is a table of events.

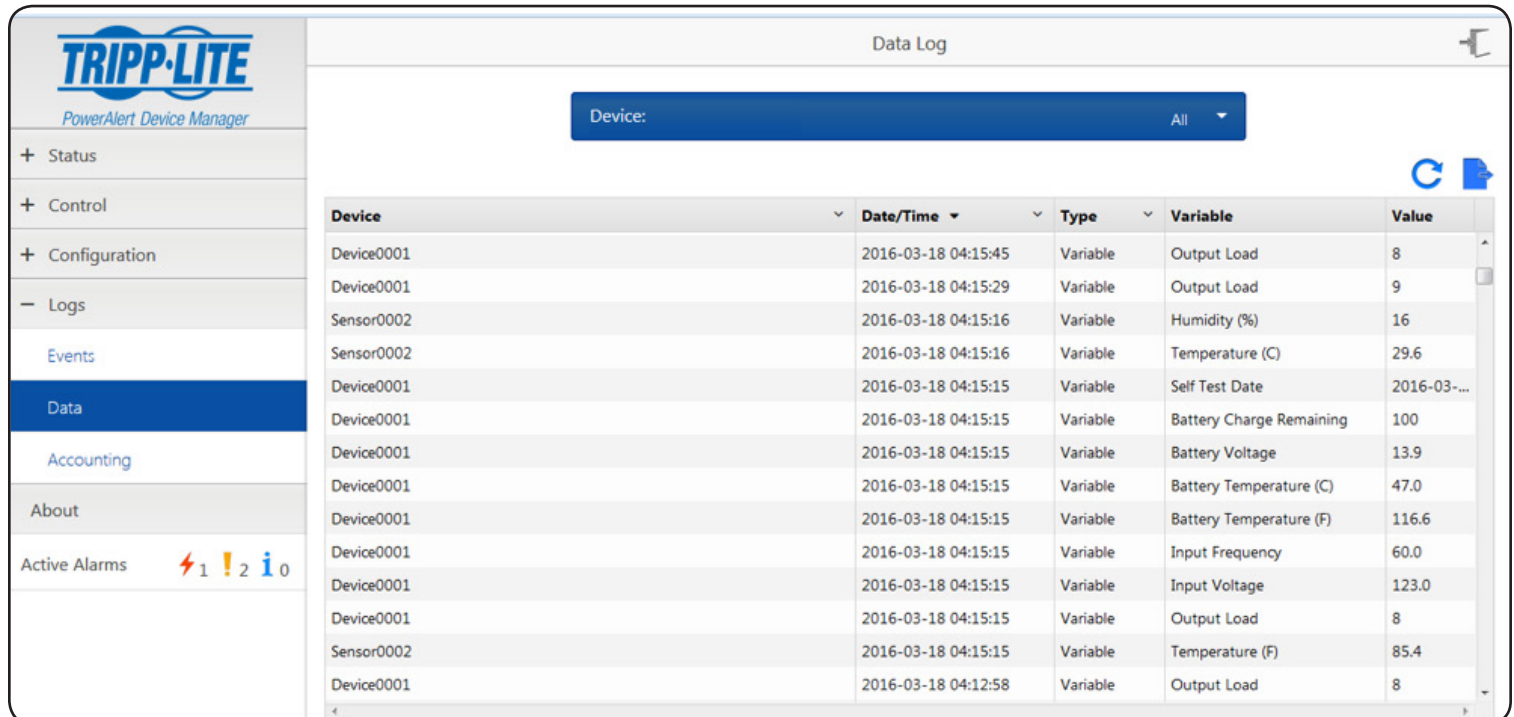
State	Device	Time Occurred	Description
!	Device0001	2016-03-18 04:56:33	Loads Not All On
!	Device0001	2016-03-18 04:56:33	Load 01 Off
⚡	Device0001	2016-03-18 04:56:33	Output Off
i	All	2016-03-18 04:14:19	PowerAlert started
i	All	2016-03-18 04:13:13	PowerAlert stopped

Figure 3-40: Events Log

3.5.2 Logs/Data Log

The Data Log displays the historical value of data points in reverse chronological order of the date and time the value was recorded by the system (Figure 3-41). The logging thresholds are fixed such that a change greater than the threshold value must be detected before a new value will be logged. Select a device from the device dropdown menu to filter the log on the specific device (Figure 3-42). Click the column header to change the sort criteria. Information on the data type, variable type, recorded value and the device it occurred on is also displayed. To view more data points, simply continue scrolling down through the log.

Note: Changes to sorting and filtering will not persist if you leave the log and return.



The screenshot shows the 'Data Log' window of the Tripp-Lite PowerAlert Device Manager. The sidebar is similar to the previous figure, but 'Data' is selected under the 'Logs' section. The main area has a 'Device:' dropdown set to 'All'. Below this is a table of data points.

Device	Date/Time	Type	Variable	Value
Device0001	2016-03-18 04:15:45	Variable	Output Load	8
Device0001	2016-03-18 04:15:29	Variable	Output Load	9
Sensor0002	2016-03-18 04:15:16	Variable	Humidity (%)	16
Sensor0002	2016-03-18 04:15:16	Variable	Temperature (C)	29.6
Device0001	2016-03-18 04:15:15	Variable	Self Test Date	2016-03-...
Device0001	2016-03-18 04:15:15	Variable	Battery Charge Remaining	100
Device0001	2016-03-18 04:15:15	Variable	Battery Voltage	13.9
Device0001	2016-03-18 04:15:15	Variable	Battery Temperature (C)	47.0
Device0001	2016-03-18 04:15:15	Variable	Battery Temperature (F)	116.6
Device0001	2016-03-18 04:15:15	Variable	Input Frequency	60.0
Device0001	2016-03-18 04:15:15	Variable	Input Voltage	123.0
Device0001	2016-03-18 04:15:15	Variable	Output Load	8
Sensor0002	2016-03-18 04:15:15	Variable	Temperature (F)	85.4
Device0001	2016-03-18 04:12:58	Variable	Output Load	8

Figure 3-41: Data Log Showing Historical Values

3. The Web Interface

TRIPP-LITE
PowerAlert Device Manager

Device: Device0001

Device	Date/Time	Type	Variable	Value
Device0001	2016-03-18 04:15:29	Variable	Output Load	9
Device0001	2016-03-18 04:15:15	Variable	Self Test Date	2016-03-...
Device0001	2016-03-18 04:15:15	Variable	Battery Charge Remaining	100
Device0001	2016-03-18 04:15:15	Variable	Battery Voltage	13.9
Device0001	2016-03-18 04:15:15	Variable	Battery Temperature (C)	47.0
Device0001	2016-03-18 04:15:15	Variable	Battery Temperature (F)	116.6
Device0001	2016-03-18 04:15:15	Variable	Input Frequency	60.0
Device0001	2016-03-18 04:15:15	Variable	Input Voltage	123.0
Device0001	2016-03-18 04:15:15	Variable	Output Load	8
Device0001	2016-03-18 04:12:58	Variable	Output Load	8
Device0001	2016-03-18 04:12:28	Variable	Output Load	9

Active Alarms: 1 ⚡ 2 ! 0 i

Figure 3-42: Filtering Log by Specific Device

3.5.3 Logs/Accounting Log

The Accounting Log operates on the same principle as the Events and Data Logs. It keeps track of changes made to the system, along with the date and time, the user who made the change and the origin (Figure 3-43).

TRIPP-LITE
PowerAlert Device Manager

Device: All

Date/Time	User	Origin	Event
2016-03-18 05:11:41	localadmin	10.22.0.6	update mainloads set execute=2 where id=1
2016-03-18 04:56:17	localadmin	10.22.0.6	update mainloads set execute=1 where id=1
2016-03-18 04:55:36	localadmin	10.22.0.6	login
2016-03-18 04:13:10	localadmin	10.22.0.6	logout
2016-03-18 04:13:09	localadmin	10.22.0.6	update restart set restartengine = 1
2016-03-18 04:12:42	localadmin	10.22.0.6	rotate eventlog
2016-03-18 03:44:08	localadmin	10.22.0.6	login
2016-03-18 03:43:03	localadmin	10.22.0.6	login
2016-03-18 02:45:01	localadmin	10.25.1.1	login
2016-03-18 02:42:44	localadmin	10.25.1.1	login
2016-03-18 02:40:15	localadmin	10.2.0.1	login
2016-03-18 02:27:15	localadmin	10.25.1.1	logout
2016-03-18 02:27:13	localadmin	10.25.1.1	update administration set softwareupdate=1
2016-03-18 02:25:50	localadmin	10.25.1.1	login

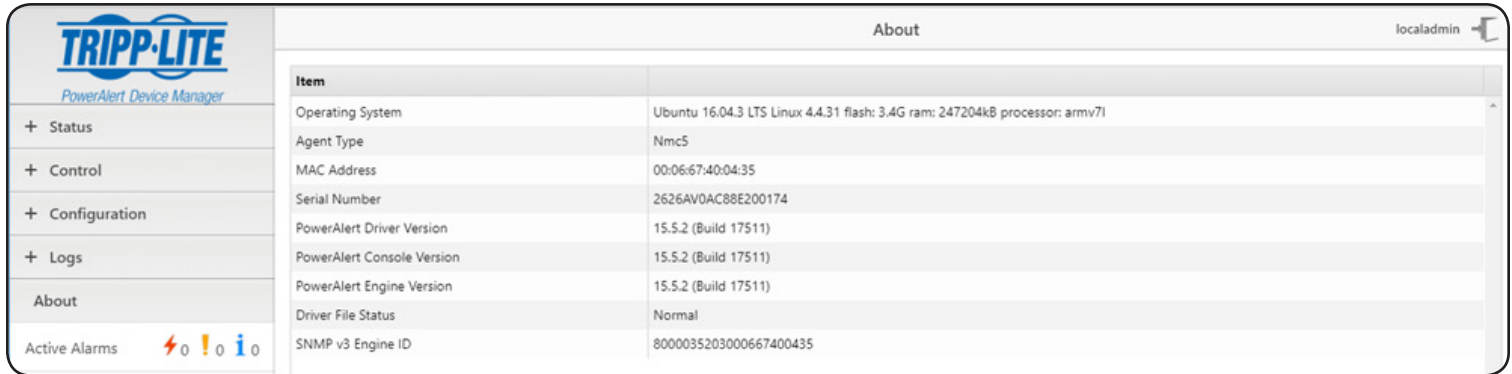
Active Alarms: 0 ⚡ 0 ! 0 i

Figure 3-43: Accounting Log

3. The Web Interface

3.6 About

The About page shows information about the LX Platform device, including its MAC Address, Serial Number and the PowerAlert Device Manager revision (Figure 3-44). The information on the About page is read-only.



The screenshot displays the 'About' page of the Tripp-Lite PowerAlert Device Manager web interface. The interface includes a sidebar on the left with navigation links: Status, Control, Configuration, Logs, and About. The main content area shows a table of system information.

Item	
Operating System	Ubuntu 16.04.3 LTS Linux 4.4.31 flash: 3.4G ram: 247204kB processor: armv7l
Agent Type	Nmc5
MAC Address	00:06:67:40:04:35
Serial Number	2626AV0AC88E200174
PowerAlert Driver Version	15.5.2 (Build 17511)
PowerAlert Console Version	15.5.2 (Build 17511)
PowerAlert Engine Version	15.5.2 (Build 17511)
Driver File Status	Normal
SNMP v3 Engine ID	8000035203000667400435

Figure 3-44: About Page

4. Telnet/SSH Console

Most of the monitoring and control features available in the Web interface (see **Section 3. The Web Interface**) are also available in the Telnet and/or SSH console. Accessing the LX Platform device through the Telnet/SSH console is ideal for mobile or resource-limited platforms.

Each menu can be thought of as one of four types: navigation, summary, detail and data collection.

Navigation Menus

Navigational menus allow a user to choose a path down the menu structure. Any data presented on these navigational menus are for information only and will require continuing down into a submenu to make any modifications.

Summary Menus

Data items that can have multiple instances will also have a summary menu. For example, the Email Recipients will have a summary menu. The summary will display a row for each member with a subset of the data for that object.

From the summary, a user may enter an ID number from the list to view/modify the detail menu for that item. If insert is allowed for the data, the user will be presented with the option to enter 'O' as well. When 'O' is chosen, the user is then automatically prompted to enter the individual detail menu items. Once all items have been entered, the user will be prompted to save the information, view the information, or abort the insert.

Detail Menus

The detail menus display the information about a collection of related individual data items. An example of a detail menu would be the menu for a single Email Recipient. From the detail menu, a user will be given the option to choose to modify the individual data items. When allowed, deletes will be done from the detail menus.

Some detail menus will immediately update the data as entered. Others will collect all the data changes and require the user to explicitly save the data in one operation. Those that require an explicit save will present an 'A' option to apply the changes. If a user has pending changes and attempts to leave the menu, an indication that the changes have not been saved will be presented and give the user the option to save or abort the changes.

Data Collection Menus

Data collection menus allow a user to enter values for an individual data item. For example, the menu to update an Email Recipient's email address would be a data collection menu. These menus do not have any submenus.

Menu Permissions

The menu descriptions in this documentation will assume that the user has Read/Write permissions to all of the data. Not all users will have this level of authorization.

The data displayed and the options presented to a given user will depend upon that user's permissions. A user will only be presented with data and options to the data that he or she is allowed to access. A more detailed discussion of user permissions can be found in the discussion on Local User definitions later in this document.

Note: The menu examples were generated using one specific device model. Because the content of many of the device-specific menus will vary based upon the device and protocol, these are simply examples to give an idea of the type of data displayed here and how it is formatted. The contents of these menus should not necessarily be expected to be displayed, unless it is explicitly stated that the setting applies for all device types.

Menus

Main Menu

The main menu is the starting menu when a user accesses the Telnet/SSH interface. It contains the entry point for all of the pieces of the system data. All other menus are accessible from the main menu.

To help keep the user informed about active alarms, the current list of active alarms is always displayed as part of the main menu.

```
Tripp Lite                                     (c) Copyright 2005-2018
PowerAlert 15.5.2 (Build 17511)                All Rights Reserved
-----
```

```
----- ALARMS -----
```

```
    No active alarms present
```

```
----- Main Menu -----
```

```
1- Devices
2- System Configuration
3- Network Configuration
4- Alarms and Logging
5- About
E- Launch CLI
Q- Logout
<ENTER> Refresh Menu
```

4. Telnet/SSH Console

4.1 Device Menu

If there is more than one device, the first menu displayed for “Device” is a choice of which device's data you would like to present. The data on all descendant menus will refer to the device chosen. If there is only one device, this choice is skipped and all descendant menus will obviously apply to the sole device.

In order to access the device menu structure, the user must have at least read permission for the DEVICE STATUS facility. Any additional permissions needed in the submenus of this structure will be indicated for that menu.

Device List Menu

```
----- Device List -----  
  
1- Device0001 (SMART750RM1UN)  
2- Sensor0004 (E2MTHDI)  
X/M- Return to Main Menu  
<ENTER> Refresh Menu -----
```

Device Main Menu

```
----- Device 1 -----  
  
Device Name      : Device0001  
Location         :  
Vendor           : TRIPPLITE      Region          :  
Protocol         : 3003           Product          : SMART750RM1UN  
State            : NORMAL         Date Installed   : 2016-04-08  
Port Mode        : RS232         Type             : UPS  
Firmware Version : 2264 (Rev A)   Port Name        : /dev/tty02  
Device ID        : 1             Serial Number     :  
Self Test Status : Done and Pass  Self Test Date   : 2016-04-08  
  
1- Status  
2- Identification  
3- Controls  
4- Events  
5- Loads  
6- Preferences and Thresholds  
7- Device Alarms  
8- Logs  
X- Device List Menu  
M- Return to Main Menu  
<ENTER> Refresh Menu
```

4. Telnet/SSH Console

4.1.1 Status

This menu displays the status variables for the device. The values in this menu are not editable. The exact data shown on this menu will be device dependent.

Device Status Menu

```
----- Device Status Menu -----

Device
=====
Self Test Date           : 2016-04-08
Self Test Status         : Done and Passed

Battery
=====
Battery Status           : Normal
Battery Charge Remaining : 100 %
Battery Voltage          : 28.0 V
Battery Temperature (C)  : 35.7 C
Battery Temperature (F)  : 96.3 F
Battery Age              : 0.0 Years

Input
=====
Input Frequency          : 60.0 Hz
Input Voltage            : 121.0 V
Device Mode              : Utility
Tap State                : Normal
Minimum Input Voltage    : 115.0 V
Maximum Input Voltage     : 123.0 V

Output
=====
Output Source            : Normal
Output Load              : 10 %

X- Device Main Menu
M- Return to Main Menu
<ENTER> Refresh Menu
```

4. Telnet/SSH Console

4.1.2 Identification

This is the section of the device menus that will contain the information about the device. This information will be both user-defined settings, such as device name or location, and equipment-specific information like vendor, product and protocol. There are data items on this menu which will be displayed for all devices and some data displayed based upon the type and protocol for the device. Any data that is modifiable by the user will have a prompt option displayed on the menu.

Device Identification Menu

```
----- Identification -----  
  
Device Name           : Device0001  
Location              :  
Region               :  
Vendor               : TRIPPLITE  
Product              : SMART750RM1UN  
Protocol             : 3003  
Date Installed        : 2016-04-08  
State                : NORMAL  
Type                 : UPS  
Port Mode            : RS232  
Port Name            : /dev/tty02  
VA Rating             : 750 VA  
Firmware Version      : 2264 (Rev A)  
Serial Number         :  
Watchdog Supported    : Yes  
Nominal Battery Voltage : 24 V  
Input Line Count      : 1  
Nominal Input Voltage  : 120 V  
Nominal Input Frequency : 60 Hz  
Load Banks Total      : 3  
Load Banks Controllable : 2  
Device ID            : 1  
  
1- Name  
2- Location  
3- Region  
4- Date Installed  
5- Serial Number  
6- Device ID  
X- Device Main Menu  
M- Return to Main Menu  
<ENTER> Refresh Menu
```

Menu Data

The following menu data should display for all devices:

Device Name

This is the user-modifiable device name. The system will give the device a default name. The default for a UPS, PDU or ATS is "DeviceX", where X is the last four digits of the device's serial number. For devices that do not have a serial number, "X" will default to "001." The default for an EnviroSense2 module is "Sensor." The default for SRCOOLNET is "AC."

Location

The user-defined device location. There is no default for location.

Region

The user-defined device region. There is no default for region.

Vendor

This is the manufacturer of the device.

Product

This is the device model.

Protocol

This is the protocol used by the device.

Date Installed

This is the date that the device was installed. For a UPS, this will be used for the battery-installed date and is therefore modifiable.

State

This is the current operating state of the device. Some valid values are:

- NORMAL
- INFORMATION
- WARNING
- STATUS
- CRITICAL
- OFFLINE

Type

This is the device type. Some valid values are:

- UPS
- PDU
- ENVIROSENSE
- ATS

4. Telnet/SSH Console

Port Mode

This is the connection mode of this device. The valid values are:

- RS232
- USB
- HID

Port Name

Name of the port this device is on.

4.1.3 Controls

This section of the menu is used to present the controls that are available for the device. When a control is chosen and it does not have any control data associated, the user will be prompted for verification that they really wish to execute the control. Upon verification, the control will be executed. If the control does have control data parameters associated with it, then that data will be presented when the control is chosen.

Note: To access the controls menu, the user must also have at least Read permission for the DEVICE STATUS and DEVICE CONTROLS facilities.

Device Controls Menu

```
----- Device Controls -----  
  
1 Turn All Loads Off  
2 Reboot SNMP Card  
3 Reboot Device  
4 Initiate Self Test  
5 Turn All Loads On  
6 Cycle All Loads  
X- Device Main Menu  
M- Return to Main Menu  
<ENTER> Refresh Menu
```

4.1.3.1 Control Data

This menu displays the list of data items associated with the control. The options from this menu are to choose the number associated with the data item or to execute ("E") the control. If "E" is chosen, the user will be prompted to verify that they wish to execute the control. If verified, the control is executed. If they choose one of the data items, they will be prompted to enter the new value.

```
----- Control Data -----  
  
-----
```

DESCRIPTION	VALUE	TYPE	MIN	MAX
Delay before reboot (seconds)	15	Integer	1	65535
Delay before restarting UPS (seconds)	60	Integer	10	16777214

```
  
1- Delay before reboot (seconds)  
2- Delay before restarting UPS (seconds)  
E- Execute  
X- Device Control Menu  
M- Return to Main Menu  
<ENTER> Refresh Menu
```

Example of choice '1' for above example

```
Description      : Delay before reboot (seconds)  
Value           : 15  
  
Enter Integer between 1 and 65535  
X- Leave value unchanged  
M- Return to Main Menu
```

Example of choice 'E' for above example

```
Do you wish to execute this control?  
Y- Yes, continue and perform operation  
N- Do Not Make Change
```

4. Telnet/SSH Console

4.1.4 Events

Events

To access the events menu, the user must have at least Read access to the DEVICE EVENTS, ACTIONS and CONTACTS facilities in addition to the DEVICE STATUS facility.

Events Summary Menu

```
----- Device Events Menu -----
```

#	CATEGORY	DESCRIPTION	ENABLED
1	WARNING	Load Level Above Threshold	Yes
2	WARNING	On Battery	Yes
3	CRITICAL	Battery Low	Yes
4	WARNING	Battery Capacity Below Warning Level	Yes
5	CRITICAL	Overload	Yes
6	WARNING	Temperature High	Yes
7	CRITICAL	Output Off	Yes
8	WARNING	Self Test Failed	Yes
9	INFORMATION	Battery Age Above Threshold	Yes
10	INFORMATION	Communications Lost	Yes
11	WARNING	Loads Not All On	Yes
12	WARNING	Load 01 Off	Yes
13	WARNING	Load 02 Off	Yes

#- Select Event
X- Device Main Menu
M- Return to Main Menu
<ENTER> Refresh Menu

Event Details Menu

```
----- Device Event Menu -----
```

Event Set Name	: Load Level Above Threshold
Event Clear Name	: Load Level Below Threshold
Event Category	: WARNING
Event Enabled	: Yes
Event Logging	: On

Set Action	Clear Action
Default Contact Notificat	Default Contact Notificat
Default Trap Notification	Default Trap Notification
Send Trap to PANMS or PAN	Send Trap to PANMS or PAN

1- Manage Actions
2- Modify Event Category
3- Disable Event
4- Disable Logging for Event
X- Device Events Menu
M- Return to Main Menu
<ENTER> Refresh Menu

Menu Data

Event Category

This specifies the severity level for the event. The user may choose to give different events different severity levels. The valid values for category are:

- CRITICAL
- WARNING
- INFORMATION

Enable/Disable Event

This allows the user to no longer consider the event an alarm event. Disabling it causes the event to no longer create an alarm, and the assigned actions will no longer fire when this event occurs. The default is for all events to be enabled.

4. Telnet/SSH Console

Enable/Disable Logging

The user may enable and disable logging for the event. The default is that all events are logged.

Device Event Actions

This will display all of the actions to occur when this event occurs and subsequently clears. The user will also be allowed to add new actions from this menu.

Device Event Actions Summary Menu

```
----- Device Event Actions -----

# Set Action                      Clear Action
-----
 1 Default Contact Notificat      Default Contact Notificat
 2 Default Trap Notification      Default Trap Notification
 3 Send Trap to PANMS or PAN      Send Trap to PANMS or PAN

#- Modify Event Set/Clear Actions
D- Add new Event Set/Clear Actions
X- Device Events
M- Return to Main Menu
<ENTER> Refresh Menu
```

Device Event Action Detail Menu

```
----- Device Event Action Menu -----

Event          : Load Level Above Threshold
Event Clear    : Load Level Below Threshold
Event Action   : Default Contact Notification
Event Clear Action : Default Contact Notification

1- Choose Set Action
2- Choose Clear Action
3- Choose Action For Both Set and Clear
A- Apply Changes
D- Delete the Event Action
X- Device Event Menu
M- Return to Main Menu
<ENTER> Refresh Menu
```

Menu Data

Event

This is the label of the event to which actions will be assigned. This is a display-only value.

Event Clear

This is the clear label of the event to which the actions are being assigned. This is a display-only value.

Event Action

This is also called the set action. It is the action to be taken when this event occurs.

Event Clear Action

This is the action to be taken when this event clears.

Options

- Choose Set Action
This allows the user to choose the set action and then be prompted to choose the clear action.
- Choose Clear Action
This choice allows the user to choose the clear action and then be prompted to choose the set action.
- Choose Action for Both Set and Clear
This option allows the user to choose a single action to be used for both the set and the clear actions.

For all of the above choices, if there are no actions that match the action that the user would like to assign, the user will be allowed to create a new action from this menu. For more information on the action menus, please refer to that section.

4. Telnet/SSH Console

4.1.5 Loads

To access the load menus, the user must have at least Read access to the DEVICE LOADS and DEVICE STATUS facilities. Additionally, a user may be able to update Loads options by accessing outlet realms.

You can control the outlets of a managed device by selecting the load plugged into it and clicking the desired [On], [Off] or [Cycle] control. Each load bank consists of one or more outlets.

You can use the "Description" field to label the banks for easy reference. The main control buttons affect all outlets at once.

Warning! The load controls start or stop the flow of electricity to your device's outlets. Make sure you know what equipment is connected to each load bank before attempting to use these controls! Check the outlet labels and/or test the load banks by plugging a circuit tester or small light into each outlet and observing the effects of the controls.

4.1.5.1 Load Configuration

Menu Data

Edit Description

Use this menu to enter custom labels for load banks. This can be used to help identify equipment quickly and easily before using the controls to cycle the bank ON or OFF.

Change Realm

Assigning a realm to an individual outlet or group of outlets creates a logical grouping that can be used to assign user access.

Turn Load On/Off

This menu controls the state of the outlet.

Cycle Load

This command can be used to turn the load OFF and back ON in a single command.

Change Ramp Action

Select if the outlet should stay OFF or turn ON when ramp actions are triggered.

Change Ramp Delay

If setting the ramp action to turn ON, this command sets the delay before the action occurs.

Change Shed Action

Select if the outlet should stay ON or turn OFF when shed actions are triggered.

Change Shed Delay

If setting the shed action to turn OFF, this command sets the delay before the action to occur.

----- Device Load Detail Menu -----

Description:

Realm: 0
State: On
Controllable: Yes
Load Group:

Ramp Settings

Action: Remain Off
Delay: 0

Shed Settings

Action: Remain On
Delay: 0

- 1- Edit Description
- 2- Change Realm
- 3- Turn Load Off
- 4- Cycle Load
- 5- Change Ramp Action
- 6- Change Ramp Delay
- 7- Change Shed Action
- 8- Change Shed Delay
- X- Load Menu
- M- Return to Main Menu
- <ENTER> Refresh Menu

>> x

-----Loads Menu -----

4. Telnet/SSH Console

4.1.5.2 Load Groups

The Load Groups menu is not available for all devices. Devices that support load groups must have two or more loads and provide a mechanism for updating multiple loads with a single command. If the device does not support load groups, then this menu will not be available.

Load Groups Summary Menu

```
----- Device Load Groups Menu -----  
  
-----  
##| State | Name | Outlets |  
-----  
01| On | load group one | 1 3 5 7 |  
-----  
#- Load Group  
0- New Load Group  
X- Device Main Menu  
M- Return to Main Menu  
<ENTER> Refresh Menu
```

Load Group Detail Menu

```
----- Load Group Detail Menu -----  
  
Load Group Name      : load group one  
Description           : odd loads  
State                : On  
Load                 : 1,3,5,7  
1- Load Group Name  
2- Description  
3- Select Loads  
4- Turn Group Loads Off  
5- Cycle Group Loads  
A- Apply Changes  
D- Delete  
X- Load Groups Menu  
M- Return to Main Menu  
<ENTER> Refresh Menu  
  
>> x
```

Menu Data Descriptions

Load Group Name

This is the name of the load group.

Description

This is the description of the load group.

State

This is the state of the load group. The valid values are:

- On – all of the loads in the group are on
- Off – all of the loads in the group are off
- Mixed – some loads in the group are on and some are off

Load

This is a comma-separated list of loads in the group. The loads in the group must be controllable, belong to only one group and must all be from the same device.

4. Telnet/SSH Console

4.1.5.3 Ramp/Shed Settings

This menu allows the user to modify the ramp and shed settings for the entire device in one operation. This is to ensure the user can make all of the changes necessary before a ramp/shed synchronization is started. The menu will prompt the user to make sure all changes have been made before saving. A message will be displayed that indicates if a ramp/shed synchronization is in progress and further updates will not be allowed. Updates of other variables will also be blocked when synchronization is in progress. This will be indicated on the menus impacted.

Ramp/Shed Settings Summary Menu

----- Ramp/Shed Settings -----

Load	Description	Ramp		Shed	
		Action After Delay	Delay	Action After Delay	Delay
1		Remain Off	0	Remain On	0
2		Remain Off	0	Remain On	0
3		Remain Off	0	Remain On	0
#- Ramp/Shed Settings					
A- Apply Changes					
X- Loads					
M- Return to Main Menu					
<ENTER> Refresh Menu					

The following shows the sequence of automatic data prompts when '1' is entered from the above summary menu and the resulting summary menu when done.

```
>> 1
----- Ramp/Shed Settings -----

----- Ramp Action Selection -----
Current Value: Remain Off
1- Remain Off
2- Turn On After Delay
>> 2

----- Ramp Delay -----
Current Ramp Delay = 0
Enter an integer less than 65536 for Ramp Delay
>> 10

----- Shed Action Selection -----
Current Value: Remain On
1- Remain On
2- Turn Off After Delay
>> 2

----- Shed Delay -----
Current Shed Delay = 0
Enter an integer less than 65536 for Shed Delay
>> 20
----- Ramp/Shed Settings -----
```

Load	Description	Ramp		Shed	
		Action After Delay	Delay	Action After Delay	Delay
1		Turn On	10	Turn Off	20
2		Remain Off	0	Remain On	0
3		Remain Off	0	Remain On	0

Menu Data

Ramp Action

This is the action to take when a ramp is initiated. The valid values are:

- Remain Off
- Turn On After Delay

Ramp Delay

This is the delay before taking the ramp action.

Shed Action

This is the action to take when a shed is initiated. The valid values are:

- Remain On
- Turn Off After Delay

Shed Delay

This is the delay before taking the shed action.

4. Telnet/SSH Console

4.1.6 Preferences and Thresholds

This menu contains the device and protocol specific data that defines the user's preferred behavior settings and thresholds. Since this menu is used to define the user's preferences, the values here should be editable.

Preferences and Thresholds Menu

```
----- Preferences and Thresholds -----
Auto Restart On Shutdown           : Enabled
Auto Restart On Delayed Wakeup     : Enabled
Auto Restart On Low Voltage        : Enabled
Auto Restart On Overload           : Disabled
Auto Restart On Overtemp           : Disabled
Auto Battery Test Period           : Disabled
Low Battery Warning Threshold      : 50 %
Battery Age Alarm Threshold        : 36 Months
Load Level Threshold - % Load     : 90 %

1- Auto Restart On Shutdown
2- Auto Restart On Delayed Wakeup
3- Auto Restart On Low Voltage
4- Auto Restart On Overload
5- Auto Restart On Overtemp
6- Auto Battery Test Period
7- Low Battery Warning Threshold
8- Battery Age Alarm Threshold
9- Load Level Threshold - % Load
X- Device Main Menu
M- Return to Main Menu
<ENTER> Refresh Menu
```

4.1.7 Device Alarms

This view is similar to the alarm view except the alarms displayed here are for the selected device only. The option to enable/disable auto-acknowledge alarms is not available at the device level. It must be done system-wide from the system alarms menu.

4.1.8 Logs

Display the logs that apply to the selected device only. The menus here are similar to the system-wide logging menus but show only the logs for the selected device.

4.2 System Configuration

This section of the menu is used to define system-wide configuration data.

System Configuration Menu

```
----- Configuration -----
----- System Configuration -----
1- Address Book
2- Global Actions
3- Security
4- Date/Time
5- Local Device Discovery
6- Restart PowerAlert
X- System Configuration
M- Return to Main Menu
<ENTER> Refresh Menu
```

4. Telnet/SSH Console

4.2.1 Address Book

This section of the menu is used to define various recipients of data from the system. These include email recipients, SNMP trap and set OID recipients and HTTP destinations used for log rotation.

To access to the address book menu, the user must have at least Read access to the CONTACTS facility.

Address Book Menu

```
----- Address Book -----  
  
1- Email Contacts  
2- SNMP Contacts  
3- HTTP Contacts  
X- System Configuration  
M- Return to Main Menu  
<ENTER> Refresh Menu
```

4.2.1.1 Email Contacts

This section of the menus is used to define the email contacts.

Summary Menu

```
----- Email Contacts -----  
  
# | Name | Email Address |  
1 | John | John@mail.com |  
2 | Nancy | Nancy@mail.com |  
  
#- Email Contact  
0- Add New Email Contact  
X- Contacts Menu  
M- Return to Main Menu  
<ENTER> Refresh Menu
```

Email Contact Detail Menu

After adding a new contact, enter "A" to apply the change. The Status field will display "No Current Email Status" until a test email has been sent. Enter "S" to send a test email.

```
Name      : Nancy  
Email     : Nancy@mail.com  
Status    : No Current Email Status
```

```
A- Apply Changes  
D- Delete  
S - Send Test Email  
X- Email Contacts  
M- Return to Main Menu  
<ENTER> Refresh Menu
```

4. Telnet/SSH Console

Menu Data

Name

This is the name of the email recipient.

Email

This is the email address of the recipient in the form mailbox@emailserver. An example of an email address in its proper form would be user1234@yahoo.com.

4.2.1.2 SNMP Contacts

The destinations defined that can be used to send SNMP traps or perform SNMP set OID operations.

SNMP Contacts Summary Menu

```
----- SNMP Contacts Menu -----  
  
-----  
# | Name | Host Address | Port | Version  
-----  
1 | mycommunity | 10.10.10.10 | 200 | SNMPV1  
2 | snmpv3 destination | 10.11.12.13 | 162 | SNMPV3  
  
#- Edit SNMP Contact  
0- Add New SNMP Contact  
X- Address Book  
M- Return to Main Menu  
<ENTER> Refresh Menu
```

SNMP V1/V2 Contact Detail

```
----- SNMP Contact Detail Menu -----  
  
SNMP Version : SNMPV2c  
Name : snmpv2 destination  
Host Address : 10.10.10.11  
Port : 162  
Community : sss  
  
1- Name  
2- Host Address  
3- Port  
4- Community  
A- Apply Changes  
D- Delete  
X- Contacts Menu  
M- Return to Main Menu  
<ENTER> Refresh Menu  
>>
```

4. Telnet/SSH Console

SNMP V3 Contact Detail Menu

```
----- SNMP Contact Detail Menu -----

SNMP Version      : SNMPV3
Name              : snmpv3 destination
Host Address      : 10.11.12.13
Port              : 162
User              : someusername
Priv Password     : somepassword
Auth Password     : somepassword

1- Name
2- Host Address
3- Port
4- User
5- Priv Password
6- Auth Password
A- Apply Changes
D- Delete
X- Contacts Menu
M- Return to Main Menu
<ENTER> Refresh Menu
>>
```

Menu Data

Name

The name is the character string which contains a unique identifying name for the SNMP destination.

Host Address

This defines the IP Address used to send SNMP Traps or SNMP Set OID requests.

Port

This defines the Host Address Port used to send SNMP Trap or SNMP Set OID requests.

Community (SNMPV1 and SNMPV2c only)

For SNMPv1 or SNMPv2 recipients, this must be a valid community for the receiving agent.

User (SNMPV3 only)

This must specify a valid SNMPV3 username defined in the VACM tables. This is the username specified in the Set OID requests.

Priv Password (SNMPV3 only)

The PRIV Password of the SNMPV3 user used for sending Set OID requests.

Auth Password (SNMPV3 only)

The AUTH password of the SNMPV3 user used for sending Set OID requests.

4. Telnet/SSH Console

4.2.1.3 HTTP Contacts

HTTP destinations to be used for sending log files when rotating logs.

HTTP Destination Summary

----- HTTP Contacts Menu -----

```
#      Name
1      http destination

#- Edit HTTP Contact
0- Add New HTTP Contact
X- Address Book
M- Return to Main Menu
<ENTER> Refresh Menu
```

HTTP Contact Detail

----- HTTP Contact Detail Menu -----

```
Name           : http destination
Protocol        : https
Address         : 10.12.14.16
Port           : 223
Contact URI     : someuri.here.com
Authentication Login Name : eightlettername
Authentication Password  : eightletterpassword
1- Name
2- Protocol
3- Address
4- Port
5- Contact URI
6- Authentication Login Name
7- Authentication Password
A- Apply Changes
D- Delete
X- Contacts Menu
M- Return to Main Menu
<ENTER> Refresh Menu
>>
```

Menu Data

Name

The name is the character string which contains a unique identifying name for the HTTP destination.

Protocol

Choose “http” for non-secured HTTP and “https” for secured HTTP.

Contact URI

Uniform Resource Identifier (URI) is a character string used to identify the destination on the internet.

Authentication Login Name

This is an optional login name used for authentication. The string must have a length between 8 and 32 characters. Alphanumeric and the following special characters are supported: !@#\$%^*(){}[]~_-

Authentication Password

This is an optional password used for authentication. It must be a string between 8 and 32 characters. If the authentication login is entered, then the authentication password should be entered as well.

4. Telnet/SSH Console

4.2.2 Global Actions

4.2.2.1 Action Profiles

Action profiles define responses to events and alarm conditions. The action profile allows the response to be defined once and applied to multiple alarm events. An action may be a response to the alarm condition or a response to the condition clearing. Where appropriate, the two actions may be the same.

```
----- Action Profiles Menu -----  
  
1- Email Notification Profiles  
2- Device Shutdown Profiles  
3- SNMP Set OID Profiles  
4- SNMP Trap Notification Profiles  
5- Load Control Action Profiles  
6- Ramp Action Profiles  
7- Shed Action Profiles  
8- Control Execution Action Profiles  
X- Global Actions  
M- Return to Main Menu  
<ENTER> Refresh Menu
```

Common Action Data

All action profiles, unless otherwise noted, have the data described in this section.

Name

All actions have a unique identifying name.

Delay

All actions have a delay in seconds. This is the amount of time before the action fires after the event occurs. When an action is the response to the action clearing, the delay is ignored and is done immediately.

Common Data

In addition to the common values for name and delay, the notification actions also allow the notifications to be sent multiple times until the event condition has been cleared. The additional data to support that is an interval and count.

Interval

This data applies to only Email and SNMP Trap Notifications. The interval allows the notification to be sent multiple times while the alarm condition is present. The interval is the amount of time in seconds before sending the next notification. The valid values are:

- 0 – the notification is sent only once
- Integer greater than or equal to 15 – the notification will be sent after this interval has elapsed and the alarm condition is still present

Count

This data applies to only Email and SNMP Trap Notifications. The count determines the number of times that the notification will be sent. The valid values are:

- 0 – valid only if interval is not 0. This implies that the notification should be sent until the alarm condition is cleared.
- 1 – valid only if interval is 0. The notification is sent only once.
- Integer greater than 1. This is a finite number of times that the notification will be sent while the alarm condition is still present.

4. Telnet/SSH Console

4.2.2.1.1 Email Notification Action Menus

Summary Menu

```
----- Email Notification Profiles -----  
  
-----  
# | Name | DELAY | INTERVAL | INTERVAL | TO  
 | | | | COUNT | ALL  
-----  
1 | Default Contact Notification | 30 | 0 | 1 | Yes  
2 | Email to Admin | 0 | 0 | 1 | No  
  
#- Edit Profile  
0- Add New Profile  
X- Action Profile Menu  
M- Return to Main Menu  
<ENTER> Refresh Menu
```

Default Email Notification Action Profile Menu

```
----- Email Action Profile Detail Menu -----  
  
Name: Default Contact Notification  
Delay: 30  
Interval: 0  
Count: 1  
Email Contacts Chosen: All  
  
1- Modify Profile Name  
2- Modify Delay  
3- Modify Interval  
4- Modify Count  
5- Manage Email Action Contacts  
6- Apply To Device Events  
A- Apply Changes  
D- Delete  
X- Email Action Profiles Menu  
M- Return to Main Menu  
<ENTER> Refresh Menu
```

Email Action Profile with Single Email Contact Example Menu

```
----- Email Action Profile Detail Menu -----  
  
Name: Email to Admin  
Delay: 0  
Interval: 0  
Count: 1  
Email Contacts Chosen: Admin John Doe  
  
1- Modify Profile Name  
2- Modify Delay  
3- Modify Interval  
4- Modify Count  
5- Manage Email Action Contacts  
6- Apply To Device Events  
A- Apply Changes  
D- Delete  
X- Email Action Profiles Menu  
M- Return to Main Menu  
<ENTER> Refresh Menu
```

4. Telnet/SSH Console

Menu Data

Email Contacts Chosen

The email notification action requires the user to define a list of contacts that will receive email notification when an event occurs. When the option is set to ALL, every email contact in the system will receive the notification and any new users added will automatically be included in the list without any further changes to the action. Alternately, the option can be set to only notify a specific list of email contacts defined in the system.

Choosing Email Contact Example Menus

```
----- Email Action Contacts Menu -----  
  
Email Contacts Chosen: All  
  
1- Select All Contacts  
2- Clear Contact List  
3- Assign Contact To List  
4- Delete Contact From List  
X- Email Action Profile Menu  
M- Return to Main Menu  
<ENTER> Refresh Menu  
>> 3  
  
----- Add Email Action Contact Menu -----  
  
Email Contacts Chosen: All  
  
-----  
# | Name | Email Address  
-----  
1 | Admin John Doe | admin_jdoe@example.com  
  
#- Assign Contact To List  
0- Create New Contact  
X- Email Action Contacts Menu  
M- Return to Main Menu  
<ENTER> Refresh Menu  
>> 1  
  
----- Add Email Action Contact Menu -----  
  
Email Contacts Chosen: Admin John Doe  
  
-----  
# | Name | Email Address  
-----  
1 | Admin John Doe | admin_jdoe@example.com  
  
#- Assign Contact To List  
0- Create New Contact  
X- Email Action Contacts Menu  
M- Return to Main Menu  
<ENTER> Refresh Menu  
>> x  
  
----- Email Action Contacts Menu -----  
  
Email Contacts Chosen: Admin John Doe  
  
1- Select All Contacts  
2- Clear Contact List  
3- Assign Contact To List  
4- Delete Contact From List  
X- Email Action Profile Menu  
M- Return to Main Menu  
<ENTER> Refresh Menu
```

4. Telnet/SSH Console

4.2.2.1.2 SNMP Trap Notification Menus

Summary Menu

```
----- SNMP Trap Notification Profiles -----  
  
-----  
# | Name | DELAY | INTERVAL | INTERVAL | TO  
 | | | | COUNT | ALL  
-----  
1 | Default Trap Notification | 30 | 0 | 1 | Yes  
  
#- Edit Profile  
0- Add New Profile  
X- Device Action Profile Menu  
M- Return to Main Menu  
<ENTER> Refresh Menu
```

Detail Menu

```
----- SNMP Trap Action Profile Detail Menu -----  
  
Name: Default Trap Notification  
Delay: 30  
Interval: 0  
Count: 1  
SNMP Contacts Chosen: All  
  
1- Modify Profile Name  
2- Modify Delay  
3- Modify Interval  
4- Modify Count  
5- Manage SNMP Trap Contacts  
6- Apply To Device Events  
A- Apply Changes  
D- Delete  
X- Script Exection Action Profiles Menu  
M- Return to Main Menu  
<ENTER> Refresh Menu
```

>> x

Menu Data

SNMP Contacts Chosen

This is the list of contacts that the SNMP trap will be sent to when the action is fired. The trap may be sent to all SNMP Contacts or to a specific list of SNMP Contacts defined in the system. When the option is set to ALL, any new contacts will automatically be sent the set request without making any further changes to the action.

4. Telnet/SSH Console

4.2.2.1.3 SNMP Set OID Action Menus

SNMP Set OID actions will make an SNMP Set request to a list of SNMP Contact Destinations.

Summary Menu

```
----- SNMP Set OID Profiles -----  
  
-----  
# | Name | DELAY | INTERVAL | INTERVAL  
-----  
1 | shed on alarm | 0 | 0 | 1  
2 | ramp on clear | 0 | 0 | 1  
  
#- Edit Profile  
0- Add New Profile  
X- Device Action Profile Menu  
M- Return to Main Menu  
<ENTER> Refresh Menu
```

Detail Menu

```
----- SNMP Set OID Action Profile Detail Menu -----  
  
Name: shed on alarm  
Delay: 0  
Interval: 0  
Count: 1  
SNMP Contacts Chosen: All  
Set OID: 1.3.6.1.4.1.850.100.1.8.3.3.0  
Set OID Data Type: Integer  
Set OID Value: 1  
  
1- Modify Profile Name  
2- Modify Delay  
3- Modify Interval  
4- Modify Count  
5- Update OID  
6- Update Data Type  
7- Update Value  
8- Manage SNMP Set OID Contacts  
9- Apply To Device Events  
A- Apply Changes  
D- Delete  
X- Script Execution Action Profiles Menu  
M- Return to Main Menu  
<ENTER> Refresh Menu
```

Menu Data

OID

This is the OID to be used in the SNMP Set request sent for the action.

Note: The OID should not start with a period.

Data Type

This is the data type used in the SNMP Set request sent for the action. Available options are Integer and String.

Value

This is the value used in the SNMP Set request sent for the action.

SNMP Contacts Chosen

This is the list of contacts that the SNMP Set request will be sent to when the action is fired. The set request may be sent to all SNMP Contacts or to a specific list of SNMP Contacts defined in the system. When the option is set to ALL, any new contacts will automatically be sent the set request without making any further changes to the action.

4. Telnet/SSH Console

4.2.2.1.4 Device Specific Menus

The device-specific menus are actions that occur on a specific device. They may be applied to any device event.

Common Data

Device ID

Since all these actions will occur on a specific device, they require the user to specify the device.

Device Shutdown Action Menus

Summary Menu

```
----- Device Shutdown Profiles -----  
  
-----  
# | Name | DELAY  
-----  
1 | Default Device Shutdown | 120  
  
#- Edit Profile  
0- Add New Profile  
X- Device Action Profile Menu  
M- Return to Main Menu  
<ENTER> Refresh Menu
```

Detail Menu

```
----- Device Shutdown Action Profile Detail Menu -----  
  
Name: Default Device Shutdown  
Delay: 120  
Device: 0  
  
1- Modify Profile Name  
2- Modify Delay  
3- Apply To Device Events  
A- Apply Changes  
D- Delete  
X- SNMP Trap Action Profiles Menu  
M- Return to Main Menu  
<ENTER> Refresh Menu
```

Load Control Action Menus

Summary Menu

```
----- Device 1 Load Control Action Profile -----  
  
-----  
# | Name | DELAY  
-----  
1 | load 1 off | 120  
  
#- Edit Profile  
0- Add New Profile  
X- Device Action Profile Menu  
M- Return to Main Menu  
<ENTER> Refresh Menu
```

4. Telnet/SSH Console

Detail Menu

```
----- Device 1 Load Control Action Profile Detail -----  
  
Name: load 1 off  
Delay: 120  
Device: 1  
Load Control: Turn Off  
Loads Chosen: 1  
  
1- Modify Profile Name  
2- Modify Delay  
3- Select Load Control  
4- Select Loads To Control  
5- Apply To Device Events  
A- Apply Changes  
D- Delete  
X- SNMP Trap Action Profiles Menu  
M- Return to Main Menu  
<ENTER> Refresh Menu
```

Menu Data

Load Control

This setting dictates what the load will do when the action is fired. The valid options are:

- Turn Off
- Turn On

Load Selection

This is the list of loads that will be controlled by the action. The display will always be a comma-separated list of loads. For data entry, the loads may be entered as a comma-separated, a range or a comma-separated list that contains ranges.

The lists (1, 2, 3, 5, 6, 7) and (1-3, 5-7) would both be accepted and result in the same selection.

Ramp Action Menus

Summary Menu

```
----- Device 1 Ramp Action Profile -----  
  
-----  
# | Name | DELAY  
-----  
1 | ramp it up | 0  
  
#- Edit Profile  
D- Add New Profile  
X- Device Action Profile Menu  
M- Return to Main Menu  
<ENTER> Refresh Menu
```

4. Telnet/SSH Console

Detail Menu

```
----- Device 1 Ramp Action Profile Detail -----  
  
Name: ramp device loads  
Delay: 0  
Device: 1  
  
1- Modify Profile Name  
2- Modify Delay  
A- Apply Changes  
D- Delete  
X- Device Ramp Action Profiles Menu  
M- Return to Main Menu  
<ENTER> Refresh Menu
```

Shed Action Menus

Summary Menu

Only one device available for this action type. Using device 1.

```
----- Device 1 Shed Action Profile -----  
  
-----  
# | Name | DELAY  
-----  
1 | shed device loads | 0  
  
#- Edit Profile  
0- Add New Profile  
X- Device Action Profile Menu  
M- Return to Main Menu  
<ENTER> Refresh Menu
```

Detail Menu

```
----- Device 1 Shed Action Profile Detail -----  
  
Name: shed device loads  
Delay: 0  
Device: 1  
  
1- Modify Profile Name  
2- Modify Delay  
3- Apply To Device Events  
A- Apply Changes  
D- Delete  
X- Device Shed Action Profiles Menu  
M- Return to Main Menu  
<ENTER> Refresh Menu
```

4. Telnet/SSH Console

Control Execution Action Menus (This feature is not yet implemented.)

Summary Menu

Only one device available for this action type. Using device 1.

```
----- Device 1 Control Execute Action Profile -----  
  
-----  
# | Name | DELAY  
-----  
1 | exec control action | 0  
2 | exec another control action | 0  
  
#- Edit Profile  
0- Add New Profile  
X- Device Action Profile Menu  
M- Return to Main Menu  
<ENTER> Refresh Menu
```

Detail Menu

Control with no control data

```
----- Device 1 Control Execute Action Profile Detail -----  
  
Name: exec control action  
Delay: 0  
Device: 1  
Control Executed: Initiate Self Test  
  
1- Modify Profile Name  
2- Modify Delay  
3- Apply To Device Events  
A- Apply Changes  
D- Delete  
X- Device Control Execute Action Profiles Menu  
M- Return to Main Menu  
<ENTER> Refresh Menu
```

Control with Control Data

```
----- Device 1 Control Execute Action Profile Detail -----  
  
Name: exec another control action  
Delay: 0  
Device: 1  
Control Executed: Reboot Device  
Control Data:  
-----  
Description | Value  
-----  
Delay before shutdown (seconds) | 1  
Delay before restart (minutes) | 1  
  
1- Modify Profile Name  
2- Modify Delay  
3- Control Data  
4- Apply To Device Events  
A- Apply Changes  
D- Delete  
X- Device Control Execute Action Profiles Menu  
M- Return to Main Menu  
<ENTER> Refresh Menu
```

Menu Data

Control

This is the control to be executed by the action.

Control Data

Some controls have additional data. For those controls, the data settings may be changed.

4. Telnet/SSH Console

4.2.2.1.5 Applying Actions to Events

Choosing this option begins the process of assigning the action to events. Each event has both a “Set” and a “Clear” action associated with it. The action being updated must be used for the “Set” action or both “Set” and “Clear” actions, as appropriate. Ramp actions are only allowed to be used for the “Clear” action and will not be present this option. The steps necessary to assign the actions to events are as follows:

1. Choose “Set” and “Clear” action pair.
2. Choose events that the use “Set” and “Clear” actions.

Choosing the Set and Clear Actions

Once all the data for an action profile has been saved, the user will have the option to apply the action to events. The next step presented depends upon the type of action profile being updated. The action profile being updated will at least be the “Set” action, unless the action type is not allowed to be used for the set action. At this time, the only type of action that cannot be used for the set action is Ramp action.

Actions to Using Both Set and Clear

For Email and SNMP Trap notifications, the same action is automatically used for both “Set” and “Clear” responses. The menu will proceed directly to choosing the events to correspond to these actions.

Actions Types Allowed for Set Only

Shed action profiles are only allowed to be used as the “Set” action on events. In the menu, only the option to use the action for “Set” will be given. The following is an example of the menu displayed for this action profile type.

```
----- Actions Set/Clear -----  
  
Using Action For Alarm Condition  
  
S- Continue to Apply to Device Events  
  
X- None  
  
M- Return to Main Menu  
  
<ENTER> Refresh Menu
```

Action Types Allowed for Clear Only

Ramp Action profiles are only allowed to be used in conjunction with Shed Action profiles and therefore must be a “Clear” action on events. Since the “Set” action must be chosen before the “Clear” action, the Ramp action will not be present in the “Set” menu and cannot be the first action applied to an event.

Action Types Allowed for Both Set and Clear

The action types not already covered are allowed to be used for both the event “Set” and “Clear” actions. Unlike the notification actions, where it is desirable for the “Set” and “Clear” action to be the same, the preference for these actions is that the “Set” and “Clear” actions be of the same type, but not the same action. The types covered here are Load Control Actions, Control Execution and SNMP Set OID. The following is an example of the menu presented for these action types.

4. Telnet/SSH Console

Menu Data

Using Action for Set Action

The action will be used for the “Set” action only. The user will be given the option to choose the “Clear” action before continuing on to select events.

Using Action for Both Set and Clear Action

The action will be used for both “Set” and “Clear” and the user can immediately continue on to choose events.

Choosing Clear Action

This is skipped if action is to be used for both “Set” and “Clear” action, or the user chose not to include a “Clear” action. The action chosen for the “Clear” action must be the same type as the “Set” action. The list of available actions will be presented. If none of the actions match what the user would like to happen on the clear, the user may choose to insert a new action.

Choosing an existing action

The number of the existing action is chosen and the user moves on to select events.

Choosing to create a new action

The user is placed into insert mode and prompted for the settings for the new actions. Once the insert of the new action is completed, it is chosen as the “Clear” action and the user is moved on to select events.

Choosing Events

----- Apply To Device Events -----

```
Set Action          : shed device loads
Clear Action        : ramp device loads

1- Apply To All Device Events
2- Apply To Events On Device 1 (SU1500RTXL2Ua)
3- Apply To Events On Probe (Envirosense)
X- None
M- Return to Main Menu
<ENTER> Refresh Menu
```

Apply To All Events

This option will apply the “Set” and “Clear” actions chosen to all of the events on all devices. If the “Set” and “Clear” actions are already assigned, but are not paired with the same “Set” and “Clear” action, the user will be prompted to leave those assignments alone or to clear those assignments and assign the chosen actions in their place.

Apply to Events of a Selected Device

----- Action Events -----

```
Set Action          : shed device loads
Clear Action        : ramp device loads
Events Chosen       : None

1- Apply To All Events
2- Clear Event List
3- Add Event To List
4- Delete Event From List
X- Apply To Device Events
M- Return to Main Menu
<ENTER> Refresh Menu
```

4. Telnet/SSH Console

Menu Data

Apply To All Events

This option will apply the “Set” and “Clear” actions chosen to all of the events on the selected devices. If the “Set” and “Clear” actions are already assigned but are not paired with the same “Set” and “Clear” action, the user will be prompted to leave those assignments alone or to clear those assignments and assign the chosen actions in their place.

Clear Event List

This will clear the “Set” and “Clear” action assignments from all of the events for the selected device only.

Add Event to List

This choice will allow the user to select an event from the list of events for the device selected. Only the events that do not currently have actions assigned will be presented.

```
----- Add Event To List -----  
  
1- Contact 1 In Alarm  
2- Contact 2 In Alarm  
3- Contact 3 In Alarm  
4- Contact 4 In Alarm  
5- Temperature Beyond Limits  
6- Humidity Beyond Limits  
X- Action Events  
M- Return to Main Menu  
<ENTER> Refresh Menu
```

Delete Event From List

Delete a chosen event from the list. The user will be presented with a list of all events that are currently using the “Set” and “Clear” action. Choosing an event will remove the actions from that event only. The following is an example of the delete event menu.

```
----- Delete Event From List -----  
  
1- Temperature Beyond Limits  
2- Humidity Beyond Limits  
X- Action Events  
M- Return to Main Menu  
<ENTER> Refresh Menu
```

Note: To have access to the action profiles menus, the user must have at least Read access to the ACTIONS and DEVICE EVENTS facilities. In addition, to be able to have access to control execution actions, the user must also have at least Read permission to the DEVICE CONTROLS as well. Similarly, to have access to load control, ramp and shed actions, the user must also have access to DEVICE LOAD. To be able to create Email notification, SNMP Trap and SNMP Set OID actions, the user must also have at least Read permission for CONTACTS.

4. Telnet/SSH Console

4.2.2.2 Schedules

Once a schedule has been created, it cannot be modified. To change a schedule, the original schedule has to be removed and a new schedule created.

```
----- Schedules Menu -----  
  
-----  
# Pending Action      Next Execution Time      Frequency  
-----  
1 Cycle All Loads     2016-06-02 17:00:00+00:00 Weekly  
2 Reboot Device       2016-06-15 18:00:00+00:00 Monthly  
3 Reboot SNMP Card    2016-06-15 22:00:00+00:00 Monthly  
4 Initiate Self Test  2017-01-15 23:00:00+00:00 Yearly  
5 Initiate Self Test  2016-11-26 08:00:00+00:00 Yearly  
  
#- View Schedule  
O- Add New Schedule  
X- Global Actions  
M- Return to Main Menu  
<ENTER> Refresh Menu
```

Execute Once Schedule

```
----- Schedule Detail Menu -----  
  
Pending Action      : Initiate Self Test  
Device Id           : 1  
Frequency            : Once  
Next Execution Time : 2016-06-01 16:00:00+00:00  
  
D- Delete Schedule  
X- Schedules Menu  
M- Return to Main Menu  
<ENTER> Refresh Menu
```

Execute Daily Schedule

```
----- Schedule Detail Menu -----  
  
Pending Action      : Cycle All Loads  
Device Id           : 1  
Frequency            : Daily  
Interval             : Every Day  
Time                 : 17:00  
Start Date           : 2016-06-01  
Until                : Forever  
  
1- Device  
2- Pending Action  
3- Frequency  
4- Time  
5- Interval  
6- Start Date  
7- Until  
A- Create Schedule  
X- Schedules Menu  
M- Return to Main Menu
```

4. Telnet/SSH Console

Execute Weekly Schedule

----- Schedule Detail Menu -----

Pending Action : Cycle All Loads
Device Id : 1
Frequency : Weekly
Day Of Week : Sunday, Thursday, Saturday
Interval : Every Week
Next Execution Time : 2016-06-02 17:00:00+00:00
Until : Forever

D- Delete Schedule
X- Schedules Menu
M- Return to Main Menu
<ENTER> Refresh Menu

Execute Monthly Schedule

Day of Month

----- Schedule Detail Menu -----

Pending Action : Reboot SNMP Card
Device Id : 1
Frequency : Monthly
On : 15th
Of : Every Month
Next Execution Time : 2016-06-15 22:00:00+00:00
Number Of Repetitions: 5

D- Delete Schedule
X- Schedules Menu
M- Return to Main Menu
<ENTER> Refresh Menu

Relative Day of Month

----- Schedule Detail Menu -----

Pending Action : Reboot Device
Device Id : 1
Frequency : Monthly
On : Third Wednesday
Of : Every Month
Next Execution Time : 2016-06-15 18:00:00+00:00
Number Of Repetitions: 5

D- Delete Schedule
X- Schedules Menu
M- Return to Main Menu
<ENTER> Refresh Menu

4. Telnet/SSH Console

Execute Yearly Schedule

Day of Month

----- Schedule Detail Menu -----

Pending Action : Initiate Self Test
Device Id : 1
Frequency : Yearly
On : 15th
Month : January
Next Execution Time : 2017-01-15 23:00:00+00:00
Until : Forever

D- Delete Schedule
X- Schedules Menu
M- Return to Main Menu
<ENTER> Refresh Menu

Relative Day of Month

----- Schedule Detail Menu -----

Pending Action : Initiate Self Test
Device Id : 1
Frequency : Yearly
On : Last Saturday
Month : November
Next Execution Time : 2016-11-26 08:00:00+00:00
Until : Forever

D- Delete Schedule
X- Schedules Menu
M- Return to Main Menu
<ENTER> Refresh Menu

4. Telnet/SSH Console

Menu Data

Device ID

This field selects the device to which the schedule is to be applied.

Pending Action

This field indicates the action to be fired according to the schedule.

Time

This setting controls the time that the scheduled action will be fired. The time and date chosen must be in the future. The default setting is 10 minutes from the current time.

Date/Start Date

For schedules that will only fire once, this is the date that the scheduled control will be executed.

For all other schedules, this is the start date for scheduling the control to be executed. The date and time chosen must be in the future. The default setting is the current date.

Frequency

This is how often the control is to be executed. Choices are: once, daily, weekly, monthly and yearly.

Interval

The interval is valid only for daily, weekly and monthly schedules. This is the number of days, weeks or months between executions of the chosen control. For example, an interval of 2 for a daily schedule means that it would happen every other day. The default for interval is 1.

Day of Week

This is the day of the week that the scheduled control should be executed. It is used for weekly schedules and for monthly/yearly schedules using a relative day selection such as "first Thursday."

Day of Month

This setting is used for monthly and yearly schedules. It specifies the day of the month that the schedule should be executed.

Month

This setting is used for yearly schedules only. This is the month that the yearly scheduled control should be executed.

Relative Days

This setting is used for monthly and yearly schedules. It allows a relative day of a month to be specified. The valid relative day selections are:

- First
- Second
- Third
- Fourth
- Last

It is used in combination with the day of the week to choose a relative day of the month like "last Friday" for a monthly schedule or "third Thursday of July" for a yearly schedule.

Until

For daily, weekly, monthly and yearly schedules, the user also needs to specify how long the schedule is in effect. The valid choices are:

- Forever – the schedule will be executed until it is deleted
- End Date – the schedule will be executed until the specified date.
- Number of Repetitions – the schedule will be executed for the specified number of times.

Automatic Removal of Schedule

A schedule will be automatically removed when it has fired for the last time. The conditions that will cause the schedule to be removed are:

- One-time schedule has been executed.
- The Until End Date has been reached.
- The Until Number of Repetitions has been reached.

4. Telnet/SSH Console

4.2.3 Security

Security Menu

----- Security Menu -----

```
1- Authentication Method
2- Local Users
3- Radius Servers
4- Change Password
X/M- Return to Main Menu
<ENTER> Refresh Menu
```

4.2.3.1 Authentication Method

Authorization Detail Menu

----- Authentication Method -----

```
Authrorization Scheme : Local Only
Accounting Scheme : Local Only
```

```
1- Authentication Scheme
2- Accounting Scheme
X- Security Menu
M- Return to Main Menu
<ENTER> Refresh Menu
```

>> 1

Authentication Scheme Data Entry Menu

----- Authentication Scheme Menu -----

```
Authentication Scheme: Local Only
```

```
1- Local Only
2- Radius Only
3- Local Then Radius
4- Radius Then Local
X- Authentication Method
M- Return to Main Menu
```

Accounting Scheme Data Entry Menu

----- Accounting Scheme Menu -----

```
Accounting Scheme: Local Only
```

```
1- Local Only
2- Radius Only
3- Local Then Radius
4- Radius Then Local
X- Authentication Method
M- Return to Main Menu
```

Authorization Scheme

The authorization scheme defines how user authentication will be done.

The authorization can be done with locally defined users only, RADIUS server defined users only or a combination of the two. The valid values are:

- Local Only

The system only uses locally defined user definitions.

- RADIUS Only

The system uses RADIUS only for authentication.

- Local Then RADIUS

The system uses locally defined user definitions first. If the user data is not found, it uses RADIUS for authentication.

- RADIUS Then Local

The system uses RADIUS for authentication first. If not authorized via the RADIUS server, the locally defined users will be used for authentication.

Accounting Scheme

This defines where the user session accounting data will be recorded.

Like the authorization, the data can be recorded locally or on the RADIUS server or a combination of the two. The valid values are:

- Local Only

Uses only the local system to record the session accounting data.

- RADIUS Only

Uses only the RADIUS servers defined to record the session accounting data.

- Local Then RADIUS

Tries to record the session accounting data locally and, if not able to, then tries to record to RADIUS.

- RADIUS Then Local

Tries to record the session accounting data on RADIUS first and, if not able to, then records locally.

4. Telnet/SSH Console

4.2.3.2 Local Users

This menu is used to define the local users. Local users include SNMPv3 users and SNMPv1/v2c communities, which must be defined locally. RADIUS authentication may not be used for SNMP access. There are a total of 12 users that may be defined with 5 default users being created initially. Available slots will be identified in the user summary table with the name/community of "User Not Defined."

The following is the data used to define the users. Not all data applies to all user types and will be identified accordingly. Alphanumeric and the following special characters can be used: !@\$%^*(){}[]~_).

```
-----User Detail Menu-----
SNMP Protocol      : SNMPV3
User Name          : localadmin
Role               : administrator
Outlet Realms      :
ACL IP Address     : ::
ACL IP Mask        : ::
Password           : rG5cF6F8E3kNU5iwHddrrg==
Auth Password      : rG5cF6F8E3kNU5iwHddrrg==
Idle Timeout in Minutes : 0
Session Expiration in Min: 0

1- Name
2- Password
3- Auth Password
A- Apply Changes
X- Security
M- Return to Main Menu
<ENTER> Refresh Menu
>>
```

Menu Data

SNMP Protocol

The SNMP Protocol is the first attribute to be defined for a user since it will need to be used to determine what data items need to be populated for the user. The valid values are:

- None

This user does not have any SNMP access allowed.

- SNMPv1

This user is a SNMPv1 community definition. Only access through SNMP is allowed for this user.

- SNMPv2c

This user is a SNMPv2c community definition. Only access through SNMP is allowed for this user.

- SNMPv3

This user has SNMPv3 access, as well as access through any of the other view interfaces.

Username (SNMPv3 and No SNMP Access Users)

This is the username. It is a string value which is 8 to 32 characters long with no spaces.

Community (SNMPv1 and SNMPv2c Users)

This is the SNMP community name. It is a string value which is 8 to 32 characters long with no spaces.

Role

This is determined by login credentials. Valid values are administrator, manager and read-only.

Outlet Realms

Outlet realms are an integer between 1 and 32 used to identify a logical grouping of outlets to be used to limit a user's access to a subset of outlets. In the user definition, it is a comma separated list of realms or range of realms that the user may access. Each load may be assigned a single realm and multiple outlets may use the same realm.

For example, a PDU may be powering devices at a co-hosting facility where Customer One has all of his equipment connected to Circuit 1 of a 3-phase PDU, Customer Two is on Circuit 2, and Customer Three is on Circuit 3. This PDU may have outlets 1, 4, 7, 10, 13, 16, 19 and 22 on Circuit 1, outlets 2, 5, 8, 11, 14, 17, 20 and 24 on Circuit 2 and outlets 3, 6, 9, 12, 15, 18, 21, and 23 on Circuit 3. The outlets on Circuit 1 could be assigned to Realm 5. The outlets on Circuit 2 could be assigned to Realm 7 and the outlets on Circuit 3 could be assigned to Realm 9. The user realm mapping would be Realm 5 for Customer One, Realm 7 for Customer Two and Realm 9 for Customer Three. Assigning the realm to the user gives Read/Write access only for the outlets assigned to the users' realms, meaning they will be able to turn On or Off outlets only in the same realm.

4. Telnet/SSH Console

Although the concept of realms may seem similar to outlet groups, it provides no other grouping functionality other than permissions.

192.168.1.1 (single)	255.255.255.255
192.168.1.0 (range)	255.255.255.0
192.168.0.0	255.255.0.0
192.0.0.0	255.0.0.0
0.0.0.0 (everyone)	0.0.0.0

The access level to the realms indicated is Read/Write. Each load may optionally be assigned to a realm. Whatever loads belong to the realms indicated here, the user may access. In order to correctly access the data, a user should have at least Read Only permission for Device Status and Device Loads to be able to user the realms.

ACL IP Address (Users with SNMP Access Only)

This defines what IP Address (or Addresses when used with the ACL IP Mask) from which this user may access the data via SNMP.

ACL IP Mask (Users with SNMP Access Only)

This defines the Subnet Mask to user with the ACL IP Address to determine if an address is one from which the user is allowed to access the data via SNMP.

Password (N/A for SNMPv1 or SNMPv2c)

This is the user password for logging in. For SNMP V3 users, this is the Priv Password.

Auth Password (N/A for SNMPv1 or SNMPv2c)

For SNMP v3 Users only, this is the Auth Password.

Idle Timeout in Minutes (N/A for SNMPv1 or SNMPv2c)

This applies to data access other than SNMP which does not use the concept of a logged in session. This is the amount of time the session can be idle before it will time out and no longer have access to the data. When the value is 0, that means idle sessions will not time out.

Session Expiration Minutes (N/A for SNMPv1 or SNMPv2c)

This applies to data access other than SNMP which does not use the concept of a logged in session. This is the amount of total time a session may last whether or not the session is idle or active. When the value is 0, the session will not expire.

4. Telnet/SSH Console

Local User Summary Menu

```
----- Local Users -----
# | NAME / COMMUNITY | SNMP
-----
1  localadmin        SNMPV3
2  localmanager      SNMPV3
3  localguest        SNMPV3
4  public            SNMPV1
5  tripplite         SNMPV2c
6  mikemike          None
7  User Not Defined
8  User Not Defined
9  User Not Defined
10 User Not Defined
11 User Not Defined
12 User Not Defined
#-  User
X-  Security Menu
M-  Return to Main Menu
<ENTER> Refresh Menu
>> 1
```

Local User Detail Menu

```
----- User Detail Menu -----
SNMP Protocol : SNMPV3
User Name : localadmin
Facility Permissions : DEFAULT FACILITY = Read Write
Outlet Realms :
ACL IP Address : ::
ACL IP Mask : ::
Password : localadmin
Auth Password : localadmin
Idle Timeout in Minutes : 0
Session Expiration in Min: 0
1- Name
2- Outlet Permissions
3- SNMP Protocol
4- ACL IP Address
5- ACL IP Mask
6- Password
7- Auth Password
8- Idle Timeout in Minutes
9- Session Expiration in Minutes
A- Apply Changes
X- Security Menu
M- Return to Main Menu
<ENTER> Refresh Menu
>> x
```

Default Users: Program users must have a minimum username length and password of 8 characters.

4. Telnet/SSH Console

Menu Data

localadmin

This is the administrator account and has Read/Write access to all program areas. This user cannot be deleted or its facility access permission be modified, but the username and password may be changed from its default settings. The default password is same as the username.

localmanager

This account has default access as Read/Write to all areas except to the security area of the program. The default password is same as the username.

localguest

This account has read-only access to Device Status, Logging, and Info areas of the program. The default password is same as the username.

public

This account is not a program user. It is an SNMPv1 Read-Only community.

tripplite

This account is not a program user. It is an SNMPv2c Read/Write community. This the default community string that Tripp Lite's PowerAlert Network Shutdown Agent uses to discover Tripp Lite SNMP devices on the network.

Users 6-12 are not defined.

4.2.3.3 RADIUS Servers

This is the section of the menu used to define the RADIUS Servers. There is a maximum of 2 RADIUS Servers that can be defined. If a slot is available to create another server, the address value will be "Server Not Defined".

Radius Servers Summary Menu

```
----- Radius Servers Menu -----
# | Address | Priority | AUTH PORT | ACCT PORT
1 10.0.0.11 1 1812 1813
2 Server Not Defined
#- Radius Server
X- Security Menu
M- Return to Main Menu
<ENTER> Refresh Menu
>> 1
```

Radius Server Detail Menu

```
----- Radius Server Detail Menu -----
Address : 10.0.0.11
Priority : 1
Shared Secret : tripplite
Authentication Port : 1812
Accounting Port : 1813
1- Address
2- Priority
3- Shared Secret
4- Authentication Port
5- Accounting Port
A- Apply Changes
C- Delete Radius Host
X- Radius Servers Menu
M- Return to Main Menu
<ENTER> Refresh Menu
>> x
```

```
----- Radius Servers Menu -----
# | Address | Priority | AUTH PORT | ACCT PORT
1 10.0.0.11 1 1812 1813
2 Server Not Defined
#- Radius Server
X- Security Menu
M- Return to Main Menu
<ENTER> Refresh Menu
```

4. Telnet/SSH Console

Menu Data

<i>Address</i> This defines the internet address of the RADIUS server.	<i>Authentication Port</i> This defines the port on the server to be used for authentication.
<i>Priority</i> This is a number that defines the priority of this RADIUS server.	<i>Accounting Port</i> This defines the port on the server to be used for accounting.
<i>Shared Secret</i> This is the shared secret value to be used with this RADIUS server.	

4.2.3.4 Change Password

This menu is used to allow a user to change his or her user password. The user will be prompted for the old password, then the new password and then finally asked to verify the new password again. The new password will take effect for the next login. For passwords, alphanumeric and the following special characters are allowed: !@#\$%^*(){}[]~_.

4.2.4 Date/Time

```
----- Date/Time -----
Current Date/Time      : 2016-06-01 16:41:40+00:00
Time Source            : Network Time Protocol
Timezone Offset        : Etc/UTC

1- Time Source
2- NTP Settings
3- Time Settings
4- Time Zone
X- System Configuration
M- Return to Main Menu
<ENTER> Refresh Menu
```

4.2.4.1 Time Source Data Entry Menu

This menu will allow the user to switch between using Network Time Protocol (NTP) or Real Time Clock (RTC) for the time. Using NTP, the system will poll an NTP server for the time. Using RTC, the values will be determined from local RTC settings.

```
----- Time Source -----
Time Source : Network Time Protocol
R- Switch To RTC
X- Date/Time
M- Return to Main Menu
<ENTER> Refresh Menu
```

4. Telnet/SSH Console

4.2.4.2 Time Zone

This menu allows the user to select a time zone.

```
----- Time zone -----
Timezone Offset      : Etc/UTC
1- Africa
2- America
3- Antarctica
4- Arctic
5- Asia
6- Atlantic
7- Australia
8- Europe
9- Indian
10- Pacific
X- Date/Time
M- Return to Main Menu
<ENTER> Refresh Menu
```

Menu Data

Time Zone Offset

The time zone offset from UTC. All times are entered as UTC and will be adjusted by the selected offset. Time zone offsets west of UTC are entered as positive numbers, and time zone offsets east of UTC are entered as negative numbers.

4.2.4.3 NTP Settings

This menu allows the user to control the various aspects of using NTP for setting the time and date.

```
----- NTP Settings -----
Primary Address      : 0.pool.ntp.org
Secondary Address    : 1.pool.ntp.org

1- Primary Address
2- Secondary Address
A- Apply Changes
X- Date/Time
M- Return to Main Menu
<ENTER> Refresh Menu
```

Menu Data

Primary Address

This is the address for the primary NTP server. The default is 0.pool.ntp.org.

Secondary Address

This is the address of the secondary NTP server. The default is 1.pool.ntp.org.

4. Telnet/SSH Console

4.2.4.4 Time Settings

This menu allows the user to set the time and date.

```
----- Time Settings -----
Date       : 2016-06-01
Day Of Week : Wednesday
Time       : 16:43:22

1- Date
2- Time
A- Apply Changes
X- Date/Time
M- Return to Main Menu
<ENTER> Refresh Menu
```

Menu Data

Date

This is the current date. The date must be entered in the format YYYY-MM-DD.

Day of Week

This is the current day of the week (Sunday through Saturday).

Time

This is the current time specified in 24-hour clock value for the current local time.

4.2.5 Local Device Discovery

This menu is used to tell the system to attempt to discover any new device connections.

To be able to effectively use this menu, the user should have Write access to the SYSTEM SETTINGS facility.

```
----- Local Device Discovery -----

Discover Serial Devices : Yes

1- Discover Devices Now
X- System Configuration
M- Return to Main Menu
<ENTER> Refresh Menu
```

Menu Data

Discover Serial Devices

This is a display-only data item that indicates devices on serial ports will be discovered.

Discover Devices Now

Start local device discovery.

4. Telnet/SSH Console

4.2.6 Restart PowerAlert Device Manager

The Restart PowerAlert menu provides the end user with an interface to restart the device interface.

Note: If a setting has changed that requires a system restart, the message "Changes have been made to require a restart to take effect" will display on this menu. This message can only be cleared with a restart. Changing the setting back to the original value will not reset this condition. Not all settings that require a restart to take effect display this indicator message.

Several restart options exist:

```
----- Restart PowerAlert -----  
  
1- Restart PowerAlert Now  
2- Reset PowerAlert To Factory Default Settings  
X- System Configuration  
M- Return to Main Menu  
<ENTER> Refresh Menu
```

The first option, *Restart PowerAlert Now*, will perform a simple restart of the device interface. You will be prompted whether or not to continue with the restart operation. Type Y to perform the restart, N to exit without restarting.

The default setting under *Reset PowerAlert to Factory Default Settings* performs a reset, but preserves network settings.

```
----- Reset PowerAlert To Factory Default Settings -----  
  
Preserve Network Settings On Factory : Yes  
  
1- Preserve Network Settings On Factory Default Settings  
2- Restart PowerAlert To Factory Default Settings Now  
X- Restart PowerAlert  
M- Return to Main Menu  
<ENTER> Refresh Menu
```

This option resets all settings to the original factory defaults except for the network settings. Since the LX Platform device has a functioning network connection with the current configuration, the network settings are not cleared. Resetting network settings would potentially disable desired connections to the system.

To change the behavior and Reset PowerAlert to Factory Default Settings (including the network settings), select option 1 and toggle Preserve Network Settings from Yes to No.

```
----- Preserve Network Settings On Factory Default Settings -----  
  
Current Preserve Network Settings On Factory Default Settings = Yes  
  
Enter Y or N for Preserve Network Settings On Factory Default Settings  
X- Leave value unchanged  
M- Return to Main Menu
```

Once the Preserve Network Settings option has been configured, select option 2- *Restart PowerAlert To Factory Default Settings Now*. You will be prompted to continue or exit before the reset will take place.

4. Telnet/SSH Console

4.3 Network Configuration

The Network Configuration menu is used to configure the network-related items such as the IP Configuration of IPV4 and IPV6 Addresses, Remote Services (e.g. Email settings) and the User Access Information, which defines what user service should be run (HTTP, SSH or Telnet).

All changes to the Network Configuration will be enacted upon the next restart of the web card.

```
----- Network Configuration -----  
  
1- IP Configuration  
2- User Access Interfaces  
3- Remote Services  
X/M- Return to Main Menu  
<ENTER> Refresh Menu
```

4.3.1 IP Configuration

This menu allows the user to have full control over the IP settings of the LX Platform device and how it interacts with the network. Both IPV4 and IPV6 addresses are supported.

```
----- IP Configuration -----  
  
Host Name           : poweralert-23b3b1b42451278  
Domain Name         : t1swdev.local  
  
IPV4 Address Information  
=====
```

Method	: dhcp
IPV4 Address	: 10.22.0.127
Subnet Mask	: 255.224.0.0
Gateway	: 10.0.0.1
Manual DNS	: Disabled
Primary DNS	: 10.0.0.11
Secondary DNS	: 10.0.0.8

```
IPV6 Address Information  
=====
```

Method	: dhcp
IPV6 Address	: 2001:db9::828f:8f6e:2fac:7adb
Prefix Length	: 128
Gateway	: ::0
Manual DNS	: Disabled
Primary DNS	: ::0
Secondary DNS	: ::0

```
1- Host Name  
2- Domain Name  
3- IPV4 Settings  
4- IPV6 Settings  
X- Network Configuration  
M- Return to Main Menu  
<ENTER> Refresh Menu
```

4. Telnet/SSH Console

4.3.1.1 Host Name

This is a character string up to 63 characters to be used as the host name for the LX Platform device.

```
----- Host Name -----
Current Host Name = poweralert-236361842451278
Enter a string between 1 and 63 characters for Host Name
X- Leave value unchanged
M- Return to Main Menu
```

4.3.1.2 Domain Data Entry Menu

This menu is used for setting the domain name associated with the LX Platform device.

```
----- Domain Name -----
Current Domain Name = tlsoftwaredev.local
Enter a string between 1 and 67 characters for Domain Name
X- Leave value unchanged
M- Return to Main Menu
```

4.3.1.3 IPV4 Settings

This menu displays current IPV4 settings and allows a user to reconfigure the method, address, subnet mask and gateway of the protocol.

----- IPV4 Settings -----	Menu Data
<pre>Saved IPV4 Address Information ===== Method : dhcp IPV4 Address : 10.22.0.127 Subnet Mask : 255.224.0.0 Gateway : 10.0.0.1 Manual DNS : Disabled Primary DNS : 10.0.0.11 Secondary DNS : 10.0.0.8 Settings On Restart ===== Method : dhcp Manual DNS : Disabled Primary DNS : 10.0.0.11 Secondary DNS : 10.0.0.8 1- Method 2- Manual DNS A- Apply Changes X- IP Configuration M- Return to Main Menu <ENTER> Refresh Menu</pre>	<i>Method</i> The method used to determine the IPV4 Address associated with the LX Platform device. The valid values are STATIC and DHCP. The value STATIC means a user-defined fixed IPV4 address will be used by the card. When this option is chosen, the user must also supply the subnet mask and gateway. The value DHCP (Dynamic Host Configuration Protocol) is used to dynamically assign the IPV4 address at initialization. When the DHCP option is chosen, the user cannot change the subnet mask or the gateway. <i>Address</i> Only applies when method is STATIC. This is the user-defined fixed IPV4 address. <i>Subnet Mask</i> Only applies when method is STATIC. This is the user-defined subnet mask. <i>Gateway</i> Only applies when method is STATIC. This is the user-defined gateway address.

4. Telnet/SSH Console

4.3.1.4 IPV6 Settings

This menu displays current IPV6 settings and allows a user to toggle the dynamic host configuration protocol and method. There can be up to six IPV6 addresses for the card. Only two of these are impacted by this menu. A user may choose to have one IPV6 Address determined through DHCP and one set statically. Any others that appear in the list have been automatically assigned by the card's software. They are shown here because they are valid IP addresses and can be used to route to the card. These addresses will have a method of AUTO.

```
----- IPV6 Settings -----

Saved IPV6 Address Information
=====
Method           : dhcp
IPV6 Address      : 2001:db9::828f:8f6e:2fac:7adb
Prefix Length     : 128
Gateway          : ::0
Manual DNS        : Disabled
Primary DNS       : ::0
Secondary DNS     : ::0

Settings On Restart
=====
Method           : dhcp
Manual DNS        : Disabled
Primary DNS       : ::0
Secondary DNS     : ::0

1- Method
2- Manual DNS
A- Apply Changes
X- IP Configuration
M- Return to Main Menu
<ENTER> Refresh Menu
```

4.3.2 User Access Interfaces

These menus control how the various available LX Platform device interfaces are started.

```
----- User Access Interfaces -----

1- Telnet/SSH
2- Web
3- SNMP
4- FTP/SFTP
X- Network Configuration
M- Return to Main Menu
<ENTER> Refresh Menu
>>
```

4.3.2.1 Telnet/SSH

This menu provides configuration access to the way the user and system interact with the Telnet/SSH interface.

```
----- Telnet/SSH Settings -----

Automatically Start SSH Menu : Yes
SSH Menu Port                : 22
Automatically Start Telnet Menu : Yes
Telnet Menu Port             : 23

1- Automatically Start SSH Menu
2- SSH Menu Port
3- Automatically Start Telnet Menu
4- Telnet Menu Port
A- Apply Changes
X- User Access Interfaces
M- Return to Main Menu
<ENTER> Refresh Menu
>>
```

4. Telnet/SSH Console

Menu Data

Automatically Start SSH Menu

This menu asks if, when the card is started, the SSH Menu application should be automatically started as well. Valid Values:

- **Yes**
Start the application. The default is Yes.
- **No**
Do not start the application.

SSH Menu Port

If the application is to be started, then this is the listening port to use. The default is 22.

Automatically Start Telnet Menu

This menu asks if, when the card is started, the Telnet Menu application should be automatically started as well. Valid Values:

- **Yes**
Start the application. The default value is Yes.
- **No**
Do not start the application.

Telnet Menu Port

If the application is to be started, then this is the listening port to use. The default is 23.

4.3.2.2 Web

```
----- Web Settings -----
Automatically Start HTTPS      : Yes
HTTPS Port                    : 443
Automatically Start HTTP      : Yes
HTTP Port                     : 80

1- Automatically Start HTTPS
2- HTTPS Port
3- Automatically Start HTTP
4- HTTP Port
A- Apply Changes
X- User Access Interfaces
M- Return to Main Menu
<ENTER> Refresh Menu
>>
```

Menu Data

Automatically Start HTTPS

This menu asks if, when the card is started, the HTTPS Web access should be started as well. Valid Values:

- **Yes**
Start the application.
- **No**
Do not start the application.

HTTPS Port

If the application is to be started, then this is the listening port to use. The default is 443.

Automatically Start HTTP

This menu asks if, when the card is started, the HTTP Web access should be started as well. Valid Values:

- **Yes**
Start the application.
- **No**
Do not start the application.

HTTP Port

If the application is to be started, then this is the listening port to use. The default is 80.

4. Telnet/SSH Console

4.3.2.3 SNMP Settings

This menu allows the user to configure SNMP set and get settings.

```
----- SNMP Settings -----
Automatically Start SNMP      : Yes
SNMP Port                    : 161
Enable SNMP V1               : Yes
Enable SNMP V2c              : Yes
Enable SNMP V3               : Yes

1- Automatically Start SNMP
2- SNMP Port
3- Enable SNMP V1
4- Enable SNMP V2c
5- Enable SNMP V3
A- Apply Changes
X- User Access Interfaces
M- Return to Main Menu
<ENTER> Refresh Menu
>>
```

Menu Data

Automatically Start SNMP

This menu asks if, when the card is started, the SNMP application should be started as well. Valid Values:

- **Yes**
Start the application.
- **No**
Do not start the application.

SNMP Port

If the application is to be started, then this is the port to use for SNMP set and get requests.

Enable SNMP V1

This indicates if SNMPv1 should be enabled on card startup.

Enable SNMP V2c

This indicates if SNMPv2c should be enabled on card startup.

Enable SNMP V3

This indicates if SNMPv3 should be enabled on card startup.

Note: The SNMP enable flags will not change the default local users created.

4.3.2.4 FTP/SFTP

This menu allows the user to configure FTP / SFTP settings. The example below shows how to change the (default) setting to disable automatic start up with Secure FTP. Note that this setting is not available with firmware versions before 15.5.2.

```
----- User Access Interfaces -----

1- Telnet/SSH
2- Web
3- SNMP
4- FTP/SFTP
X- Network Configuration
M- Return to Main Menu
<ENTER> Refresh Menu

>> 4

----- FTP/SFTP Settings -----

Automatically Start Secured FTP : Yes

1- Automatically Start Secured FTP
A- Apply Changes
X- User Access Interfaces
M- Return to Main Menu
<ENTER> Refresh Menu

>> 1
```

4. Telnet/SSH Console

```
----- Automatically Start Secured FTP -----  
  
Current Automatically Start Secured FTP = Yes  
  
Enter Y or N for Automatically Start Secured FTP  
X- Leave value unchanged  
M- Return to Main Menu  
  
>> n  
You are requesting this service to be turned off with the next restart.  
Do you wish to turn it off?  
  
Y- Yes, continue and perform operation  
N- Do Not Make Change  
>> y  
  
----- FTP/SFTP Settings -----  
  
Automatically Start Secured FTP : No  
  
1- Automatically Start Secured FTP  
A- Apply Changes  
X- User Access Interfaces  
M- Return to Main Menu  
<ENTER> Refresh Menu
```

4.3.3 Remote Services

This menu provides access to the configuration of the Remote Services provided by the LX Platform device, including distributing notification emails and logs.

```
----- Remote Services -----  
1- Email Settings  
2- Remote Syslog Servers  
3- Auto Probes  
X- Network Configuration  
M- Return to Main Menu  
<ENTER> Refresh Menu
```

4. Telnet/SSH Console

4.3.3.1 Email Settings

```
----- Email Settings -----

Relay Server Settings
Server Name           :
Port                  : 25
Authentication Login Name :
Authentication Password :

Authentication Methods
Digest MD5 Authentication Supported: Yes
CRAM MD5 Authentication Supported  : Yes
Login Authentication Supported     : Yes
Plain Authentication Supported     : Yes

Message Data
From Address           : poweralert@tripplite.com
Subject                : PowerAlert Notification

1- Server Name
2- Port
3- Authentication Login Name
4- Authentication Password
5- Digest MD5 Authentication Supported
6- CRAM MD5 Authentication Supported
7- Login Authentication Supported
8- Plain Authentication Supported
9- From Address
10- Subject
A- Apply Changes
X- Remote Services
M- Return to Main Menu
<ENTER> Refresh Menu
```

Menu Data

Server Name

This defines the email server address information used for sending out email messages.

Port

This defines the port on the email server used for sending out email messages.

Authentication Login Name

If authentication is required by the email server, this is the login name to use. This is optional.

Authentication Password

If authentication is required by the email server, this is the password for the authentication login name. If an Authentication Login Name is specified, then the Authentication Password must also be provided.

Digest MD5 Authentication Supported

This indicates if the email server supports Digest MD5 Authentication.

CRAM MD5 Authentication Supported

This indicates if the email server supports CRAM MD5 Authentication.

Login Authentication Supported

This indicates if the email server supports Login Authentication.

Plain Authentication Supported

This indicates if the email server supports Plain Authentication.

From Address

This is the information to be used as the "From" address in the message.

Subject

This is the information to be used as the "Subject" line in the message.

4. Telnet/SSH Console

4.3.3.2 Remote Syslog Servers

These settings are used to define the remote syslog servers to send log entries. There are a maximum of four remote syslog servers that can be defined. To enforce this maximum, there are four predefined slots for the servers. An available slot will have a blank Host value and default values for Port, Log Level and Facility. Once all of those slots are used, no more may be defined. To add a new server to a slot, the user will select the number for the slot and then will be prompted for all of the values for that server. When a slot is chosen for a defined remote server, the detail menu for that server will be displayed.

```
----- Remote Syslog Servers -----  
  
-----  
# | Host | Port | Log Level | Facility  
-----  
1 |      | 514  | disabled  | 23  
2 |      | 514  | disabled  | 23  
3 |      | 514  | disabled  | 23  
4 |      | 514  | disabled  | 23  
  
#- Remote Syslog Server  
X- Remote Services  
M- Return to Main Menu  
<ENTER> Refresh Menu  
  
----- Remote Syslog Server -----  
  
Host          : remotesysloghost  
Port          : 514  
Log Level     : info  
Facility      : 23  
Application Logging : Yes  
Event Logging : Yes  
Data Logging  : Yes  
  
1- Host  
2- Port  
3- Remote Syslog Severity Level  
4- Facility  
5- Application Logging  
6- Event Logging  
7- Data Logging  
A- Apply Changes  
C- Clear Syslog Server  
X- Remote Syslog Servers  
M- Return to Main Menu  
<ENTER> Refresh Menu  
  
>> a
```

4. Telnet/SSH Console

Menu Data

Host

Host Name or IP address for the Remote Syslog server.

Port

This defines the port for the Remote Syslog server. The default is 514.

Log Level

The supported values are:

- Disabled – no logging to this server
- Emergency
- Alert
- Critical
- Error
- Warning
- Notice
- Info
- Debug
- Trace

The values in this list are equivalent to the Severity values as defined in RFC 4524. The two values that do not match our choices are “Disabled,” which is used to turn off logging to the server without removing the definition, and “Trace” which is a more detailed severity level for debug. This will be mapped to the Debug Syslog Severity level. The default log level is “Disabled.”

Facility

The logging facility values are the Syslog facilities as defined in RFC 5424.

Numerical Code	Facility
0	kernel messages
1	user-level messages
2	mail system
3	system daemons
4	security/authorization messages
5	messages generated internally by syslogd
6	line printer subsystem
7	network news subsystem
8	UUCP subsystem
9	clock daemon
10	security/authorization messages
11	FTP daemon
12	NTP subsystem
13	log audit
14	log alert
15	clock daemon
16	local use 0 (local0)
17	local use 1 (local1)
18	local use 2 (local2)
19	local use 3 (local3)
20	local use 4 (local4)
21	local use 5 (local5)
22	local use 6 (local6)
23	local use 7 (local7)

The default logging facility is 23.

4. Telnet/SSH Console

Example of assigning a new Remote Syslog Server

```
>> 1
----- Remote Syslog Server -----
----- Host -----
Current Host =
Enter a string between 1 and 128 characters for Host
>> sysloghost

----- Port -----
Current Port = 514
Enter an integer value for Port
>> 514

----- Remote Syslog Severity Level -----
Current Remote Syslog Severity Level =
1- Disabled
2- Emergency
3- Alert
4- Critical
5- Error
6- Warning
7- Notice
8- Info
9- Debug
10- Trace
X- Return to Remote Syslog Servers
>> 8

----- Facility -----
Current Facility = 23
Enter an integer between 1 and 23 for Facility
>> 23

----- Application Logging -----
Current Application Logging = Yes
Enter Y or N for Application Logging
>> y

----- Event Logging -----
Current Event Logging = No
Enter Y or N for Event Logging
>> y

----- Data Logging -----
Current Data Logging = No
Enter Y or N for Data Logging
>> y

----- Remote Syslog Server -----
Host                : sysloghost
Port                : 514
Log Level           : info
Facility            : 23
Application Logging  : Yes
Event Logging       : Yes
Data Logging        : Yes

1- Host
2- Port
3- Remote Syslog Severity Level
4- Facility
5- Application Logging
6- Event Logging
7- Data Logging
A- Apply Changes
C- Clear Syslog Server
X- Remote Syslog Servers
M- Return to Main Menu
<ENTER> Refresh Menu
```

4. Telnet/SSH Console

4.3.3.3 Auto Probes

The Auto Probe feature allows for the automatic execution of an action when triggered by an unsuccessful confirmation of network connectivity, using Ping and/or NTP probes. For example, an LX Platform PDU can be configured to ping a router over the network; if the router fails to respond, the PDU will automatically power cycle one of its outlets – to which the router is connected – thereby power cycling the router.

When an Auto Probe is added, an event bearing the name of the probe is automatically associated to it. As with other events, actions can be added to the Auto Probe event via the Web or menu interfaces and/or CLI . Email, SNMP trap and logging actions are associated with Auto Probes, as a default

Note: This feature is not available with firmware versions before 15.5.2.

```
----- Remote Services -----
1- Email Settings
2- Remote Syslog Servers
3- Auto Probes
X- Network Configuration
M- Return to Main Menu
<ENTER> Refresh Menu

>> 3

----- Auto Probes -----

-----
# | Name | Type | Primary Address | Interval | Retries | Status
-----
1 | Ping Watchdog | Ping | 10.22.0.1 | 3 | 5 | Okay
2 | NTP Watchdog | NTP | 10.22.0.2 | 15 | 3 | Fault
3 | Probe 3 | NTP | 10.22.0.5 | 3 | 5 | InitFl
4 | Probe 4 | NTP | 10.22.0.6 | 15 | 4 | Okay

#- Auto Probe
0- Add New Auto Probe
X- Remote Services
M- Return to Main Menu
<ENTER> Refresh Menu

>> 1

----- Auto Probes -----

-----
# | Name | Type | Primary Address | Interval | Retries | Status
-----
1 | Ping Watchdog | Ping | 172.17.48.192 | 3 | 3 | Okay
2 | NTP Watchdog | NTP | 10.22.0.1 | 3 | 3 | Off

#- Auto Probe
0- Add New Auto Probe
X- Remote Services
M- Return to Main Menu
<ENTER> Refresh Menu

>> 2

----- Auto Probe Detail Menu -----
Type : NTP
Name : NTP Watchdog
Description : Default Watchdog NTP Probe
Primary Address : 10.22.0.1
Primary Port : 123
Secondary Address : 12.22.0.2
Secondary Port : 123
Interval : 3
Retries : 3
Enabled : No
```

4. Telnet/SSH Console

```
1- Name
2- Description
3- Primary Address
4- Primary Port
5- Secondary Address
6- Secondary Port
7- Interval
8- Retries
9- Enabled
A- Apply Changes
C- Clear Auto Probe
X- Auto Probes
M- Return to Main Menu
<ENTER> Refresh Menu
```

Menu Data

Probe Detail

Multiple probes may be defined to perform a selected action, such as verifying network connectivity or turning on/off a specified outlet.

- **Name**
This is an editable string for naming the probe
- **Description**
This is an editable string for describing the probe
- **Primary Address**
This is the primary IPv4 address to which the probe will be sent.
- **Primary Port**
This is the port associated with the primary address.
- **Secondary Address**
This is the secondary IPv4 address to which the probe will be sent.
- **Secondary Port**
This is the port associated with the secondary address.
- **Interval**
This defines how often, in minutes, the probe will be sent.
- **Retries**
This is the number of times that the probe request fails before considering the test to be a failure.
- **Enabled**
This enables or disables the probe

Note: For a Ping Probe, Ports (Primary and Secondary) are not required.

Add New Probe

Below is an example of creating and enabling an NTP probe

```
----- Auto Probes -----
# | Name | Type | Primary Address | Interval | Retries | Status
1 | Ping Watchdog | Ping | 10.22.0.1 | 3 | 5 | Okay
2 | NTP Watchdog | NTP | 10.22.0.2 | 15 | 3 | Fault
3 | Probe 3 | NTP | 10.22.0.5 | 3 | 5 | InitF1
4 | Probe 4 | NTP | 10.22.0.6 | 15 | 4 | Okay

#- Auto Probe
0- Add New Auto Probe
X- Remote Services
M- Return to Main Menu
<ENTER> Refresh Menu
```

>> 0

4. Telnet/SSH Console

```
----- Auto Probe Detail Menu -----
----- Auto Probe Type Selection -----
      1 - NTP
      2 - Ping
>> 1

----- Name -----
      Current Name =
      Enter a string between 1 and 32 characters for Name
>> Probe 5

----- Description -----
      Current Description =
      Enter a string between 1 and 128 characters for Description
>> Cycle Load 5

----- Primary Address -----
      Current Primary Address =
      Enter a string between 1 and 255 characters for Probe Address
>> 10.2.0.2

Note: Probe Primary Port is omitted for Ping Probe.

----- Probe Primary Port-----
      Current Port = 0
      Enter an integer between 1 and 65535 for Probe Primary Port
>> 123

----- Secondary Address -----
      Current Secondary Address =
      Enter a string between 1 and 255 characters for Secondary Address
>> 10.2.0.3

Note: Probe Secondary Port is omitted for Ping Probe.

----- Secondary Port-----
      Current Port = 0
      Enter an integer between 1 and 65535 for Secondary Port
>> 123

----- Interval -----
      Current Interval = 3
      Enter an integer between 3 and 1440 for Interval
>> 45

----- Retries -----
      Current Retries = 3
      Enter an integer between 3 and 10 for Retries
>> 3
```

4. Telnet/SSH Console

```
----- Enabled -----

Current Enabled = No
Enter Y or N for Enabled

>> y

----- Auto Probe Detail Menu -----
Type           : NTP
Name           : Probe 5
Description    : Cycle Load 5
Primary Address : 10.2.0.2
Primary Port   : 123
Secondary Address : 10.2.0.3
Secondary Port : 123
Interval      : 45
Retries       : 3
Enabled       : Yes
1 - Type
2 - Name
3 - Description
4 - Primary Address
5 - Primary Port
6 - Secondary Address
7 - Secondary Port
8 - Interval
9 - Retries
10 - Enabled
A - Apply Changes
D - Delete
X - Auto Probes
M - Return to Main Menu
<ENTER> Refresh Menu

>> a

----- Auto Probes -----

-----
# | Name | Type | Primary Address | Interval | Retries | Status
-----
1 | Ping Watchdog | Ping | 10.22.0.1 | 3 | 5 | Okay
2 | NTP Watchdog | NTP | 10.22.0.2 | 15 | 3 | Fault
3 | Probe 3 | NTP | 10.22.0.5 | 3 | 5 | InitF1
4 | Probe 4 | NTP | 10.22.0.6 | 15 | 4 | Okay
5 | Probe 5 | Ping | 10.10.10.10 | 5 | 8 | Unk

#- Auto Probe
D- Add New Auto Probe
X- Remote Services
M- Return to Main Menu
<ENTER> Refresh Menu

>>

The Status column will display one of the following states:

Off - the probe is disabled

Okay – a connection has been established and the probe is active

Fault – a connection had been established but subsequently failed

InitFI – initial connection failed.

Unk – Unknown state. This occurs when an initial connection has not yet been established, i.e. after a reboot, when a new probe is enabled, and when a previously disabled probe is re-enabled.
```

4. Telnet/SSH Console

Associating an Action to an Auto-Probe

In the following example, the action of Cycle All Loads is associated with the Auto-Probe created in the above example.

```
----- Main Menu -----
1- Devices
2- System Configuration
3- Network Configuration
4- Alarms and Logging
5- About
E- Launch CLI
Q- Logout
<ENTER> Refresh Menu

>> 2

----- System Configuration -----
1- Address Book
2- Global Actions
3- Security
4- Date/Time
5- EnergyWise Settings
6- Local Device Discovery
7- Restart PowerAlert
X/M- Return to Main Menu
<ENTER> Refresh Menu

>> 2

----- Global Actions -----
1- Action Profiles
2- Schedules
X- System Configuration
M- Return to Main Menu
<ENTER> Refresh Menu

>> 1

----- Action Profiles Menu -----
1- Email Notification Profiles
2- Device Shutdown Profiles
3- SNMP Set OID Profiles
4- SNMP Trap Notification Profiles
5- Load Control Action Profiles
6- Ramp Action Profiles
7- Shed Action Profiles
8- Control Execution Action Profiles
X- Global Actions
M- Return to Main Menu
<ENTER> Refresh Menu

>> 8
```

4. Telnet/SSH Console

```
----- Control Execution Action Profiles -----  
  
-----  
# | Name | DELAY  
-----  
1 Default Reboot Control Action 30  
Device Number: 1  
  
#- Edit Profile  
0- Add New Profile  
X- Action Profiles Menu  
M- Return to Main Menu  
<ENTER> Refresh Menu  
  
>> 0  
  
----- Device 1 Control Execute Action Profile Detail -----  
  
----- Action Profile Name -----  
  
Current Action Profile Name =  
Enter a string for Action Profile Name  
  
>> Auto-Probe Cycle All Loads  
  
----- Action Profile Delay in Seconds -----  
  
Current Action Profile Delay in Seconds =  
Enter an integer value for Action Profile Delay in Seconds  
  
>> 5  
  
----- Select Device Control -----  
  
1 Turn All Loads Off  
2 Reboot SNMP Card  
3 Reboot Device  
4 Initiate Self Test  
5 Turn All Loads On  
6 Cycle All Loads  
  
>> 6  
  
----- Device 1 Control Execute Action Profile Detail -----  
  
Name: Auto-Probe Cycle All Loads  
Delay: 5  
Device: 1  
Control Executed: Cycle All Loads  
  
1- Modify Profile Name  
2- Modify Delay  
A- Apply Changes  
D- Delete  
X- Device Control Execute Action Profiles Menu  
M- Return to Main Menu  
<ENTER> Refresh Menu  
  
>> a
```

4. Telnet/SSH Console

```
----- Device 1 Control Execute Action Profile Detail -----
Name: Auto-Probe Cycle All Loads
Delay: 5
Device: 1
Control Executed: Cycle All Loads

1- Modify Profile Name
2- Modify Delay
3- Apply To Device Events
A- Apply Changes
D- Delete
X- Device Control Execute Action Profiles Menu
M- Return to Main Menu
<ENTER> Refresh Menu

>> 3

----- Actions Set/Clear -----

S- Use Action For Only Set Alarm Condition
B- Use Action For Both Set and Clear Action
X- None
M- Return to Main Menu
<ENTER> Refresh Menu

>> s
Would you like to choose a clear action now

Y- Yes, continue and perform operation
N- Do Not Make Change

>> n

----- Apply To Device Events -----

Set Action          : Auto-Probe Cycle All Loads
Clear Action        :

1- Apply To All Device Events
2- Device0001
X- None
M- Return to Main Menu
<ENTER> Refresh Menu

>> 2

----- Action Events -----

Set Action          : Auto-Probe Cycle All Loads
Clear Action        :
Events Chosen       : None

1- Apply To All Events
2- Clear Event List
3- Add Event To List
4- Delete Event From List
X- Apply To Device Events
M- Return to Main Menu
<ENTER> Refresh Menu

>> x
```

4. Telnet/SSH Console

----- Apply To Device Events -----

Set Action : Auto-Probe Cycle All Loads
Clear Action :

1- Apply To All Device Events
2- Device0001
X- None
M- Return to Main Menu
<ENTER> Refresh Menu

>> m

----- Main Menu -----

1- Devices
2- System Configuration
3- Network Configuration
4- Alarms and Logging
5- About
E- Launch CLI
Q- Logout
<ENTER> Refresh Menu

>> 1

----- Device 1 -----

Device Name	: Device0001	Region	:
Location	:	Product	: SMART500RT1U
Vendor	: TRIPPLITE	Date Installed	: 2018-01-16
Protocol	: 3005	Type	: UPS
State	: NORMAL	Port Name	: /dev/ttyS2
Port Mode	: RS232	Keyword	: ups
Role	: UPS		
Importance	: 1	Serial Number	:
Firmware Version	: 29AF (Rev A)	Self Test Date	:
Device ID	: 65535		
Self Test Status	: No Test		

1- Status
2- Identification
3- Controls
4- Events
5- Loads
6- Preferences and Thresholds
7- Device Alarms
8- Logs
X/M- Return to Main Menu
<ENTER> Refresh Menu

>> 4

4. Telnet/SSH Console

----- Device Events Menu -----

#	CATEGORY	DESCRIPTION	ENABLED
1	WARNING	Load Level Above Threshold	Yes
2	WARNING	On Battery	Yes
3	CRITICAL	Battery Low	Yes
4	WARNING	Battery Capacity Below Warning Level	Yes
5	CRITICAL	Overload	Yes
6	WARNING	Temperature High	Yes
7	CRITICAL	Output Off	Yes
8	WARNING	Self Test Failed	Yes
9	INFORMATION	Battery Age Above Threshold	Yes
10	INFORMATION	Communications Lost	Yes
11	WARNING	Loads Not All On	Yes
12	WARNING	Load 01 Off	Yes
13	WARNING	Ping Watchdog Ping Probe Failed	Yes
14	WARNING	NTP Watchdog NTP Probe Failed	Yes

#- Select Event
X- Device Main Menu
M- Return to Main Menu
<ENTER> Refresh Menu

>> 14

----- Device Event Menu -----

Event Set Name : NTP Watchdog NTP Probe Failed
Event Clear Name : NTP Watchdog NTP Probe 0k
Event Category : WARNING
Event Enabled : Yes
Event Logging : Off

Set Action Clear Action

Default Reboot Control Ac

1- Manage Actions
2- Modify Event Category
3- Disable Event
4- Enable Logging for Event
X- Device Events Menu
M- Return to Main Menu
<ENTER> Refresh Menu

>> 1

----- Device Event Actions -----

Set Action Clear Action

1 Default Reboot Control Ac

#- Modify Event Set/Clear Actions
0- Add new Event Set/Clear Actions
X- Device Events
M- Return to Main Menu
<ENTER> Refresh Menu

>> 0

4. Telnet/SSH Console

```
----- Device Event Action Menu -----

Event          : NTP Watchdog NTP Probe Failed
Event Clear    : NTP Watchdog NTP Probe 0k
Event Action   :
Event Clear Action :

1- Choose Set Action
2- Choose Clear Action
3- Choose Action For Both Set and Clear
A- Apply Changes
D- Delete the Event Action
X- Device Event Menu
M- Return to Main Menu
<ENTER> Refresh Menu

>> 1

----- Device Event Action Selection Menu -----

1- Email Notification Profiles
2- Device Shutdown Profiles
3- SNMP Set OID Profiles
4- SNMP Trap Notification Profile
5- Load Control Action Profiles
6- Shed Action Profiles
7- Control Execution Action Profiles
X- Device Event Action Menu
M- Return to Main Menu
<ENTER> Refresh Menu

>> 7

----- Control Execution Action Profiles -----

-----
# | Name | DELAY
-----
1 | Default Reboot Control Action | 30
2 | Auto-Probe Cycle All Loads | 5

#- Choose Profile
D- Add New Profile
X- Event Action Menu
M- Return to Main Menu
<ENTER> Refresh Menu

>> 2
Would you like to choose a clear action now

Y- Yes, continue and perform operation
N- Do Not Make Change

>> n

----- Device Event Action Menu -----

Event          : NTP Watchdog NTP Probe Failed
Event Clear    : NTP Watchdog NTP Probe 0k
Event Action   : Auto-Probe Cycle All Loads
Event Clear Action :

1- Choose Set Action
2- Choose Clear Action
3- Choose Action For Both Set and Clear
A- Apply Changes
D- Delete the Event Action
X- Device Event Menu
M- Return to Main Menu
<ENTER> Refresh Menu

>> a
```

4. Telnet/SSH Console

```
----- Device Event Actions -----
# Set Action          Clear Action
-----
1 Default Reboot Control Ac
2 Auto-Probe Cycle All Load

#- Modify Event Set/Clear Actions
0- Add new Event Set/Clear Actions
X- Device Events
M- Return to Main Menu
<ENTER> Refresh Menu
```

4.4 Alarms and Logging

This menu allows for in-depth viewing, configuration and acknowledgement of logs and alarms that come across the system.

Alarms and Logging

```
----- Alarms and Logging -----
1- Alarms
2- View Logs
3- Logging Settings
X/M- Return to Main Menu
<ENTER> Refresh Menu
```

4.4.1 Alarms

This menu provides a summary of all alarm conditions, where they have occurred and whether they have been acknowledged.

Alarm Summary

```
----- Alarm List -----

Auto Acknowledge Alarms: On

#      Device      Alarm Detail      ACT      ACK
-----
536    1           Loads Not All On   Yes      Yes
537    1           Load On Off       Yes      Yes

#- Alarm Id
A- Acknowledge All Alarms
D- Disable Alarm Auto Acknowledgement
X- Alarms and Logging
M- Return to Main Menu
<ENTER> Refresh Menu
```

Menu Data

Auto-Acknowledge Alarms

This is a system-wide setting that will automatically acknowledge every alarm on the system. This will force alarm entries to be removed as soon as the alarm condition clears. This setting should be enabled if using with PowerAlert Network Management System (PANMS) or the PowerAlert Network Shutdown Agent (PANSA).

Acknowledge All Alarms

This option gives the user the ability to acknowledge all of the active alarms. Any inactive, unacknowledged alarms will be deleted when this is done. The alarms acknowledged will be marked as such. When the alarm condition clears, it will be removed.

4. Telnet/SSH Console

4.4.1.1 Alarm Details

The detail for each alarm can be displayed by choosing its ID. Once it is displayed, the user has the option to acknowledge that alarm only.

<i>Alarm ID</i> This is a number that uniquely identifies the alarm.	<i>Active</i> This indicates if the alarm condition is still present
<i>Device ID</i> This is the numeric device ID with the alarm condition. This value will be 0 if the alarm does not apply to a specific device but is associated with the system as a whole.	<i>Time</i> This is the time that the alarm event occurred.
<i>Detail</i> This is the text description of the alarm condition.	<i>Time Cleared</i> This is only displayed for inactive alarms. It is the time that the alarm condition cleared.
<i>Category</i> This is the severity level category. Alarm categories are: • CRITICAL • WARNING • INFORMATION • STATUS • OFFLINE	<i>Acknowledged</i> This indicates if the alarm has already been acknowledged.

4.4.2 View Logs

This section of the document allows the user to view the event and data log for the entire system.

```
----- View Logs -----  
  
1- Data Log  
2- Event Log  
3- Accounting Log  
X- Alarms and Logging  
M- Return to Main Menu  
<ENTER> Refresh Menu  
  
>>
```

4. Telnet/SSH Console

4.4.2.1 Data Log

View the data logs for the system. The data log will log only variables marked in the system to be logged.

```
----- Data Log -----  
  
Order           : Descending  
Filter          : None  
Time Range      : Display All Entries  
  
V- Start Viewing Log  
O- Change Viewing Options  
C- Clear Log (Force Rotation)  
X- Logs Menu  
M- Return to Main Menu  
<ENTER> Refresh Menu
```

Data Log Viewing Options

```
----- Log Viewing Options -----  
  
Order           : Descending  
Filter          : None  
Time Range      : Display All Entries  
  
1- Display Order  
2- Filter  
3- Choose Time Range  
R- Reset To Defaults  
X- Data Log  
M- Return to Main Menu  
<ENTER> Refresh Menu
```

Menu Data

Start Viewing Log

Choosing this option will begin the data log display using the various viewing options chosen. A maximum of 10 entries will be displayed at a time. Once viewing is started, the user has the option to display the next set of entries or reverse the viewing order to go back. The next option will be offered until there are no more entries to be displayed.

Display Order

The logs may be displayed in ascending or descending order by time. The default is to view the log in descending order with the newest entries displayed first.

Filter

The log entries displayed can be limited by applying a filter. Only entries that match the filter criteria will be displayed. The data log can be filtered on device variables. The variables may be all variables for all devices (default), all variables on one specific device or up to three specific variables that are either across all devices or applied to a single device.

Data Log Filter Menu Example

```
----- Data Log Filter -----  
  
Filter          : None  
  
1- Device Variable  
C- Clear Filter  
X- Log Viewing Options  
M- Return to Main Menu  
<ENTER> Refresh Menu  
  
>> 1
```

4. Telnet/SSH Console

```
----- Device Selection Menu -----  
  
1- Choose from All Device Variables  
2- Choose Variables From Device0001 (SU1500RTXL2U)  
3- Choose Variables From Sensor0002 (E2MTHDI)  
4- Choose Variables From Sensor0003 (E2MTDI)  
X- Data Log Filter  
M- Return to Main Menu  
<ENTER> Refresh Menu
```

>> 2

Data Log Filter Device Variable Selection Menu Example

```
----- Device Variable -----  
  
Filter on a maximum of 3 variables.  
Filter On          : Only Variables for Device 1  
  
1- Battery Charge Remaining  
2- Battery Minutes Remaining  
3- Battery Temperature (C)  
4- Battery Temperature (F)  
5- Battery Voltage  
6- Input Voltage  
7- Input Voltage 1  
8- Input Voltage 12  
9- Input Voltage 2  
10- Input Voltage 3  
11- Output Current  
12- Output Current 1  
13- Output Current 2  
14- Output Current 3  
15- Output Load  
16- Output Load 1  
17- Output Load 2  
18- Output Load 3  
19- Self Test Date  
X- Data Log Filter  
M- Return to Main Menu  
<ENTER> Refresh Menu
```

Choose Time Range

Display Order

This determines the way the log is displayed. Options are Ascending and Descending.

Filter

The log can be filtered on a maximum of three variables.

Start Date

This sets the starting date for a range of log entries to be displayed. Enter the date in the form YYYY-MM-DD.

Start Time

This sets the starting time for a range of log entries to be displayed. Enter a 24-hour clock time in the form HH:MM[:SS].

End Date

This sets the ending date for a range of log entries to be displayed. Enter the date in the form YYYY-MM-DD.

End Time

This sets the ending time for a range of log entries to be displayed. Enter a 24-hour clock time in the form HH:MM[:SS].

Clear Time Range

This removes any previously applied Time Ranges.

4. Telnet/SSH Console

4.4.2.2 Event Log

This menu allows the user to view the event log entries for the entire system.

```
----- Event Log -----
Order      : Descending
Category   : All
Time Range : Display All Entries
V- Start Viewing Log
O- Change Viewing Options
C- Clear Log (Force Rotation)
X- Logs Menu
M- Return to Main Menu
<ENTER> Refresh Menu

>>
```

Start Viewing Log

Choosing this option will begin the data log display. Only 10 entries will be displayed at a time using the various viewing options chosen. Once viewing is started, the user has the option to display the next set of entries or reverse the viewing order to go back. The next option will be offered until there are no more entries to be displayed.

```
----- Display Event Log -----

Display Order: Descending

Date: 2016-06-04
#      Category      Time      Device      Description
=====
329    WARNING        10:07:10    1          Self Test Failed
328    CRITICAL        10:07:07    1          Output Off
327    INFO           10:07:04    2          Temperature Okay
326    CRITICAL        10:07:02    2          Temperature Beyond Limits
325    INFO           10:06:59    1          Battery Age Above Threshold

N- Next Page
X- Event Log
M- Return to Main Menu
<ENTER> Refresh Menu

>>
```

Menu Data

The event entries are grouped by the date the events occurred. When the date changes, a new date heading is printed.

(Event ID)

This is the ID of the event.

Category

This is the severity category of the event. The possible values for the event category are:

- NORMAL
- CRITICAL
- WARNING
- INFORMATION
- STATUS
- OFFLINE

Time

This is the time the event occurred.

Device ID

For an event that occurs on a specific device, this is the ID of that device.

Description

This is a text description of the event that occurred.

4. Telnet/SSH Console

Change Viewing Options

Changing the viewing options will allow the user to decide the order to view the log, as well as define filters to limit logs to be viewed. These options are active only for the single instance of viewing the log and are not persisted.

```
----- Log Viewing Options -----
Order       : Descending
Category    : All
Time Range  : Display All Entries
1- Display Order
2- Category
3- Choose Time Range
R- Reset To Defaults
X- Event Log
M- Return to Main Menu
<ENTER> Refresh Menu

>>
```

Menu Data

Display Order

This is the order, by date and time, that the events will be displayed. The valid values are Ascending and Descending. The default value is Descending.

Category

The Category field allows the user to limit which event logs display by limiting the severity categories. Multiple categories may be chosen to be displayed.

Example Menus for Choosing Multiple Event Categories

```
----- Device Event Category -----
1- NORMAL
2- CRITICAL
3- WARNING
4- INFORMATION
5- STATUS
6- OFFLINE
X- Device Event Menu
M- Return to Main Menu
<ENTER> Refresh Menu

>> 2

----- Device Event Category -----
Current Selected Categories: CRITICAL
1- NORMAL
2- WARNING
3- INFORMATION
4- STATUS
5- OFFLINE
C- Clear Selection
X- Device Event Menu
M- Return to Main Menu
<ENTER> Refresh Menu

>> 2

----- Device Event Category -----
Current Selected Categories: CRITICAL, WARNING
1- NORMAL
2- INFORMATION
3- STATUS
4- OFFLINE
C- Clear Selection
X- Device Event Menu
M- Return to Main Menu
<ENTER> Refresh Menu

>> 2
```

4. Telnet/SSH Console

```
----- Device Event Category -----
Current Selected Categories: CRITICAL, WARNING, INFORMATION
1- NORMAL
2- STATUS
3- OFFLINE
C- Clear Selection
X- Device Event Menu
M- Return to Main Menu
<ENTER> Refresh Menu
>> 2
----- Device Event Category -----
Current Selected Categories: CRITICAL, WARNING, INFORMATION, STATUS
1- NORMAL
2- OFFLINE
C- Clear Selection
X- Device Event Menu
M- Return to Main Menu
<ENTER> Refresh Menu
>> 2
----- Device Event Category -----
Current Selected Categories: CRITICAL, WARNING, INFORMATION, STATUS, OFFLINE
Maximum Number Of Categories Selected
C- Clear Selection
X- Device Event Menu
M- Return to Main Menu
<ENTER> Refresh Menu
>>
```

Choose Time Range

Display Order

This determines the way the log is displayed. Options are Ascending and Descending.

Filter

The log can be filtered on a maximum of three variables.

Start Date

This sets the starting date for a range of log entries to be displayed. Enter the date in the form YYYY-MM-DD.

Start Time

This sets the starting time for a range of log entries to be displayed. Enter a 24-hour clock time in the form HH:MM[:SS].

End Date

This sets the ending date for a range of log entries to be displayed. Enter the date in the form YYYY-MM-DD.

End Time

This sets the ending time for a range of log entries to be displayed. Enter a 24-hour clock time in the form HH:MM[:SS].

Clear Time Range

This removes any previously applied Time Ranges.

4. Telnet/SSH Console

4.4.3 Logging Settings

This section defines the preference settings for the various types of logs. These settings include maximum log file sizes, logging severity levels and actions to take when the log is rotated.

```
----- Logging Settings -----  
  
1- Accounting Log  
2- Application Log  
3- Data Log  
4- Event Log  
5- Logging Report Format  
X- Alarms and Logging  
M- Return to Main Menu  
<ENTER> Refresh Menu  
  
>>
```

4.4.3.1 Accounting Log Settings

```
----- Accounting Log -----  
  
Maximum Entries           : 1024  
Actions On Rotate         : No Actions Defined  
  
1- Maximum Entries  
2- Actions On Rotate  
X- Logging Settings  
M- Return to Main Menu  
<ENTER> Refresh Menu  
  
>>
```

Menu Data

Maximum Entries

This is the maximum number of entries that can be in the log before it is rotated. Valid values are integers between 64 and 1024. The default value is 1024.

Actions on Rotate

This defines the actions to take when the log is rotated. The accounting log may be archived by sending to a single destination using email or HTTP. The log may be sent to multiple destinations by creating multiple actions.

4.4.3.2 Application Log Settings

```
----- Application Log -----  
Console Log Severity Level : Info  
  
1- Console Log Severity Level  
X- Logging Settings  
M- Return to Main Menu  
<ENTER> Refresh Menu  
  
>> 1
```

Menu Data

Console Log Severity Level

This is the minimum level of severity that is logged. For example, if "Error" level is chosen, then "Error," "Critical," "Alert" and "Emergency" logs will be displayed on the console log.

The valid logging levels for the console log are:

- | | |
|-------------|-----------------|
| • Disabled | • Warning |
| • Emergency | • Notice |
| • Alert | • Info(default) |
| • Critical | • Debug |
| • Error | • Trace |

4. Telnet/SSH Console

4.4.3.3 Data Log Settings

The data log settings are used to define the maximum data log size and actions to take when the log is rotated.

```
----- Data Log -----  
  
Maximum Entries           : 1024  
Actions On Rotate        : No Actions Defined  
  
1- Maximum Entries  
2- Actions On Rotate  
X- Logging Settings  
M- Return to Main Menu  
<ENTER> Refresh Menu
```

Menu Data

Maximum Entries

The maximum number of entries that can be in the log before it is rotated. The valid values are an integer between 64 and 1024. The default value is 1024.

Actions On Rotate

This defines the actions to take when the log is rotated. The log data may be archived by sending to a single destination using email or HTTP. The log may be sent to multiple destinations by creating multiple actions.

```
----- Actions On Rotate -----  
  
#      Format      Protocol      Delivery Target  
-----  
1      log         smtp         Admin John Doe  
  
#- Edit Rotate Action  
0- Add New Rotate Action  
X- Data Log  
M- Return to Main Menu  
<ENTER> Refresh Menu  
  
----- Rotate Action -----  
  
Format           : log  
Protocol         : smtp  
Delivery Target  : Admin John Doe  
  
1- Protocol  
2- Delivery Target  
A- Apply Changes  
D- Delete  
X- Actions On Rotate  
M- Return to Main Menu  
<ENTER> Refresh Menu
```

4. Telnet/SSH Console

Menu Data

Protocol

This defines the protocol to use when sending the data log file. The valid values are:

- SMTP – email to destination
- HTTP – use HTTP to send to destination

Destination

This field is used to select the destination for the data log file. When the protocol is SMTP, the destination will be an email contact. When the protocol is HTTP, the destination will be an HTTP contact.

If no contacts have been created, or the desired destination has not already been created, the user may create a new destination from this menu. The contacts added here are then also available for use on other menus using the contacts, i.e., the email notification actions.

4.4.3.4 Event Log Settings

The event log settings are used to define the maximum event log size and actions to take when the log is rotated.

```
----- Event Log -----
Maximum Entries           : 1024
Actions On Rotate         : No Actions Defined

1- Maximum Entries
2- Actions On Rotate
X- Logging Settings
M- Return to Main Menu
<ENTER> Refresh Menu
```

Menu Data

Maximum Entries

The maximum number of entries that can be in the log before it is rotated. The valid values are an integer between 64 and 1024. The default value is 1024.

Actions On Rotate

This defines the actions to take when the log is rotated. The log data may be archived by sending to a single destination using email or HTTP. The log may be sent to multiple destinations by creating multiple actions.

```
----- Actions On Rotate -----
#      Format      Protocol      Delivery Target
-----
1      xml         http         httpupload

#- Edit Rotate Action
0- Add New Rotate Action
X- Event Log
M- Return to Main Menu
<ENTER> Refresh Menu

----- Rotate Action -----
Format           : xml
Protocol         : http
Delivery Target  : httpupload

1- Protocol
2- Delivery Target
A- Apply Changes
D- Delete
X- Actions On Rotate
M- Return to Main Menu
<ENTER> Refresh Menu
```

4. Telnet/SSH Console

Menu Data

Protocol

This defines the protocol to use when sending the event log file. The valid values are:

- SMTP – email to destination
- HTTP – use HTTP to send to destination

Destination

This field is used to select the destination for the data log file. When the protocol is SMTP, the destination will be an email contact. When the protocol is HTTP, the destination will be an HTTP contact.

If no contacts have been created, or the desired destination has not already been created, the user may create a new destination from this menu. The contacts added here are then also available for use on other menus using the contacts, i.e., the email notification actions.

4.4.3.5 Format Settings

```
----- Format -----  
  
Format=xml  
  
1- csv  
2- log  
3- xml  
X- Rotate Action  
M- Return to Main Menu  
<ENTER> Refresh Menu  
  
>>
```

Menu Data

Format

This defines the format of the log file to be sent on rotation. The valid values are:

- csv – comma separated values
- log – log text file
- xml – xml format file

4.5 About

This menu contains information about PowerAlert. The data on this menu is read-only. The data on this menu is:

```
----- About PowerAlert -----  
  
OS : Ubuntu 16.04.3 LTS Linux 4.4.31 flash: 3.4G ram: 247204kB  
processor: armv7l  
Agent Type : PAL_NMC5  
MAC Address : 00:06:b7:40:04:35  
Card Serial Number : 2626A0AC88E200174  
Driver Version : 15.5.2 (Build 17511)  
Engine Version : 15.5.2 (Build 17511)  
Driver File Status : Normal  
EnergyWise API Version : 1.2.0  
  
X/M- Return to Main Menu  
<ENTER> Refresh Menu
```

5. Command Line Interface

The LX Platform device firmware supports features on the command line interface (CLI). Many of the functional controls available in the Web console and Telnet interface are available on the command line interface. The CLI allows for the use of user-created scripts and easier integration with third-party systems.

The CLI can be accessed on the LX Platform device via the USB Micro or RJ45 CONFIG port, via SSH on the default port 22, and via Telnet on the default port 23. For security purposes, some features are only enabled on the USB Micro and SSH interfaces. Refer to section 4.3.2 for more information on starting the CLI from the Telnet or SSH menu.

This section of the user manual will familiarize you with the way the CLI interprets your input and the meaning of the CLI output.

5.1 Syntax Conventions

The PowerAlert CLI uses its own standard syntax to interpret your input. The syntax defines standard conventions which are used to describe any problems with the input. The next definitions are important for understanding the rest of this document and the CLI error messages.

1. Program - The 'program' refers to the software module that will interpret the user input and perform the work.
2. Program Name - The command keyword that is typed to invoke the program.
3. Directive - The entire phrase entered, including the program name and any arguments. The directive is broken down into several parts of grammar, like a sentence.
4. Mode - The mode tells the program what to do with your arguments. A program can usually perform several different operations on the same data. Program modes are: List, Add, Update, Delete, and Test. In some programs, the mode can be inferred without your specification; in other programs, entering the mode will be required.
5. Mode Modifier - If the mode alone can't describe your request, the program will have a mode modifier list. The mode modifier usually specifies 'what' to list and 'where' and 'what' to add, update, or delete.
6. Identifier - The update and delete modes support entering a numeric identifier to choose what data your new input will affect. The list mode often allows an optional identifier to display more information about a single set of data.
7. Option - The option precedes your input parameter and specifies which value you are updating. An option will always begin with a dash followed by a letter or double dash followed by a number or word.
8. Parameter - If an option requires a parameter, the parameter will follow the option or be appended to the option (for example, when choosing SNMPv3: '--v3').

The directive syntax breaks down along the grammatical boundaries shown below.

Directive			
Preamble		Predicate	
Program	Mode	Mode Modifier	Identifier
Subject	Verb	Direct Object	Indirect Object (List)
addrbook	-u	email	4
	--name	santa	--email santa@morthpole.org

All pieces of syntax are separated with single spaces. The interface does not support input containing spaces at this time, and the input cannot include a single quote character.

5. Command Line Interface

5.2 Manual Pages

Each program has its own man page (short for 'manual page') built right into the software. You will not have to remember long lists of directives. The information you need is available any time by typing 'man' followed by the program name.

The program synopsis in each program manual page describes the format of the directive and the valid modes and options for the program. The synopsis uses a familiar format to indicate when you should enter your own data and when you should type exactly what you see. The typical synopsis format interpretation is shown in the next table.

Synopsis Format	Interpretation of the Format
< >	Angle brackets mean the argument is required.
[]	Square brackets mean the argument is optional.
	The vertical bar is used to separate mutually exclusive choices.
...	A list of space-separated parameters can be entered here.
<word>	You must enter a value. The value is chosen by you. The 'word' loosely describes what the value is supposed to mean.
<a b>	You must enter a value. The value is exactly either 'a' or 'b'.
[--word <value>]	The '--word' option is optional, but if used then 'value' is required.
--word <x1...xN>	The '--word' option supports a list of parameters separated by spaces. The values are chosen by you. You do not append a '1' or 'N' to your input. Usually, the values in a list are data identifiers, but they are sometimes preceded by a '+' or '-', indicating your choice to add or remove the identifier within the directive's context.

5.3 Output Conventions

Additions, updates and deletions usually result in simple output messages prefixed with either an error code or a data identifier return code, followed by a colon and a short result string. The prefixes are described in the next table.

Result Prefix	Interpretation of the Result Prefix
X00:	The 'X' indicates that program is responding with an error. If available, the error code will follow the 'X', and the result string will contain an error message.
00:	The program is indicating a success message if no 'X' is preceding the return value. If the number is non-zero, the return value is the data identifier of the last piece of data used. For example, in add mode, the return value will be the data identifier of the new data. To update this data later, provide the same identifier to the update mode.
YN:	The program is requesting a Yes or No confirmation before taking action.
QQ:	The program is requesting additional input that is not a simple Yes or No.
...:	The program has dispatched your request and it should happen in a few moments.

5.4 Getting Started with the PowerAlert CLI

Remember, most of your configuration changes will take effect immediately, so you can try out your configuration before committing to it. However, the changes are not saved permanently until you 'reboot' the device interface. You should reboot when your configuration is complete and prior to testing configurations that simulate a power outage. Refer to **Section 2. Installation and Configuration** for additional information.

When you first log in to the CLI, you can type 'help' to invoke the 'help' program and see a list of all programs. Each program does only a small amount of the work, and programs can be used in succession to accomplish a task. The next paragraphs describe example goals and which programs can be used together to accomplish them.

Note: Most programs are available only after the system has fully booted.

5. Command Line Interface

How Do I ...

See the list of available programs?

1. Use the 'help' program to display all available programs.

See the manual for any program?

1. Use the 'man' program to display the manual for any program. It is invoked by typing 'man <program name>' without the angle brackets and the 'program name' replaced by the name of the program you are interested in.

See my devices?

1. Use the program 'devmgr' to view the list of devices and individual device details.
2. Use the program 'devselect' to choose a device to work with.

See my device status?

1. Use the program 'devstatus' to view the device status (called 'variables').
2. Use the program 'alarm' to view the active alarms.

Set the time?

1. Use either 'hwclock' to change the Real-Time Clock (RTC) or 'ntpcfg' to change the network time settings.
2. Use either 'hwclock' to synchronize the system clock or skip ahead and use 'reboot' to persist the changes and synchronize automatically on the next restart.

Set up email?

1. Use the program 'addrbook' to add your email addresses.
2. Use the program 'emailcfg' to configure outgoing email.
3. [Optional] Use the 'action' program to create an email action. Do this if you want to add only a few of the email addresses or if you want to make the system delay before emailing.
4. [Optional] Use the 'actcfg' program to assign the email action to alarm triggers. By default an email action is already assigned to all alarms, but if you made a new action you will assign it yourself.

Control my power protection device loads?

1. [Optional] Use the program 'loadcfg' to configure ramp and shed settings and create load groups.
2. Use the program 'loadctl' to control loads and load groups, the main load, and execute ramp or shed sequences.

Add a user or SNMP Community?

1. Use the program 'user' to add or modify local user accounts & SNMP communities.
2. Use the program 'passwd' to set the password for any new non-SNMP account, which will cause the account to activate.
3. [Optional] Use the 'snmpcfg' program to modify SNMP protocol access.

Reset PowerAlert to factory default settings?

1. Use the program 'freset' to reset all user data to factory default.
2. Use the 'reboot' program to bring the system down and back up with factory default settings.

Enable or disable SFTP?

1. Use either 'sftpcfg --enable' or 'sftpcfg --disable'n

6. Troubleshooting

If you encounter a problem:

- Check all connections and confirm that they are secure.
- Refer to the following list of problems and implement any recommended solutions.
- If the problem persists after trying the recommended steps, contact Tripp Lite Technical Support.

Problem	Possible Solution
The IP address of the LX Platform device is unknown.	If your network's DHCP server assigned an IP address to the LX Platform device, contact your network administrator to learn the IP address assigned to the card or view it during terminal session at boot-up. You'll need to know the MAC address of the LX Platform device. If your network does not use DHCP, or if you need to assign a static IP address for another reason, follow the instructions for assigning a static IP address via terminal mode configuration. Refer to the printed manual that came with your LX platform device for more information.
Unable to perform SNMP get operations.	Check the SNMP settings of the LX Platform device (See Section 3.4.6). Select "User" in the settings dropdown menu. The IP address and community name of the device or application trying to perform the SNMP get operation must be entered with a "Read Only" or "Read/Write" ("Manager" or "Administrator") role.
Unable to perform SNMP set operations.	Check the SNMP settings of the LX Platform device (See Section 3.4.6). Select "User" in the settings dropdown menu. The IP address and community name of the device or application trying to perform the SNMP set operation must be entered with a "Read Only" or "Read/Write" ("Manager" or "Administrator") role.
Unable to receive traps at your management station.	Check the SNMP settings of the LX Platform device (See Section 3.4.3). Verify that you have added an SNMP trap action profile to send traps to the IP address of the management station of choice. See Section 3.4.4.1.3 for configuring actions.
LX Platform device email notifications are not working.	Verify that you have added an email action profile to send emails to the appropriate destination entered in the address book. See Section 3.4.4.1.1 for configuring actions. Note: Confirm email notification works by sending a test message. See Section 4.2.1.1 for instructions.

7. Technical Support

Before contacting Tripp Lite Technical Support, refer to **Section 6. Troubleshooting** for possible solutions. If you are still unable to resolve the problem, contact Tripp Lite Technical Support at:

www.tripplite.com/support
Email: techsupport@tripplite.com

Tripp Lite has a policy of continuous improvement. Specifications are subject to change without notice.

8. Appendix

Configuring RADIUS Authentication in PowerAlert

PowerAlert supports RADIUS authentication, authorization and accounting. In addition to configuring PowerAlert to use RADIUS, one or more RADIUS servers must be configured to provide the appropriate exchange of information. This document assumes the following:

- The user understands the steps necessary to configure one or more RADIUS hosts in PowerAlert
- The user understands the steps necessary to configure PowerAlert to use RADIUS for authentication and/or accounting, either as a sole option or in relationship to local authentication and/or accounting
- Some flavor of RADIUS server has been installed and configured and is accessible by PowerAlert

For the rest of this document, when we reference a specific RADIUS server type, we will be using FreeRadius (www.freeradius.org) as our default. Your specific configuration may vary.

Configuring the Dictionary

This refers to the definition of the attributes that can be exchanged between a RADIUS server and a RADIUS client, in this case PowerAlert. Sample A of this document shows a sample 'dictionary.tripp-lite' configuration for use with a FreeRadius server.

The first thing that needs to be configured is a Vendor ID for TrippLite; the assigned code is 850. This is necessary so that the vendor-specific attributes that PowerAlert will send to the RADIUS server are understood and accepted. Likewise, it allows the server to respond with vendor-specific information. The configuration requires and defines three string attributes.

TrippLite-Authorization

This string contains the authorization definition for a defined user. It is how PowerAlert determines what facilities within PowerAlert may be accessed or modified by a given user.

TrippLite-Outlet-Realms

This string contains the individual outlet realms for which a user is granted access. This is how PowerAlert has implemented user-controlled outlets.

TrippLite-Message

This is a simple string containing a textual message that will be sent from PowerAlert to the RADIUS server during the accounting process.

Once the dictionary has been configured, the RADIUS server should now understand how to handle information exchange with PowerAlert.

Configuring the Users

Each user requires a unique configuration. For the sample FreeRadius server, those entries go into a single file called "users." A sample of the configuration file is given in Sample B.

Sample Administrative User

This entry in the user table defines a sample administrative user for PowerAlert:

radiusadmin	Cleartext-Password := "radiusadmin" Reply-Message = "Hello, %{User-Name}", TrippLite-Authorization = "default=rw", Session-Timeout = 2400, Idle-Timeout = 1200
--------------------	---

This entry defines a user with the name of 'radiusadmin' and a password of 'radiusadmin'. It is important to note that PowerAlert will only generate authentication requests with a **Cleartext-Password**; no other exchange mechanism is supported at this time.

The **Reply-Message** line simply indicates a textual response sent back if the user authenticates successfully. It is not required by PowerAlert, but is a standard component of a response to an authentication request.

The **TrippLite-Authorization** string is required in all successful authentication responses. Failure to return said string will default the user to no authorization. In this case, as described in the dictionary, this user has default Read-Write access to all of the facilities within PowerAlert.

The **Session-Timeout** and **Idle-Timeout** strings are not defined in the dictionary. They are not vendor-specific attributes, but are instead part of the standard RADIUS configuration defined by RFC 2865.

Session-Timeout "sets the maximum number of seconds of service to be provided to the user before termination of the session or prompt. This Attribute is available to be sent by the server to the client in an Access-Accept or Access-Challenge." In the case of PowerAlert, if this value is not sent, a user's session will never timeout.

Idle-Timeout "sets the maximum number of consecutive seconds of idle connection allowed to the user before termination of the session or prompt. This Attribute is available to be sent by the server to the client in an Access-Accept or Access-Challenge." In the case of PowerAlert, if this value is not sent, a user's session will never expire due to inactivity.

Sample Managerial User

This entry in the user table defines a sample managerial user for PowerAlert:

radiusmanager	Cleartext-Password := "radiusmanager" Reply-Message = "Hello, %{User-Name}", TrippLite-Authorization = "default=rw,security=ro", Session-Timeout = 1200, Idle-Timeout = 600
----------------------	--

For the most part, this is identical to the administrative account above: A user name and password on the first line, a **Reply-Message** on the second line, and a **TrippLite-Authorization** string on the third line. We end the entry with slightly shorter **Session-Timeout** and **Idle-Timeout** entries. The only major difference between the default manager and the default administrator is that the manager is explicitly denied Write access to the security facility, meaning they can view security resources, such as user accounts and authentication schemes, but not change them.

8. Appendix

Sample Guest User

This entry in the user table defines a sample guest user for PowerAlert:

radiusguest	Cleartext-Password := "radiusguest"
	Reply-Message = "Hello, %{User-Name}",
	TrippLite-Authorization = "default=ro,security=none",
	TrippLite-Outlet-Realms = "1-10,31",
	Session-Timeout = 600,
	Idle-Timeout = 300

Once again, the format remains fairly standard in terms of username, password, **Reply-Message** and timeout parameters. The shorter idle and session timeout values reflect the limited scope of access. The two major changes are in the **TrippLite-Authorization** and **TrippLite-Outlet-Realm** definitions. The guest user has read-only access to all facilities by default and explicitly has no access to the security realm. This gives the guest the ability to monitor PowerAlert, but not change any of the configuration.

This is also the only entry with a **TrippLite-Outlet-Realm** definition. In this case, while the guest can monitor the rest of the system, they have been provided the ability to control individual outlets on devices that support them that fall within the realms of 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 and 31. In this manner, an account can be restricted to only be able to change the state of those specific outlets.

Configuring Client Access

Once the dictionary and user configurations are in place, the RADIUS server must be configured to allow PowerAlert to send requests and receive responses. This is very specific to the particular RADIUS server involved, so check your documentation carefully. For the FreeRadius server, entries would be added to the clients.conf file following the instructions provided with the sample entries.

8. Appendix

Sample A

Sample 'dictionary.tripp-lite' FreeRadius Configuration File

```
#####
VENDOR      TrippLite      850
BEGIN-VENDOR TrippLite

#
# Access is granted to the various facilities within the PowerAlert software
# by means of the TrippLite-Authorization attribute, which is a comma-delimited
# string of facility-code to access-level pairs.
#
# Facility Codes: default, security, networksettings, systemsettings, systeminfo,
#                 logging, devicestatus, devicecontrols, deviceevents,
#                 deviceloads, actions, schedules, discovery
#
# Access Levels: none (or 0), ro (or 1), rw (or 2)
#
# Example: default=rw,security=none,systemsettings=ro
#
#           - The default access for all non-specified facilities is read/write
#           - The user has no access to the security facility
#           - The user has read-only access to the system settings
#
ATTRIBUTE    TrippLite-Authorization    1      string

#
# Comma-delimited string of outlet security realms from 1 through 32 to which
# an otherwise restricted user has read-write access.
#
# Example: 1-5,10,15
#
#           - User has read-write access to realms 1, 2, 3, 4 and 5
#           - User has read-write access to realms 10 and 15
#
ATTRIBUTE    TrippLite-Outlet-Realms    2      string

#
# Simple message, usually sent as part of accounting
#
ATTRIBUTE    TrippLite-Message          3      string

END-VENDOR TrippLite
```

8. Appendix

Sample B

Sample 'users' FreeRadius Configuration File Snippet

The following snippet defines simple sample of an administrative, managerial and guest account for PowerAlert.

```
# -----#  
# PowerAlert Entries  
# -----#  
  
radiusadmin      Cleartext-Password := "radiusadmin"  
                  Reply-Message = "Hello, %{User-Name}"  
                  TrippLite-Authorization = "default=rw"  
                  Session-Timeout = 2400  
                  Idle-Timeout = 1200  
  
radiusmanager    Cleartext-Password := "radiusmanager"  
                  Reply-Message = "Hello, %{User-Name}"  
                  TrippLite-Authorization = "default=rw,security=ro"  
                  Session-Timeout = 1200  
                  Idle-Timeout = 600  
  
radiusguest      Cleartext-Password := "radiusguest"  
                  Reply-Message = "Hello, %{User-Name}"  
                  TrippLite-Authorization = "default=ro,security=none"  
                  TrippLite-Outlet-Realms = "1-10,31"  
                  Session-Timeout = 600  
                  Idle-Timeout = 300
```

