R-Series PDU v4
Instruction Manual

Table of Contents

1   Revision History

Date	Version	Revisions
07/28/2016	Rev 1.0	Updates to support v4.4.0 firmware release
12/14/2016	Rev 2.0	Minor text edits
03/01/2017	Rev 3.0	Minor updates to text

2   Specifications

Overview

The R-Series are rack level power distribution units (PDUs) with monitoring via a built-in web server. Web pages, including logging and graphs, are generated by the unit to monitor power and environmental conditions within the cabinet, several data formats are available. R-Series PDUs support optional external sensors and network cameras. These units can be built for installation in single-phase, three-phase Delta or Wye building wiring configurations. There are four families within the R-Series; RCX, RCO, RCM-O and RCU-O

	Input Power Monitoring	Outlet Level Power Monitoring	Outlet Level Switching
RCX	●		
RCO	●	●	
RCM-O	●		●
RCU-O	●	●	●

2.1   Environmental

2.1.1   Temperature

Operating	10°C (50°F) min	45°C (113°F) max
Storage	-25°C (-13°F) min	65°C (149°F) max

2.1.2 Humidity

Operating	5% min	95% max (non-condensing)
Storage	5% min	95% max (non-condensing)

2.1.3 Elevation

Operating	0 m (0 ft) min	2000 m (6561 ft) max
Storage	0 m (0 ft) min	15240 m (50000 ft) max

2.2 Electrical

See nameplate for unit ratings.

2.3 Receptacle Ratings

Type	Ratings
NEMA 5-15R or L5-15R	125Vac, 15A
NEMA 5-20R or L5-20R	125Vac, 20A
NEMA 6-20R or L6-20R	250Vac, 20A
NEMA L5-30R	125Vac, 30A
NEMA L6-30R	250Vac, 30A
IEC-60320 C13	250Vac, 10A (UL & CSA 15A, 250Vac)
IEC-60320 C19	250Vac, 16A (UL & CSA 20A, 250Vac)

2.4 Networking

2.4.1 Ethernet Link Speed

10/100 Mbit; full-duplex

2.4.2 Protocols

ARP	IPv4	IPv6	ICMP	ICMPv6	NDP	TCP
UDP	DNS	HTTP	HTTPS	SMTP	SMTPS	DHCP
SNMP (v1/v2c/v3)	LDAP	NTP	SSH	Telnet	Syslog	

2.4.3 User Interfaces

- JSON-based web GUI
- Command-line interface using SSH/Telnet
- SNMP

2.5 EMC Verification

This Class A device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1) This device may not cause harmful interference.

2) This device must accept any interference received, including interference that may cause undesired operation.

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Warning: Changes or modifications to this unit not expressly approved by the party

responsible for compliance could void the user's authority to operate this equipment.

3   Installation

3.1   Guidelines

- The ambient temperature of the rack should be no greater than 45°C.

- Install the PDU such that the amount of airflow required for safe operation of equipment is not compromised.

- Mount the PDU so that a hazardous condition is not achieved due to uneven mechanical loading.

- Follow nameplate ratings when connecting equipment to the branch circuit. Take into consideration the effect that overloading of the circuits might have on overcurrent protection and supplied wiring.

- The PDU relies on the building installation for protection from overcurrent. A certified overcurrent protection device is required in the building installation. The overcurrent protection device should be sized according to the PDU's nameplate ratings and local/national electrical code.

- Reliable earth grounding of rack-mount equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit. The PDU must be connected to an earthed outlet.

- PDU is intended for restricted-access locations. Only qualified service personnel should install and access the PDU.

- For pluggable equipment, install the PDU so the input plug or appliance coupler may be disconnected for service.

- The PDU is intended for indoor use only. Do not install the unit in wet or outdoor environments, and do not install it next to water tanks or plumbing.

- The PDU is intended for use with TN, TT, or IT power supply systems.

3.2   Mounting

Optional brackets sold separately.

1. Using appropriate hardware, mount unit to rack. (See below examples.)
2. Plug PDU into an appropriately-rated and protected branch-circuit receptacle.
3. Plug in the devices to be powered by the PDU.
4. Turn on each device connected to the PDU. Sequential power-up is recommended to avoid high inrush currents.

3.2.1   Full Length Brackets
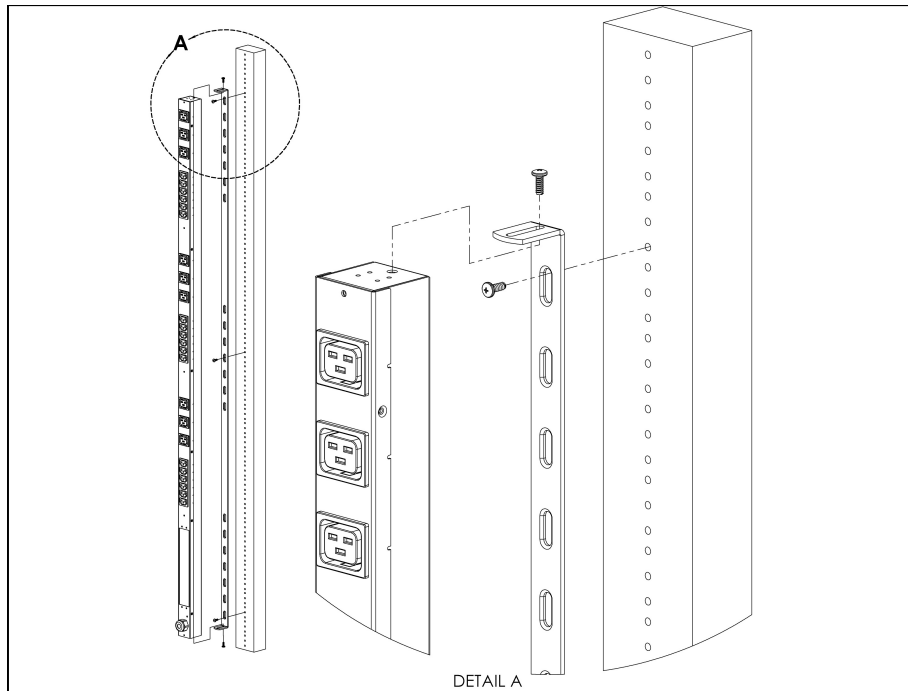
Full Length Bracket

3.2.2 Mini "L" Brackets (SLB-4)

DETAIL A

DETAIL B
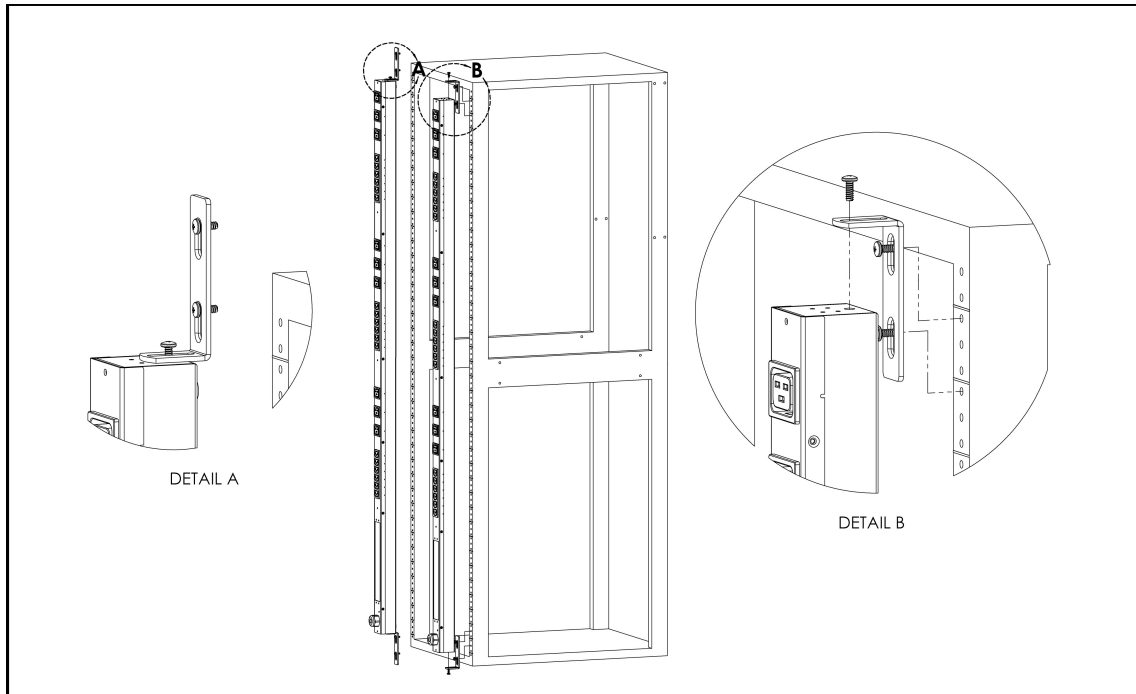
Mini "L" Brackets (SLB-4)

3.2.3 Vertical Extension Brackets (VCB-1)

DETAIL A

DETAIL B
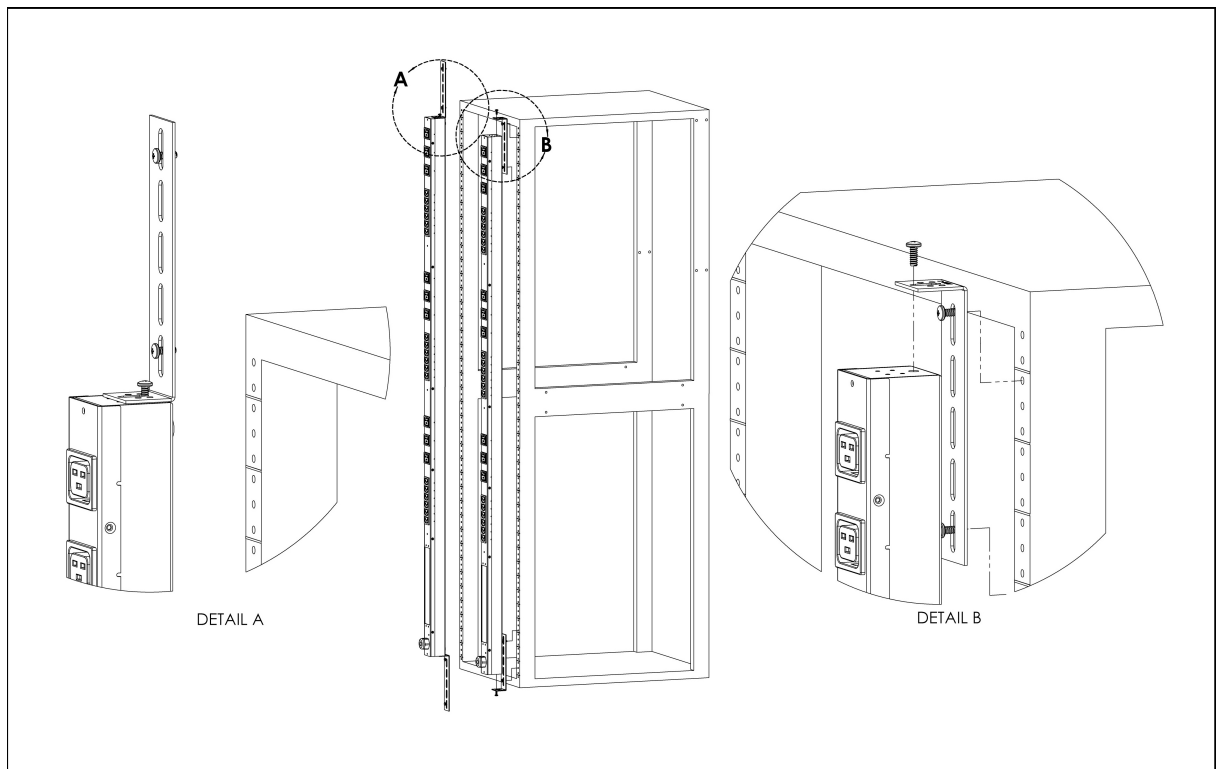
Vertical Extension Brackets (VCB-1)

3.2.4   Toolless Mounting Hardware (11621)
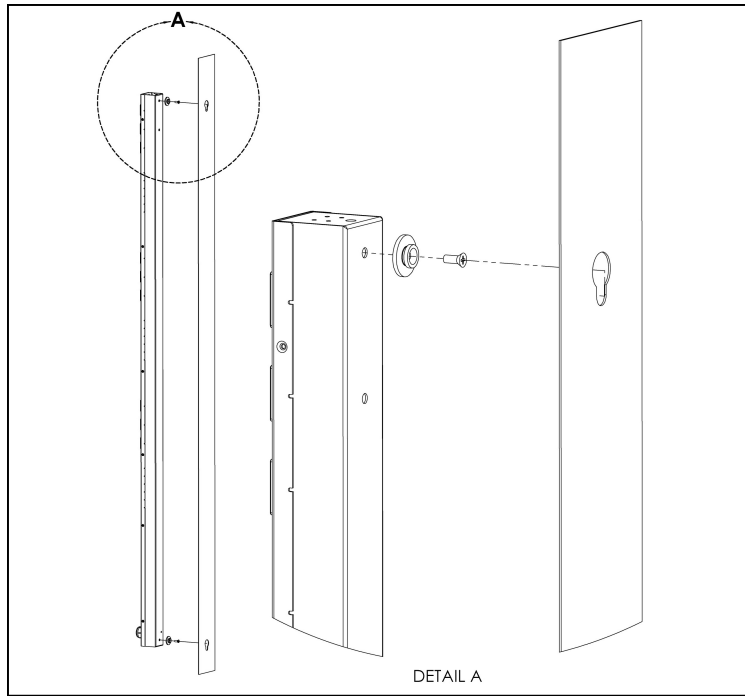
Toolless Mounting Hardware

3.2.5   Toolless Full Length Brackets (TLFL)
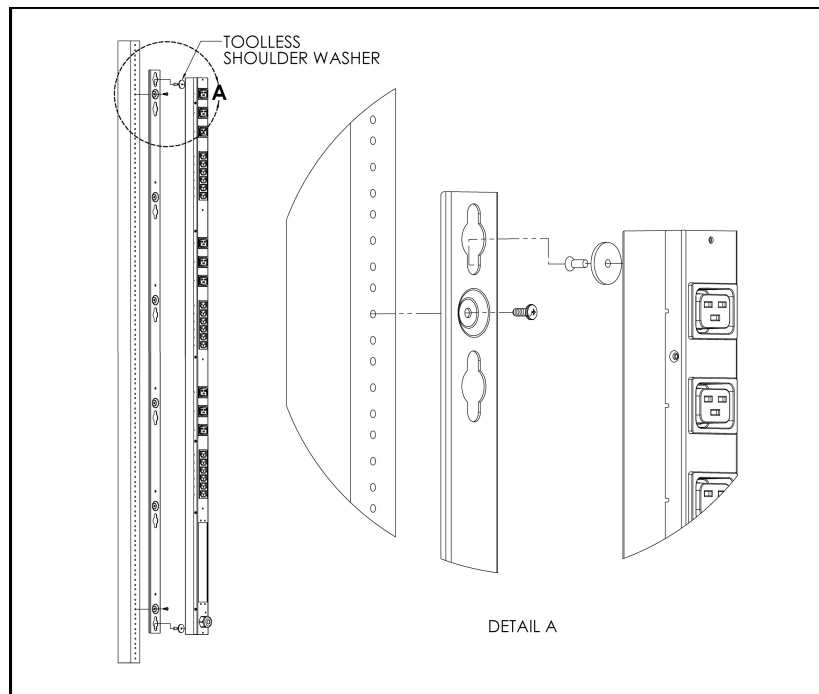
Toolless Full Length Brackets (TLFL)

3.2.6   Single Side Mount 2 Unit Brackets (TSMX2)
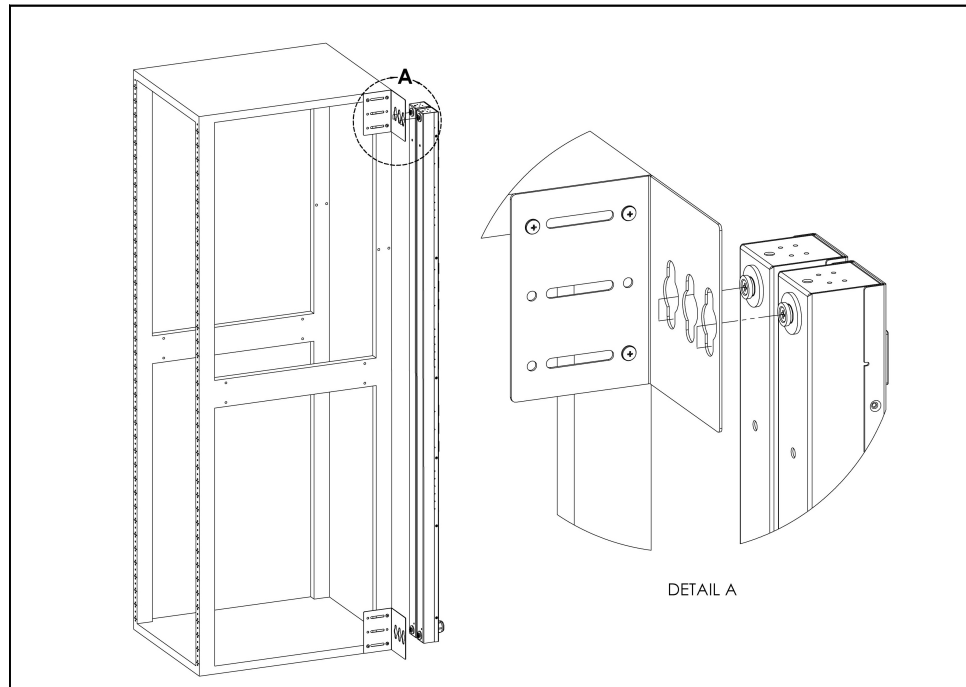
Single Side Mount 2 Unit Brackets (TSMX2)

3.2.7   Offset/Side Mount Brackets (EZB-1)
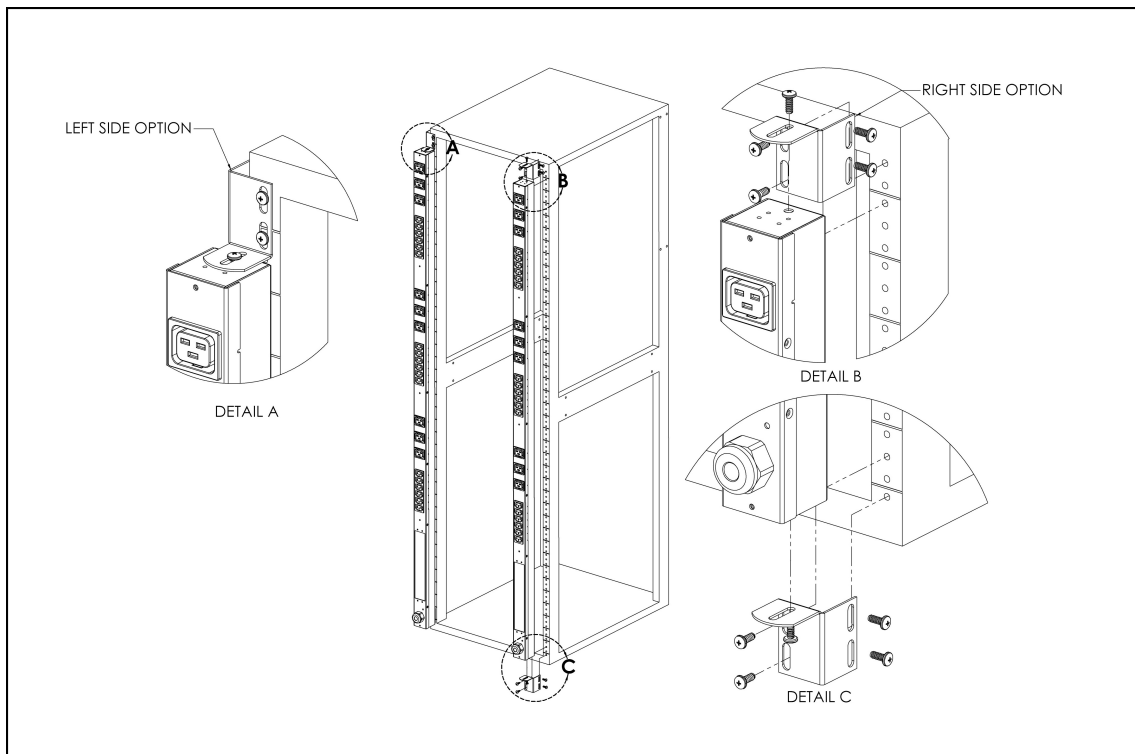
Offset/Side Mount Brackets

3.2.8 7" Extension Brackets (XB-7)
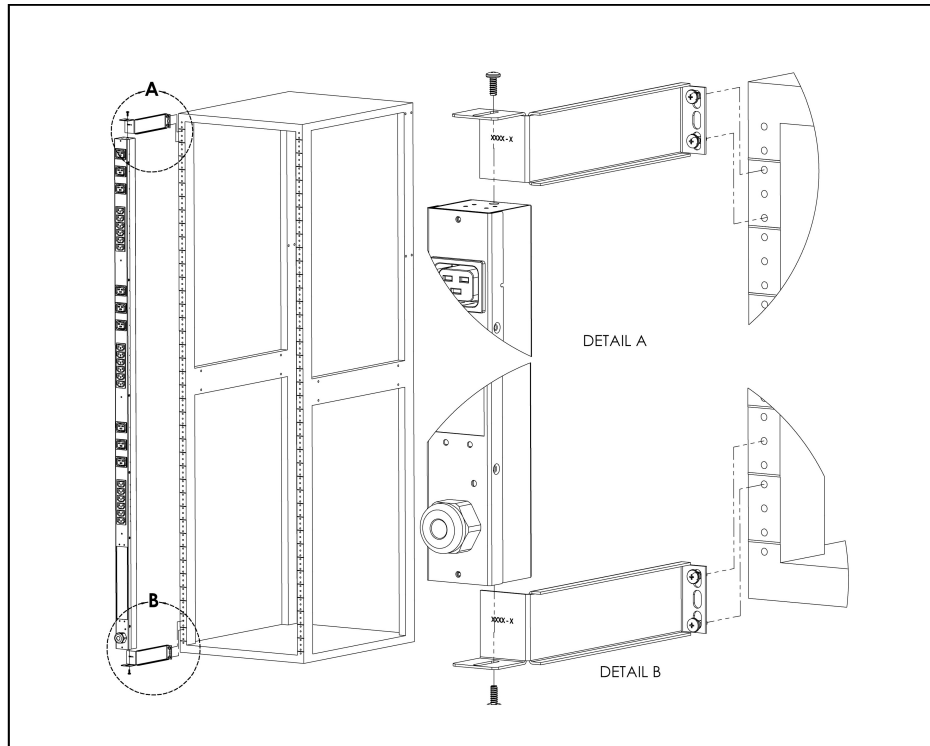
7" Extension Brackets

3.2.9 Flush Mount Brackets (FM)
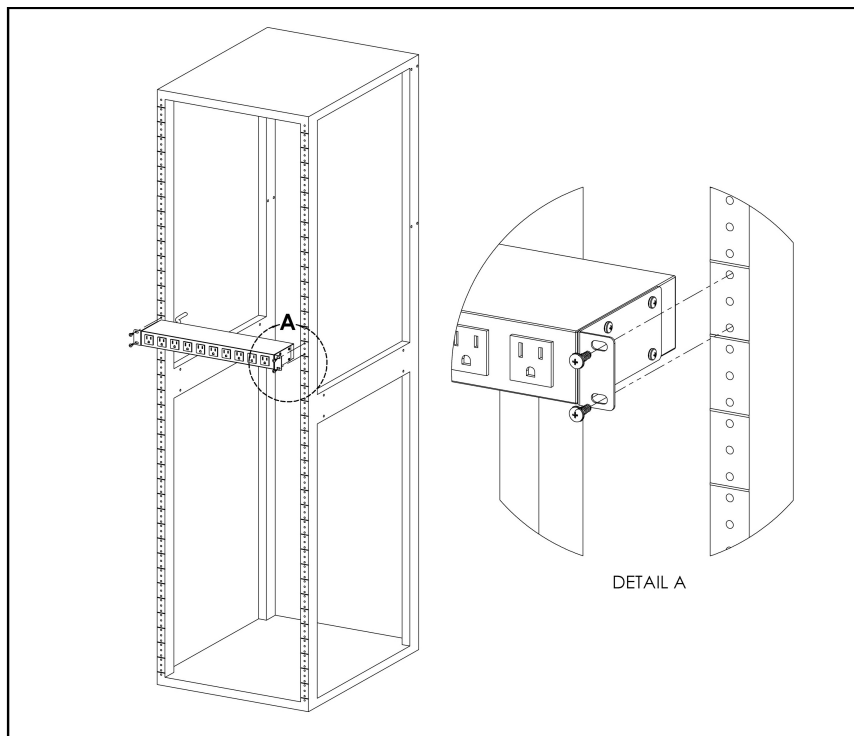
Flush Mount Brackets (FM)

3.2.10 Adjustable Mount Brackets (AM)

DETAIL A
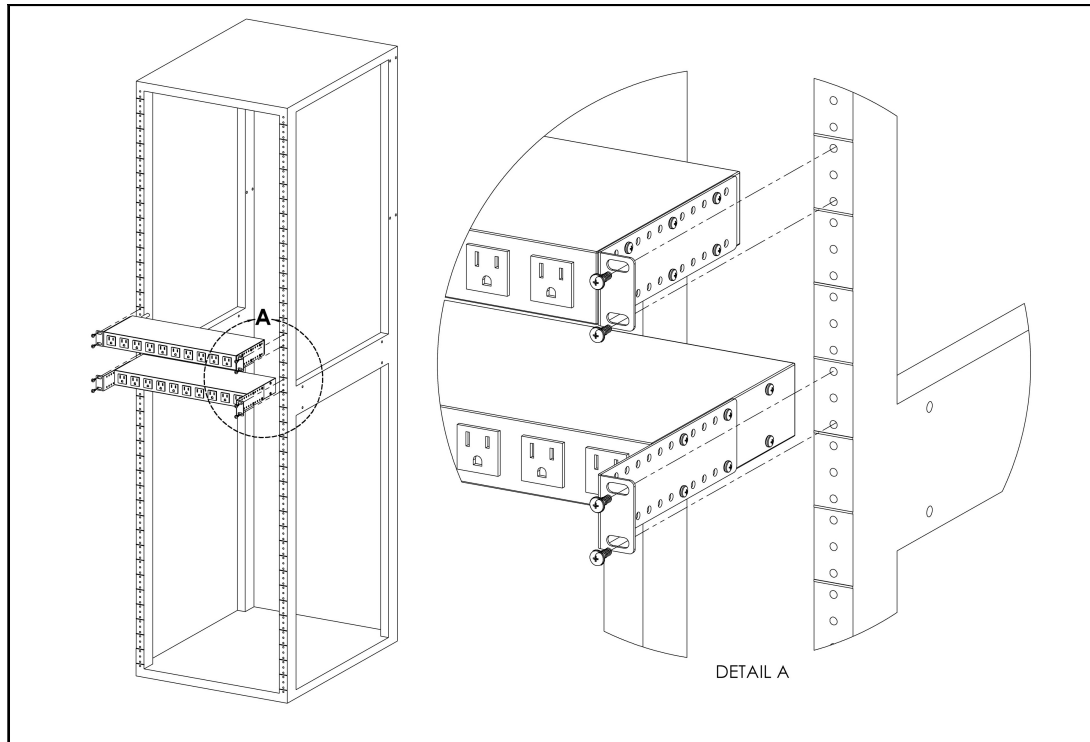
Adjustable Mount Brackets

3.2.11 Panel Mount Brackets (PM)

DETAIL A
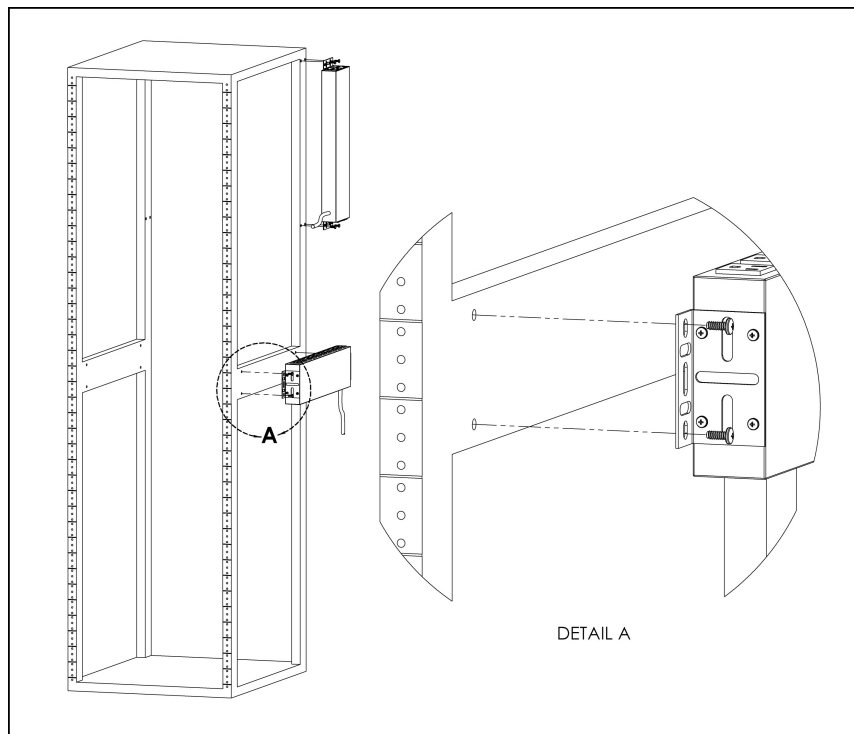
Panel Mount Brackets

3.2.12 23" Conversion Mounting Brackets (23-RM)

23" Conversion Mounting Brackets (23-RM)

DETAIL A
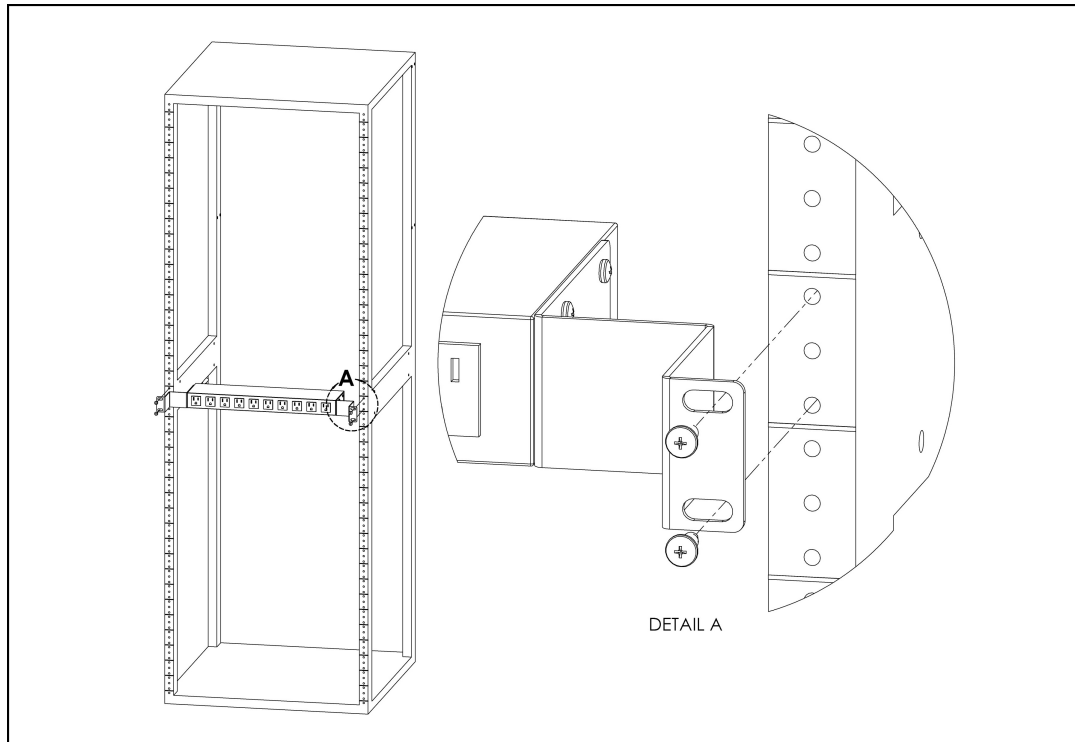
3.2.13 Cable Mount Brackets (CMB-1)

DETAIL A

DETAIL B
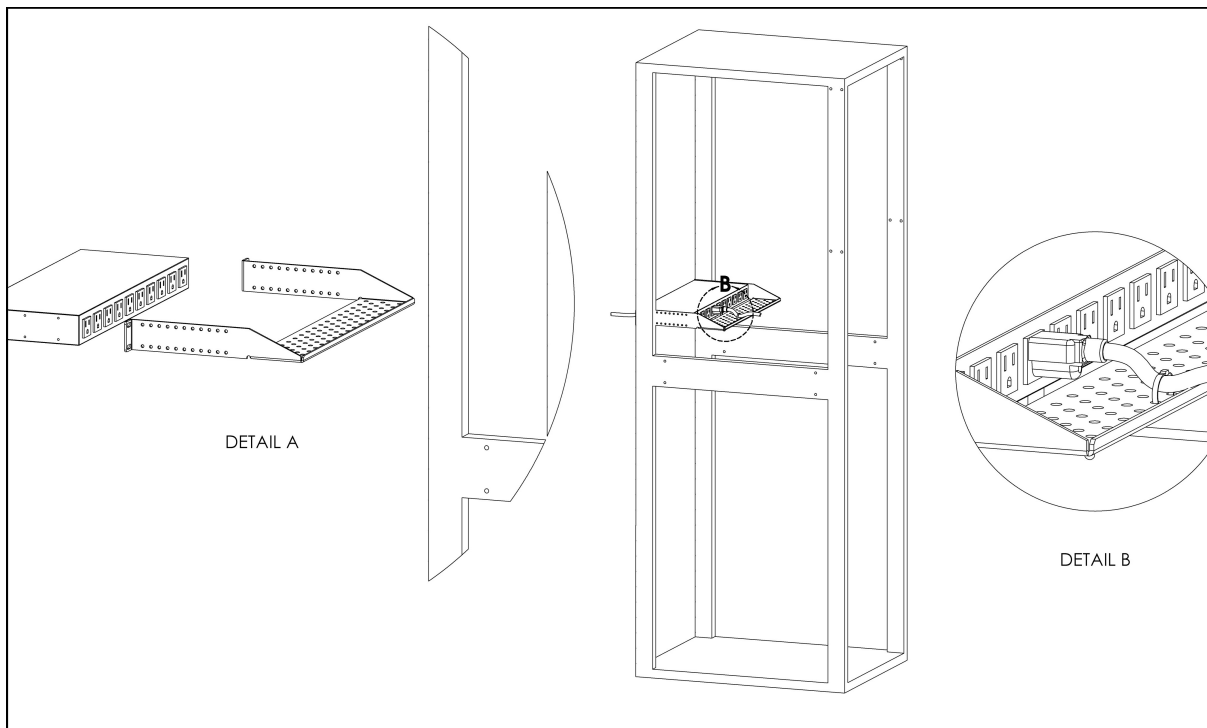
Cable Mount Brackets (CMB-1)

3.2.14 19" Horizontal/Panel Mount Brackets (7938)

DETAIL A
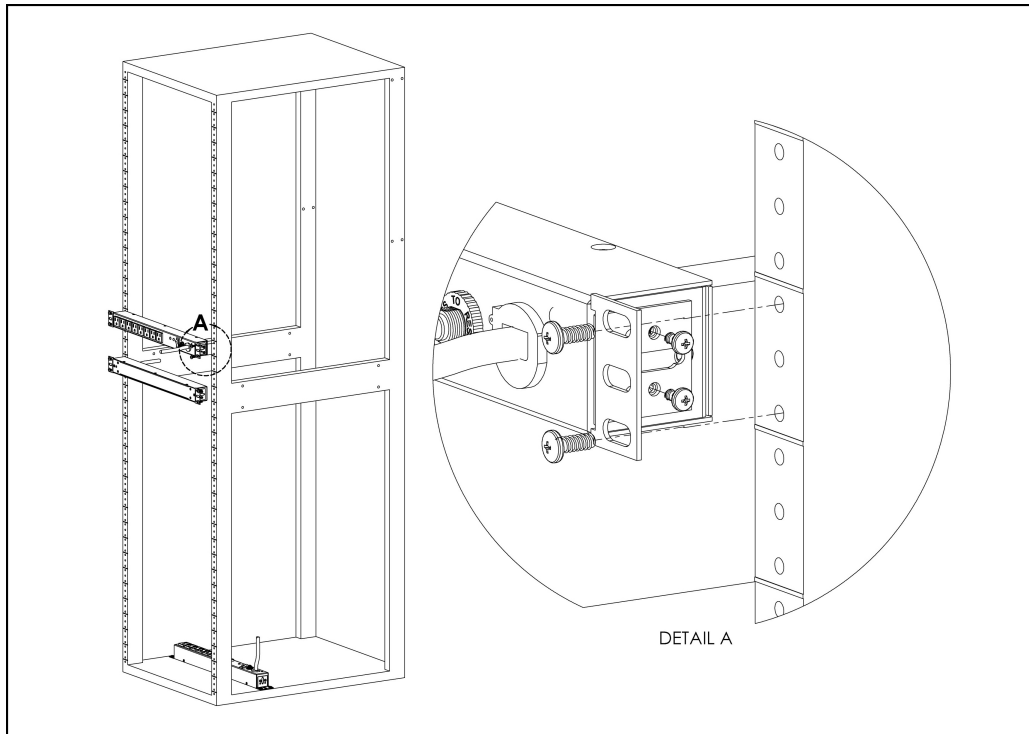
19" Horizontal/Panel Mount Brackets (7938)

4   Hardware

4.1   Interface

The R-Series PDUs have an advanced feature set for data centers that need full remote monitoring, logging and alarms with options for outlet level monitoring and switching control. The PDU supports multiple I/O options.
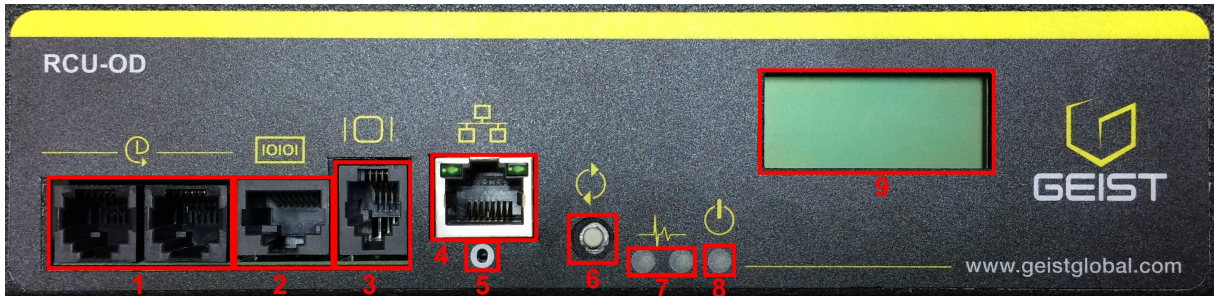
1. **Remote Sensor Port ( ):** Two RJ12 ports for connecting Geist plug-and-play remote sensors (sold separately). Splitters may be used to add additional sensors. Each sensor has a unique serial number and is automatically discovered. R-Series PDUs support up to sixteen sensors.

2. **Serial Communication Port ( ):** The R-Series PDUs provide an out-of-band, serial monitoring interface. The unit provides a RJ-45 port for RS-232 serial communication, providing support for Telnet and SSH via command line.

3. **Remote Display Port ( ):** An optional remote display (RSD2X8) can be connected to the R-Series PDU.

4. **Ethernet Port ( ):** RJ45 port for connecting the PDU to a TCP/IP network.

5. **Network-Reset Button ( ):** Holding the network-reset button for 5 seconds during normal operation will restore the default IP address and reset the user accounts.

6. **Hard-Reboot Button ( ):** Press & release of the hard-reboot button reboots the monitoring device. This acts as a power-cycle for the monitoring device, and does not change or remove any user information. *Note: This will NOT affect power to the outlets*. Note: On 1U horizontal Switched Outlet Level Monitoring (RCU) units, holding the reboot button down for ~45 seconds will cycle the relays on the PDU causing a temporary loss of power to the connected equipment.

7. **Activity/Idle LEDs ( )**

8. **Power Status LED ( )**

9. **Local LCD Display**: The local display scrolls through the values of the measurements selected on the LCD Display page.

For R-Series Switched PDUs, there is an LED next to each outlet providing feedback for the current state.

- Green: Outlet is on.
- Orange: Outlet is being switched or in an error state. Check the web page or contact technical support for more information.
- Red: Outlet is off.

4.2   Network Setup

Geist R-Series PDUs have a default IP address for initial setup and access. Once an IP address is assigned the default IP address will no longer be active. To restore the default IP address and reset all user-account information press and hold the network-reset button located below the Ethernet port for 5 seconds while the unit is powered on (See Section 3.1.5). This feature can also be used if the user-assigned IP address or account credentials are lost or forgotten.

The Network page (located under the System Tab) allows you to assign the network properties manually or use DHCP to connect to your network.

Default address:

IP Address:	192.168.123.123
Subnet Mask:	255.255.255.0
Gateway:	192.168.123.1

To access the unit for the first time, you will need to temporarily change your computer's network settings to match the 192.168.123.xxx subnet. To set up the unit, connect it to your computer's Ethernet port, then follow the appropriate instructions for your computer's operating system in the following section(s).

4.2.1   Windows

- **Windows 2000 / XP / Server 2003:**

Click the **Start** button, choose **Settings**, then **Network Connections.**

- **Windows 7 / Server 2008:**

Click the **Start** button, then choose **Control Panel** >> **Adjust Your Computer's Settings** >> **View Network Status and Tasks** >> **Change Adapter Settings**.

(Alternatively, on some Windows 7 machines, this may be **Start**, then **Settings** >> **Control Panel** >> **Network and Sharing Center** >> **Change Adapter Settings**.)

- **Windows 8 / Server 2012:**

Move the mouse cursor to the bottom or top right corner of the screen, click the **Settings** icon, then select **Control Panel**. Change the view type from **Category** to **Large** or **Small Icons** if necessary, then select **Network and Sharing Center**, then

Change Adapter Settings.

Locate the entry under ***LAN or High-Speed Internet*** which corresponds to the network card (NIC) which the unit is connected to. (Note: Most computers will only have a single Ethernet NIC installed, but a WiFi or 3G adapter could also show as a NIC in this list.)

Double-click on the network adapter's entry in the ***Network Connections*** list to open its status dialog box, then click the ***Properties*** button to open the ***Local Properties*** window.
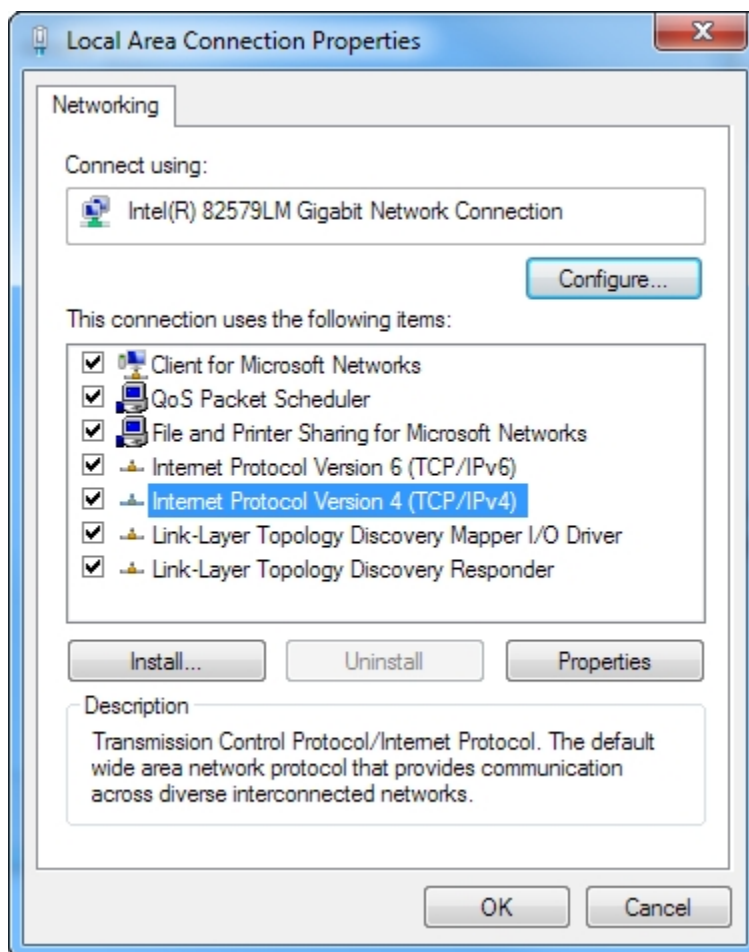
Find the entry titled "***Internet Protocol Version 4 (TCP/IPv4)***" in the list, then click the ***Properties*** button to open the ***Internet Protocol Properties*** window. If you see more than one TCP/IP entry, as in the example above, the computer may be configured for IPv6 support as well as IPv4; make sure to select the entry for the IPv4 protocol.
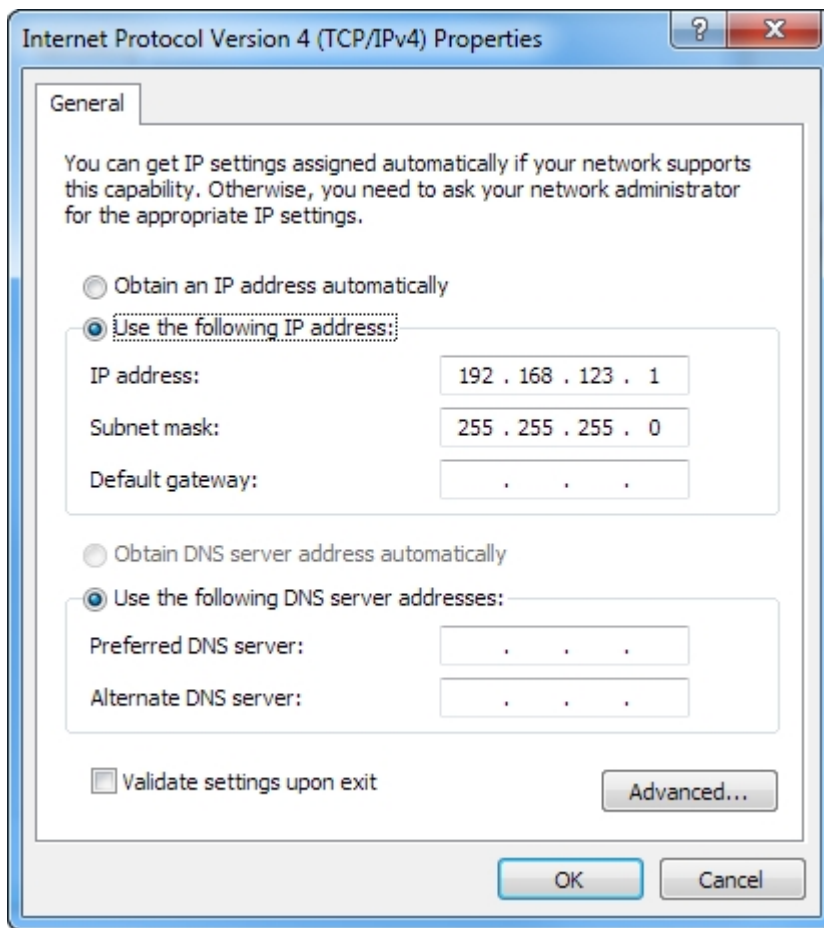
Choose the **Use the following IP address** option, then set **IP address** to 192.168.123.1 and **Subnet Mask** to 255.255.255.0. For this initial setup, **Default Gateway** and the **DNS Server** entries can be left blank. Select **OK**, then **OK** again to close both the **Internet Protocol Properties** and **Local Properties** windows.

Once the NIC settings are configured properly, you should be able to access the unit by typing "http://192.168.123.123" into the address bar of your web browser. If you are setting up the unit for the first time, or if the unit has been reset back to factory defaults via the network-reset button, the unit will require you to create an Admin account and password before you can proceed.

Once you have created the Admin account and logged into it, the unit's default **Sensors** page should come up by default. Navigate to the **System** tab, then the **Network** page to configure the device's network properties. The unit's IP Address, Subnet Mask, Gateway, and DNS settings can either be assigned manually, or acquired via DHCP.

Note: Changes to settings will take effect instantly when the **Save** button is clicked,

*so the browser will no longer be able to reload the web page from the default/
previous address. Once you have finished configuring the unit's IP address, simply
repeat the steps above, and change the computer's Ethernet NIC card settings back
to the ones you wrote down prior to changing them, to restore its normal network and
internet settings.*

4.2.2 Mac

Click the **System Preferences** icon on the Dock, and choose **Network**.
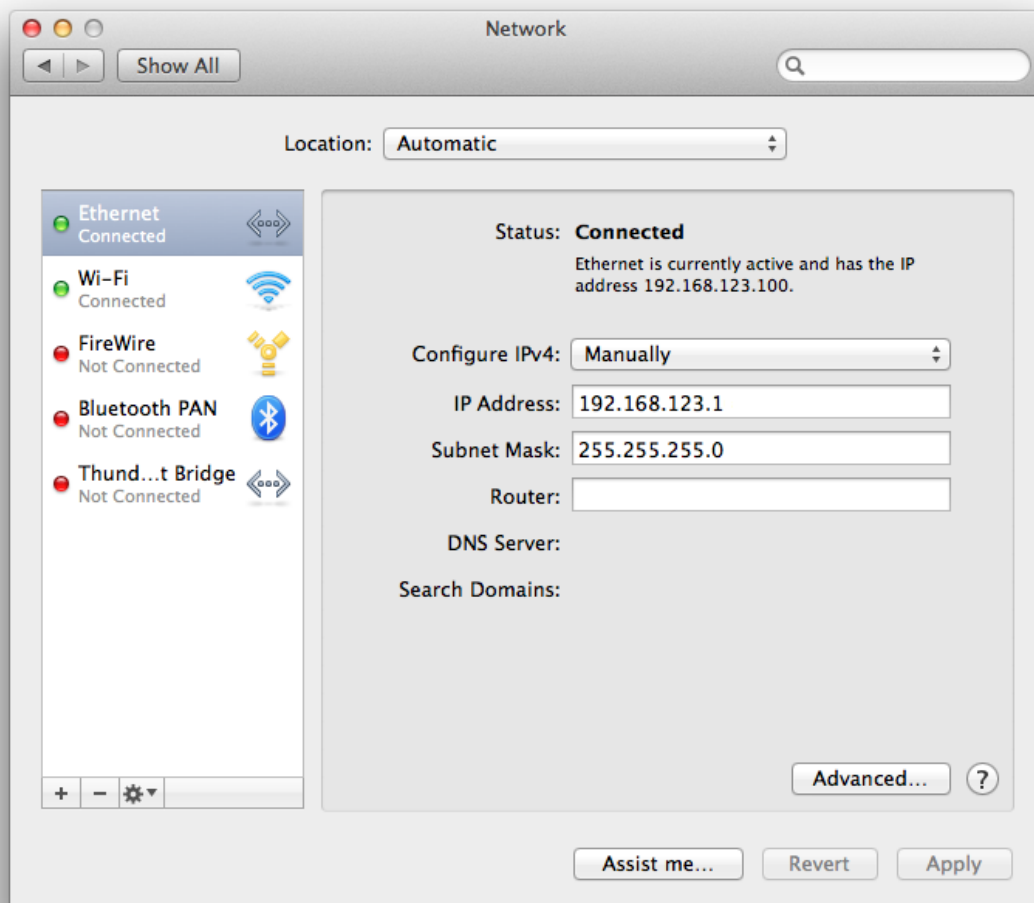
Be sure **Ethernet** is highlighted on the left side of the NIC window. (In most cases,
there will only be one Ethernet entry on a Mac.)

Select **Manually** from the **Configure IPv4** drop-down list, then set **IP Address** to
192.168.123.1 and **Subnet Mask** to 255.255.255.0. (The **Router** and **DNS Server**
settings can be left blank for this initial setup.) Click **Apply** when finished.

Once the NIC settings are configured properly, you should be able to access the unit by typing "http://192.168.123.123" into the address bar of your web browser. If you are setting up the unit for the first time, or if the unit has been reset back to factory defaults via the network-reset button, the unit will require you to create an Admin account and password before you can proceed.

Once you have created the Admin account and logged into it, the unit's default **Sensors** page should come up by default. Navigate to the **System** tab, then the **Network** page to configure the device's network properties. The unit's IP Address, Subnet Mask, Gateway, and DNS settings can either be assigned manually, or acquired via DHCP.

Note: Changes to settings will take effect instantly when the **Save** button is clicked, so the browser will no longer be able to reload the web page from the default/ previous address. Once you have finished configuring the unit's IP address, simply repeat the steps above, and change the computer's Ethernet NIC card settings back to the ones you wrote down prior to changing them, to restore its normal network and internet settings.

5   Web Interface

The Geist R-Series PDUs come with an embedded web interface. The unit is accessible via a standard, unencrypted HTTP connection, or via an encrypted HTTPS (SSL) connection.

Note: An administrator account (username and password) must be created when logging onto the device for the first time.

5.1   Sensors

5.1.1   Overview

The Sensors Overview page displays the PDU's data. R-Series PDUs measure power, voltage, current and energy. Readings on the Overview page are provided in real-time for all of the unit's measurements.

1. Geist Logo

- Clicking on this logo from any page will reload the Sensor Overview page.

2. Sensors, System, and Help Tabs

- Mouse over to show sub-menus:

Sensors	System		Help
Overview	Users	LCD Display	Admin	Info
Alarms & Warnings	Network	Time	Locale	Support Site
Cameras	Web Server	Email	Utilities	
Logging	Reports	SNMP		
	LDAP	Syslog		

3. Log In / Log Out

- Click to log in or log out of the unit. Note that both user-name and password are case sensitive; prohibited characters are: $&`:<>[ ] { }"+%@/ ; =?\^|~',

4. Alarms and Warnings

- Indicates the number of Alarms and Warnings currently occurring, if any.

5. Device Label

- Displays the user-assigned label of this unit (see "Configuration and Operation")

6. Device ID

- Unique product identification. May be required for technical support.

7. Total and Individual Phase or Line Monitor

- Displays AC current, voltage, and power statistics for each individual phase,

and for the total of all phases combined.

8. Current Monitor

- Displays AC current draw statistics for each individual circuit on the PDU.

Note: Groupings for Total, Line, Phase and Current Monitor will vary depending on the PDU's configuration and wiring.

5.1.1.1 Configuration and Operation

Configuration Icon   Operation Icon

Note: Only users with control-level authorizations have access to these settings.

Device, Phase and Circuit Configuration:

1. Click the desired Configuration icon to change the device's *Label*. (*Name* is the PDU's factory name or model, and cannot be changed.)

2. Once done, click *Save*.
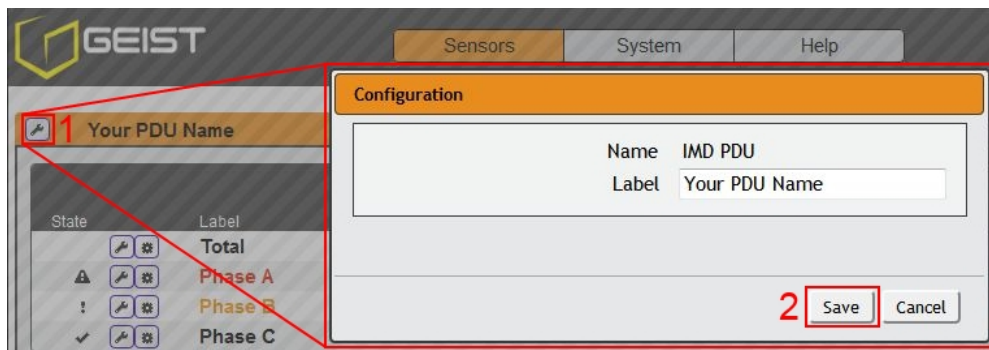
Outlet Configuration:

1. Click the desired Outlet Configuration icon.
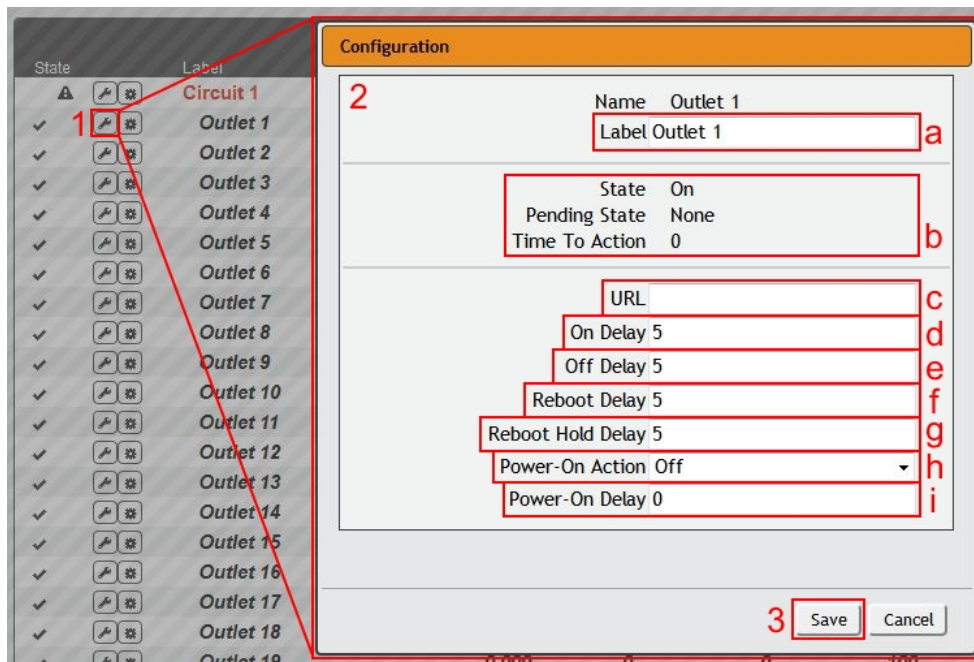
2. Configuration pop-up box will appear.

   a. Use the text box to change the outlet's *Label*.

   b. The outlet's state is described by three descriptors:

- *State* describes the outlet's current state (On/Off).

- *Pending State* describes the state the outlet is currently transitioning to, if it is in the process of switching.

- *Time To Action* describes the time left before the pending action will take place. This is adjusted using *Delays*.

   c. Enter a *URL* to convert the Outlet Name to a hyperlink. This is intended to provide a link to the device powered by this outlet.

   d. *On Delay* is the time, in seconds, the unit waits before switching an outlet on.

   e. *Off Delay* is the time, in seconds, the unit waits before switching an outlet off.

   f. *Reboot Delay* is the time, in seconds, the unit waits before rebooting an outlet.

   g. *Reboot Hold Delay* is the time, in seconds, the unit waits after switching the outlet off, but before switching an outlet on during a reboot.

   h. *Power-On Action* describes the state the outlet will start at power-on (On, Off or Last).

   i. *Power-On Delay* is the time, in seconds, the unit waits after power-on before performing the power-on action for the outlet.

3. Click the *Save* button if any settings are changed.

Device Operation:

1. Click the Operation icon.

2. Select the operation you wish to perform:

   - *On/Off* turns on/off all outlets.

   - For outlets currently on, *Reboot* cycles the outlets off, then back on *after the reboot hold delay*. For outlets currently off, *Reboot* turns the outlets on.

   - *Cancel* will cancel the current operation if it has not been completed yet.

   - *Reset kW Hours* will reset the total Energy measured in kWh.

     Caution: These actions affect the entire device.

3. For operations involving the state of the outlets, setting *Delay* to True will use the current *Delay* configuration for each outlet when performing the selected operation.

4. Select *Submit* to issue the action.
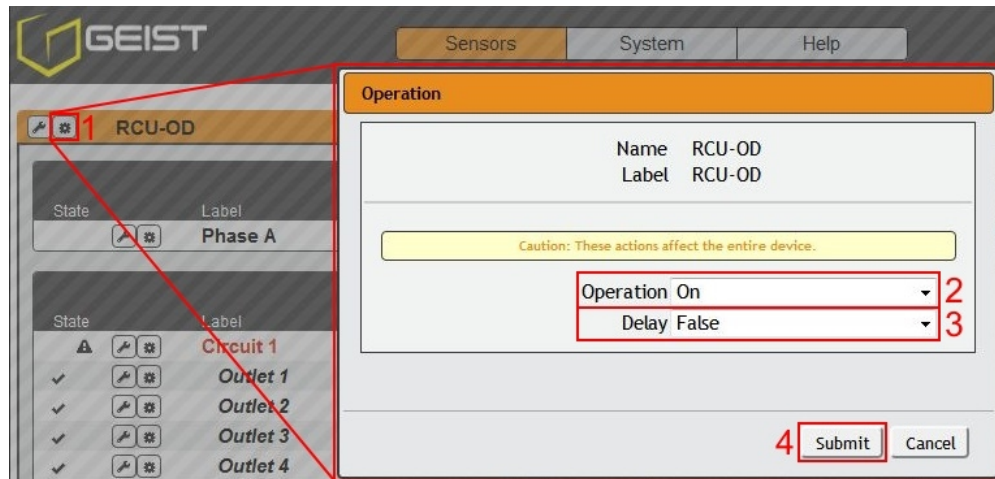
Note: Power-on action delays reference the time since the unit was plugged in, not the time since it fully booted. They will likely execute before the unit fully boots.

Phase/Circuit Operation:

1. Click the Operation icon. For Phase/Circuit operation only the Reset kW Hours (energy) operation is available.

2. Click the *Submit* button to reset the energy of the Phase/Circuit.
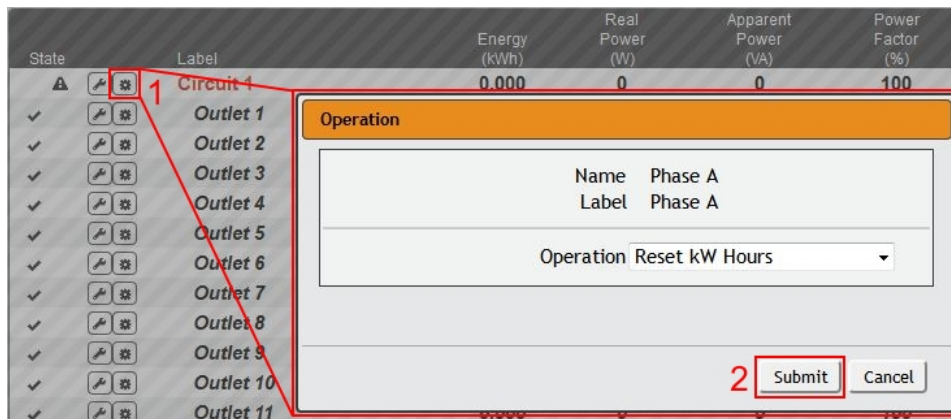
Outlet Operation:

1. Click the desired Outlet Operation icon.
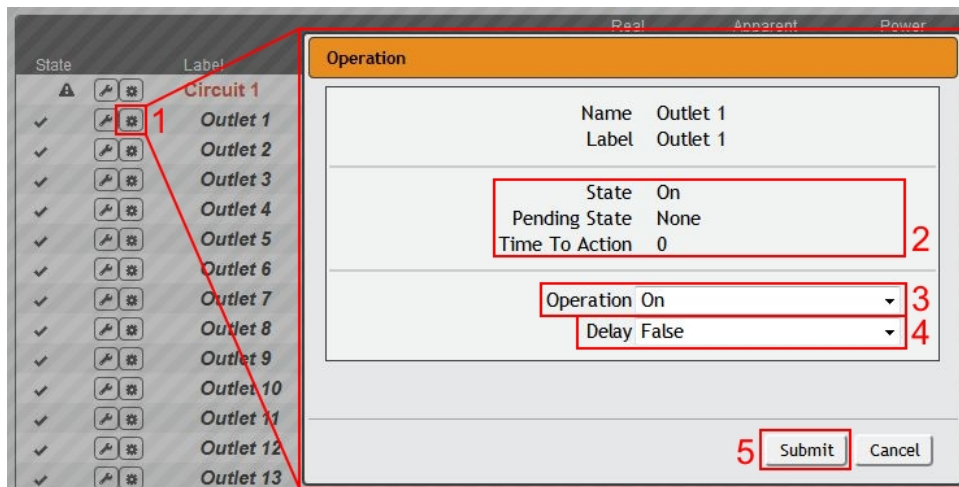
2. The outlet's state is described by three descriptors:

   • *State* describes the outlet's current state (On/Off).

   • *Pending State* describes the state the outlet is currently transitioning to, if it is in the process of switching.

   • *Time To Action* describes the time left before the pending action will take place. This is adjusted using *Delays*.

3. Select the operation you wish to perform:

   • *On/Off* turns on/off the selected outlet.

   • For an outlet currently on, *Reboot* cycles the outlet off, then back *on after the reboot hold delay*. For an outlet currently off, *Reboot* turns the outlet on.

   • *Cancel* will cancel the current operation if it has not been completed yet.

   • *Reset kW Hours* will reset the total Energy measured in kWh for the selected

outlet.

4. For operations involving the state of the outlet, setting **Delay** to True will use the current **Delay** configuration for each outlet when performing the selected operation. Delays are configured in "Outlet Configuration".

5. Select **Submit** to issue the action.

5.1.2 Alarms & Warnings

The Alarms & Warnings page allows users to establish alarm or warning conditions (hereafter referred to as "Events") for each power and circuit readings. Events are triggered when a measurement exceeds a user-defined threshold, either going above the threshold ("high-trip") or below it ("low-trip"). Events are displayed in different sections, based on the device or measurement the Event is associated with. Each Event can have one or more Actions to be taken when the Event occurs.

1. **State**: Shows the status of each Event.

   • Empty: No alert condition.

   • ! : This symbol indicates that this particular "Warning" Event has been tripped. A tripped Warning Event displays in orange.

   • ▲ : This symbol indicates that this particular "Alarm" Event has been tripped. A tripped Alarm Event displays in red.

   • ✓ : This symbol will indicate that this Event has been acknowledged by user after being tripped. It will remain this way until the condition being measured by this Event returns to normal (i.e. ceases to exceed the trigger threshold for this Event.)

2. **Configuration**: Add/Delete/Modify Alarms & Warnings.

   • ⊕ : Add new Alarms & Warnings.

   • 🔧 : Modify existing Alarms & Warnings.

   • ⊖ : Delete Existing Alarms & Warnings.

3. **Notification**: Notify user of tripped Events, and request acknowledgment.

   • Empty: No alert condition.

   • ✓ : Acknowledge button. When a Warning or Alarm Event has occurred; the

user can click on this symbol to acknowledge the Event and stop the unit from sending any more notifications about it. (***Note****: Clicking this symbol does not clear the Warning or Alarm Event, it just stops the notifications from repeating.*)

4. The actual conditions for the various Alarms & Warnings settings are shown here.

5.1.2.1 Alarms & Warnings Configuration

To add a new Alarm or Warning Event:

1. Click the Add/Modify Alarms & Warnings button:
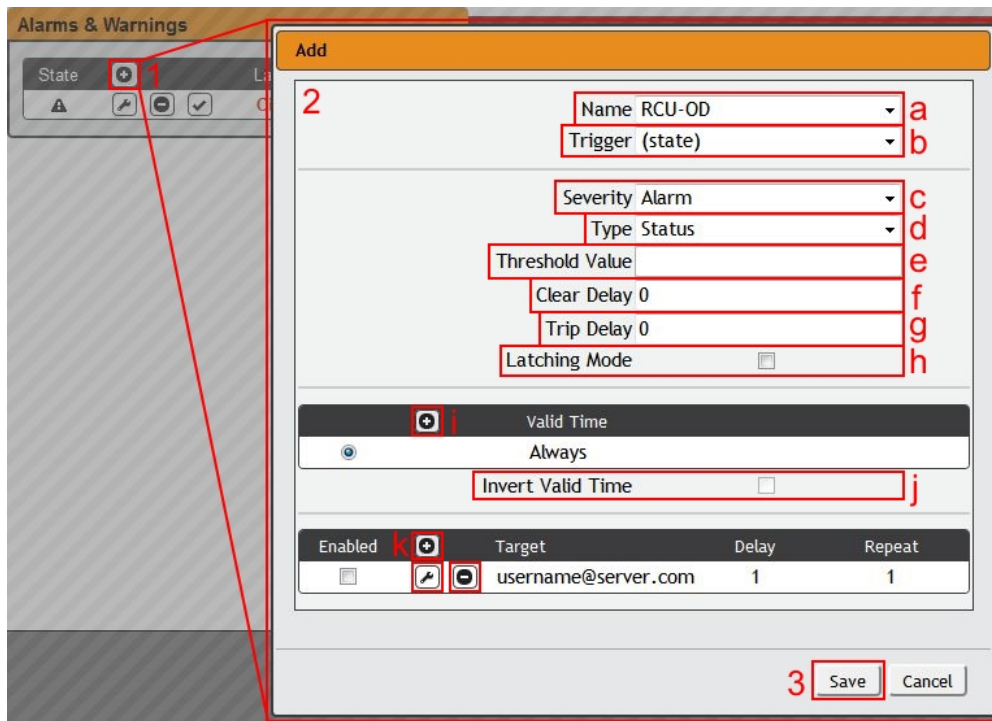
2. Set the desired conditions for this Event as follows:
   a. Select the ***Name*** of the phase or circuit you wish to set an Event on.
   b. Select the measurement (current, voltage, etc.) you want to ***Trigger*** the Event.
   c. Set the ***Severity*** level ("Warning", or "Alarm") for this Event.
   d. Select the threshold ***Type***, "high" (trips if the measurement goes above the threshold) or "low" (trips if the measurement goes below the threshold).
   e. Type in the desired ***Threshold Value*** (any number between -999.0 ~ 999.0 is valid).
   f. Type in the desired ***Clear Delay*** time in seconds. Any value other than "0" means that once this Event is tripped, the measurement must return to normal for this many seconds before the Event will clear and reset. *Clear Delay* can be up to 14400 seconds (4 hours).
   g. Type in the desired ***Trip Delay*** time in seconds. Any value other than "0"

means that the measurement must exceed the threshold for this many seconds before the Event will be tripped. *Trip Delay* can be up to 14400 seconds (4 hours).

h. *Latching Mode*: If enabled, this Event and its associated Actions (see below) remain active until the Event is acknowledged, even if the measurement subsequently returns to normal.

i. *Valid Time* decides when an Alarm notification can be sent. *Valid Time* is set by clicking the Add/Modify icon and setting the days and time ranges notifications will be sent. Then clicking **Save**.

Note: Only one valid time can be selected per alarm.
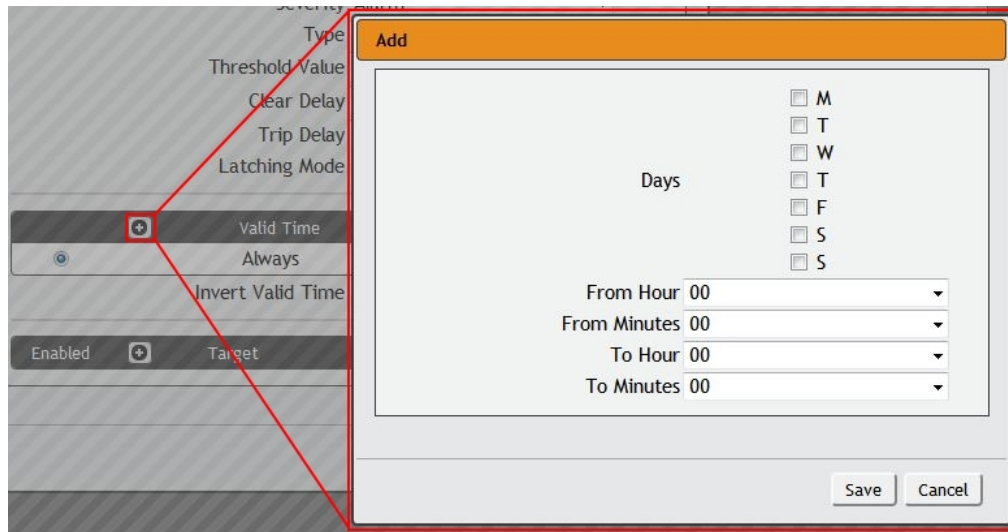
j. The *Invert Valid Time* check box inverts the selected *Valid Time* setting.

k. To determine where the alert notifications will be sent to when this particular Alarm or Warning Event occurs, click the Add icon to create a new Action, then select the desired options from the drop-down menu:
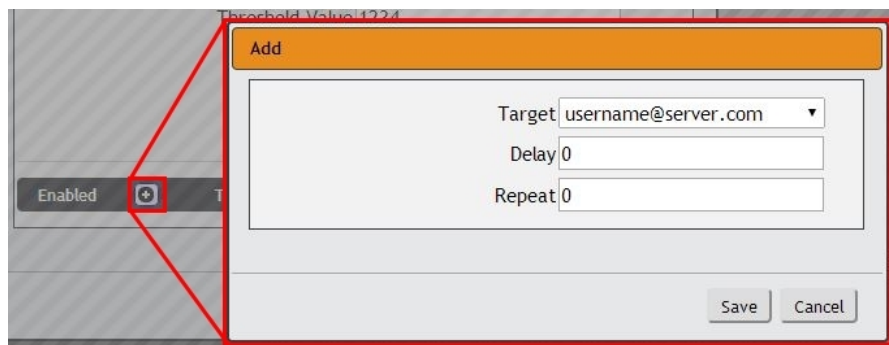
- *Target* is the e-mail address or SNMP manager to which notifications should be sent when the Event is tripped. Other options, such as "buzzer", may be available depending on your Geist PDU.

- *Delay* determines how long this Event must remain tripped before this Action's first notification is sent. (Note that this is different from the *Trip Delay*, above; *Trip Delay* determines how long the threshold value has to be exceeded <u>before</u> the Event itself is tripped.) *Delay* can be up to 14400 seconds (4 hours). A *Delay* of 0 will send the notification immediately.

- *Repeat* determines whether multiple notifications will be sent for this Event Action. *Repeat* notifications are sent at the specified intervals until the Event is acknowledged, or until the Event is cleared and reset. The *Repeat* interval can be up to 14400 seconds (4 hours). A *Repeat* of 0 disables this feature, and only one notification will be sent.

Then, click *Save* to save this notification Action.

If required, multiple Actions can be set for an Alarm or Warning; to add multiple Actions click the Add icon again and set each one as desired. Each alert can have up to 32 Actions associated with it.

To change an existing notification Action, click the Modify icon next to the Action you wish to change, then modify its settings as above.
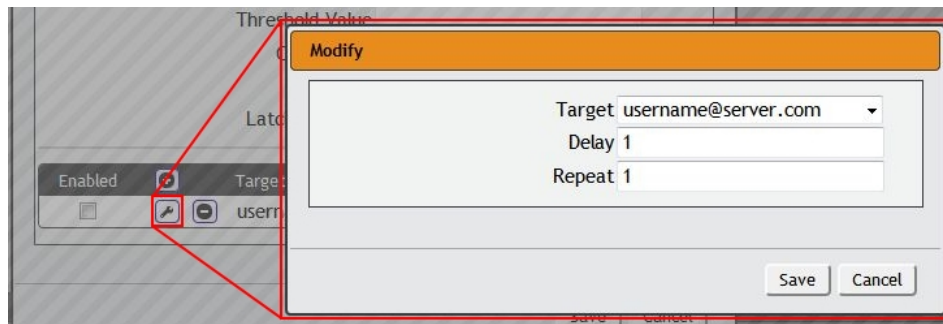
Once an Action has been added, each Action has its own checkbox in the "enabled" column at the far left. The default is unchecked (disabled) when you first add each Action; set the checkbox to enable it. (This allows you to selectively turn different Actions on and off for testing.)

To remove a notification Action entirely, click the Delete icon to remove the Action from the list, then click *Delete* to confirm:
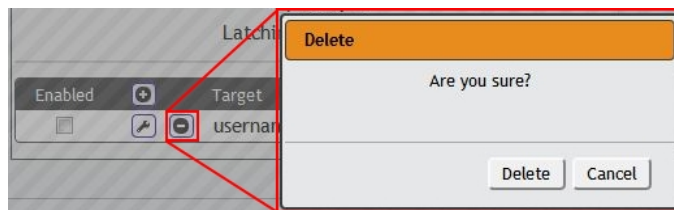
3. When finished, click *Save* to save this Alarm or Warning event.

To change an existing Alarm or Warning Event:

Click the Modify icon next to the Alarm or Warning Event you wish to change, then modify its settings as above.

To delete an existing Alarm or Warning Event:

Click the Delete icon next to the Alarm or Warning Event you wish to change, then click *Delete* to confirm.

5.1.3 Cameras

The Cameras page is a place for all of the data center's web based monitoring cameras. After a camera is added, the image is shown under the *Cameras* section.
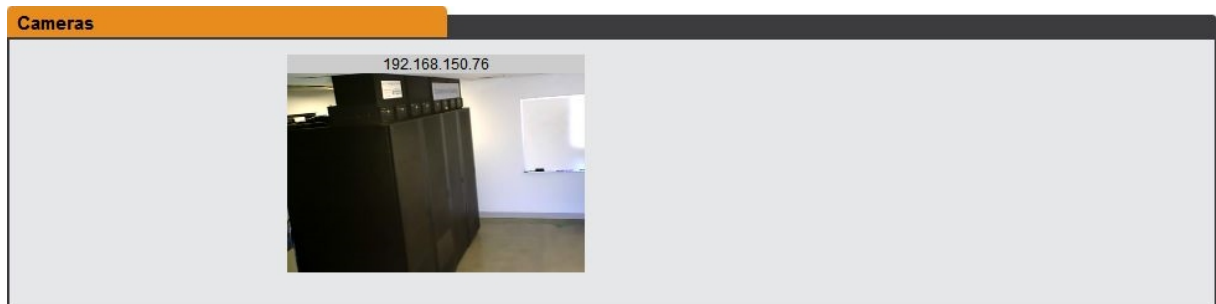
5.1.3.1 Camera Configuration

To add a new Camera:

1. Click the Add/Modify Camera button:
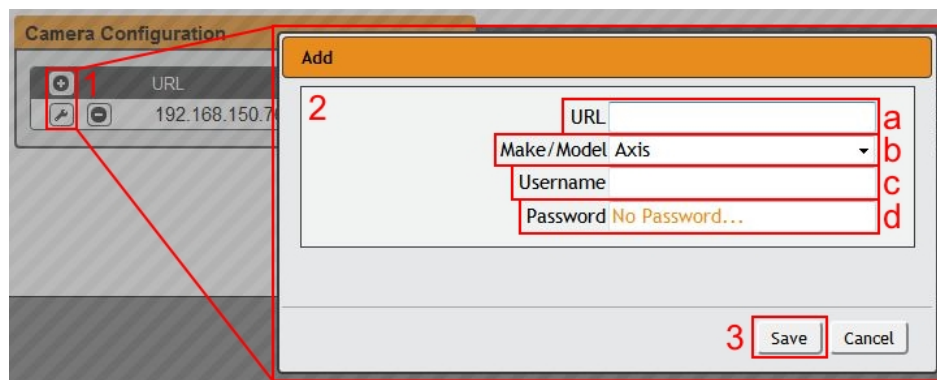
2. Set the desired conditions for this Event as follows:

   a. Enter the *URL* of the online camera.

   b. Select the *Make/Model* of camera you are connecting to.

   c. Enter the *Username* if necessary.

   d. Enter the *Password* if necessary.

3. Click *Save*.

To delete a Camera:

To remove a Camera entirely, click the Delete icon to remove the Camera from the list, then click *Delete* to confirm:
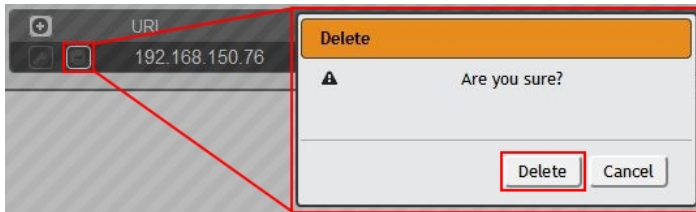
5.1.4 Logging

The Logging page allows the user to access the historical data recorded by the PDU by selecting the desired sensors and time range to be logged. The **Data Graph** section contains the historical graph, time range drop-down menu, and a list of enabled measurements. Only those with the "Graph" check-box selected will be graphed.

The PDU will default to log all data at a rate of one point per minute. Please note that although data is logged once per minute, all sensor data used in the real time display and alarm functions is read at least once every 15 seconds for internal sensors and approximately once every 30 seconds for external sensors.
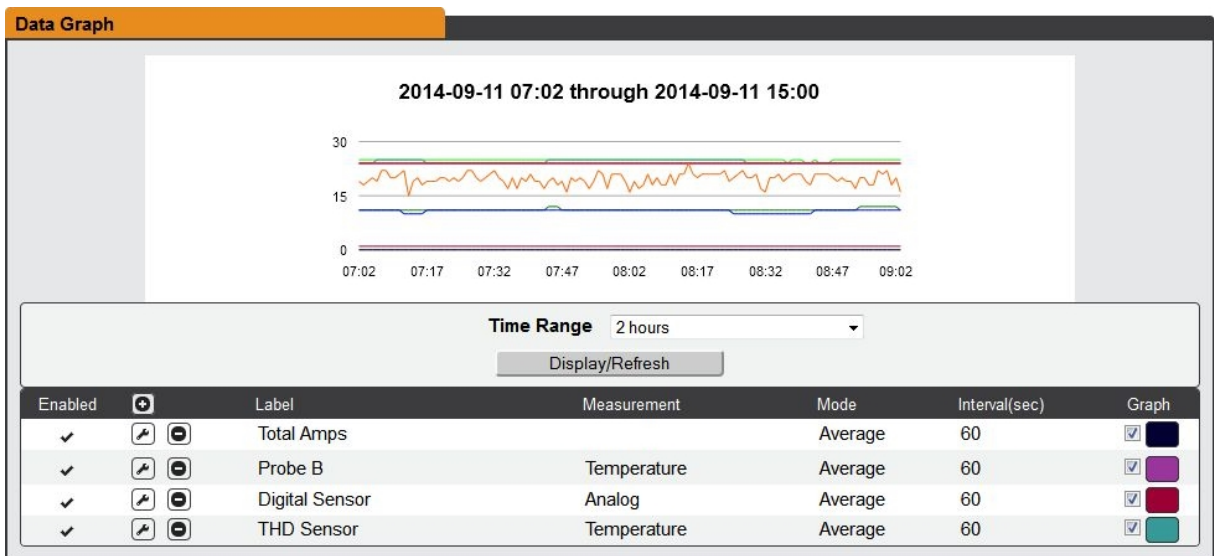
Recorded data is available for download in CSV and JSON file formats. To reset the logs click the "Clear the Log" button.
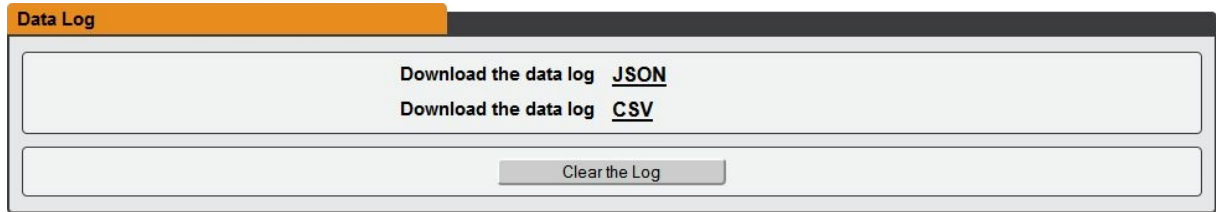
5.1.4.1 Logging Configuration

To add a new Measurement for logging:

1. Click the Add Measurement button:
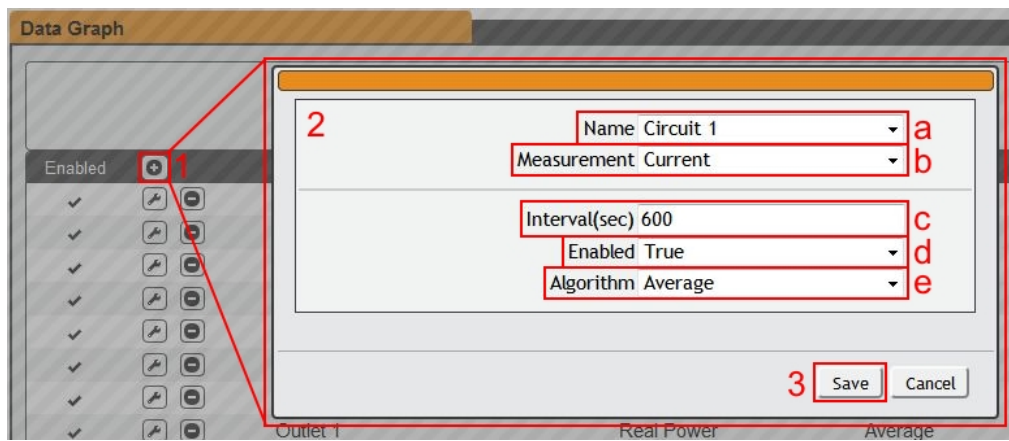
2. Set the desired conditions for this Measurement as follows:
   a. Select the *Name* of the phase or circuit you wish to measure.
   b. Select the *Measurement* (current, voltage, etc.) you want to record.
   c. Set the *Interval*, in seconds, for this Measurement.
   d. *Enable/Disable* the Measurement.
   e. Choose the *Algorithm* the device will use to record. Options are High, Low or Average.
3. Click *Save*.

To modify a Measurement:

1. Click the Modify Measurement button:
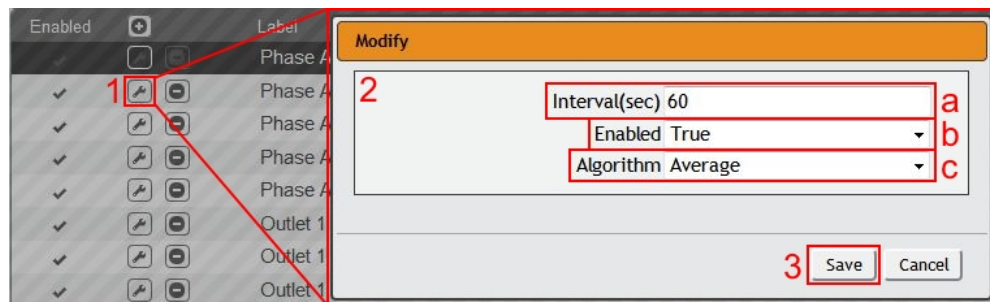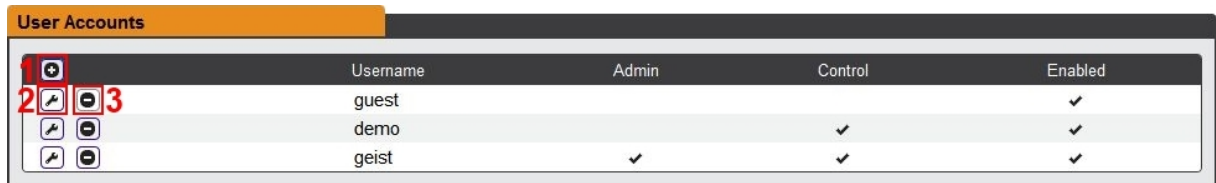
2. Set the desired conditions for this Measurement as follows:
   a. Set the *Interval*, in seconds, for this Measurement.
   b. *Enable/Disable* the Measurement.
   c. Choose the *Algorithm* the device will use to record. Options are High, Low or Average.
3. Click *Save*.

5.2 System

5.2.1 Users

The **Users** page allows you to manage or restrict access to the unit's features by creating accounts for different users.
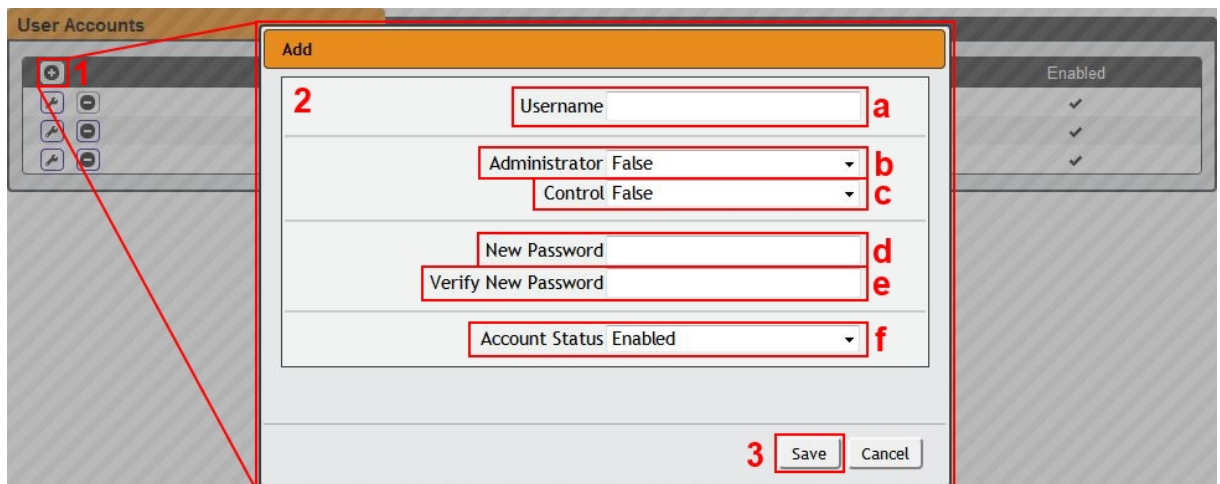
There are three buttons available on the User Accounts page:

1. **Add** New User Account
2. **Modify** User's Account
3. **Delete** User's Account

To Add or Modify a user account:

1. Click the **Add** or **Modify** User icon.
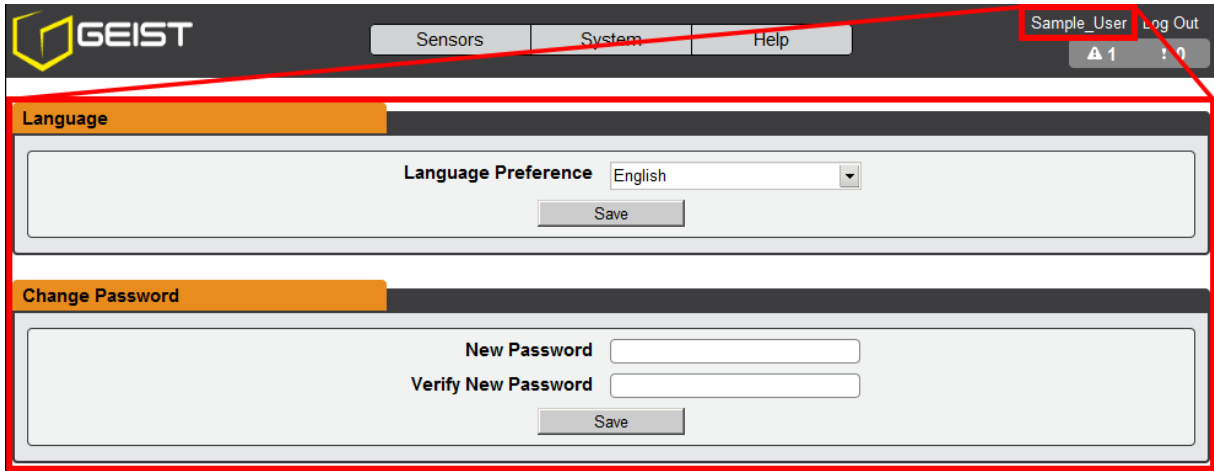
2. Create or modify the account information as follows:

   a. *Username:* the name of this account. User names may be up to 24 characters long, are case-sensitive, and may not contain spaces or any of these prohibited characters: $&`:<>[ ] { }"+%@/ ; =?\^\|~', Note that an account's username cannot be changed after the account is created.

   b. *Administrator:* if set to *True*, this account has Administrator-level access to the unit, and can change any setting.

   c. *Control:* if set to *True*, this account has Control-level access. (Setting *Administrator* to *True* will automatically set *Control* to *True* as well.) Setting this to *False* makes the account a View-Only account.

   d. *New Password:* account passwords may be up to 24 characters long, are case-sensitive, and may not contain spaces or any of these prohibited characters: $&`:<>[ ] { }"+%@/ ; =?\^\|~',

   e. *Verify New Password:* retype the account password from (d), above. Both fields must match for the password to be accepted.

   f. *Account Status:* set the account to *Enabled* or *Disabled*. Disabling an account prevents it from being used to log in, but does not delete it from the account list.

3. Click the *Save* button when finished.

Account Types:

- **Administrator**: Administrator accounts (accounts with both *Administrator* and *Control* authority set to *True*, as above) have full control over <u>all</u> available functions and settings on the device, including the ability to modify System settings and add, modify, or delete other users' accounts.

- **Control**: Control accounts (accounts with only *Control* set to *True*) have control over all settings pertaining to the device's sensors. They can add, modify, or delete Alarms & Warning Events and notification Actions, and can change the names or labels of the device and its sensors. Control accounts <u>cannot</u> modify System settings or make changes to other users' accounts.

- **View**: If both *Administrator* and *Control* are set to *False*, the account is a View-Only account. The only changes a View-Only account is permitted to make are changing their own account's password, and changing the preferred language for their own account. View-Only accounts cannot change any device or system settings.

- **Guest**: Anyone who brings up the unit's web page without logging in will automatically be viewing the unit as Guest. By default, the Guest account is a View-Only account, and cannot make changes to any settings, although the Administrator can elevate the Guest account to Control-level access if desired, allowing anyone to make changes to names, labels, alarm events, and notifications without logging in. The Guest account cannot be deleted, but it can be disabled by the Administrator.

Note: Once a user has logged in to their account, they can change their password or language preference by clicking their username, shown next to the Log Out hyperlink at the top right-hand corner of the web page, as shown here:

5.2.2   Network

The unit's network configuration is set on the Network tab of the Configuration page. Settings pertaining to the unit's network connection are:

- *Hostname:* Allow you to set the Hostname for the PDU.

- *DHCP*: Allows the unit to request a dynamic IP address from a server on the network when Enabled. (The default is Enabled, or dynamic IP addressing.)

- **DNS**: Allows the unit to resolve host names for Email, NTP and SNMP servers as well as cameras. Clicking on the Add/Modify icon will allow you to add/change the DNS Server Addresses. *Note: a maximum of 2 DNS servers are allowed*.

- **Gateway (IPv4)**: The IP address of the network gateway bridging your private network (LAN) to the public internet network. This is required if the unit needs to reach any services on the internet, such as a public email or NTP server. (If DHCP is Enabled, this field will automatically be filled in when the DHCP service assigns the unit an IP address.)

- *IP Address*: Displays the IPv4 and IPv6 addresses currently being used by the unit. Clicking on the Add/Modify icon will allow you to change the unit's IPv4 address and Netmask. (Note that if DHCP is enabled, then there will be no Modify icon, indicating that this address can't be changed by the user.) The IPv6 address is a "Link Local" address inherent to the unit, and cannot be changed.

Hostname

Hostname [quetzal]

[Save]

Network

Name ethernet
MAC Address 00:19:85:E8:4B:A6
DHCP [Disabled ▼]
Gateway (IPv4) [192.168.117.254]

[Save]

⊕	IP Address		Prefix/Netmask
⊖	192.168.117.188	/	24 (255.255.255.0)
⊖	192.168.117.104	/	24 (255.255.255.0)
	fe80::219:85ff:fee8:4ba6	/	64

⊕		DNS Server Address
🔧 ⊖		208.67.222.222
🔧 ⊖		208.67.220.220

- **HTTP Services**: Enables/disables access via HTTP and HTTPS. Available options are: HTTP and HTTPS, HTTP only, and HTTPS only. It is not possible to disable the web interface completely.

- **HTTP/HTTPS Server Port:** Allows you to change the TCP ports which the HTTP and HTTPS services listen to for incoming connections. The defaults are port 80 for HTTP, and 443 for HTTPS.

HTTP

HTTPS is always enabled.

HTTP Interface [Enabled ▼]
HTTP Port [80]
HTTPS Port [443]

[Save]

5.2.3 Web Server

Web Server

- **HTTP Services**: Enables/disables access via HTTP and HTTPS. Available options are: HTTP and HTTPS, HTTP only, and HTTPS only. It is not possible to disable the web interface completely.

- **HTTP/HTTPS Server Port:** Allows you to change the TCP ports which the HTTP and HTTPS services listen to for incoming connections. The defaults are port 80 for HTTP, and 443 for HTTPS.

- **SSL Certificate (Firmware version 4.4.0 or later):** Allows you to upload your

own signed SSL Certificate file to replace the default one. The certificate can be either self-signed or signed from a Certification Authority. Certificate must meet the following parameters:

Certificate must be in either PEM or PFX (PKCS12) format

- *PEM Format*
1. The public certificate and private key must reside in the same file
2. The certificate must follow standard x.509
3. The private key must be generated with the RSA algorithm and in PEM format
4. The PEM RSA private key may be password secured.

- *PFX Format*

   Support is also available for the PKCS12 standard (.pfx) which is a binary encrypted combination of a PEM public certificate and its PEM private key. When generating a PFX certificate you will be prompted for an optional password.

Note: If the certificate is password protected, you will need to enter that password into the GUI to upload the certificate successfully.

HTTP

	HTTPS is always enabled.

HTTP Interface	Enabled
HTTP Port	80
HTTPS Port	443
	Save

SSL Certificate

SSL Certificate File		Browse...
Password	No Password...	
	Submit	

5.2.4 Reports
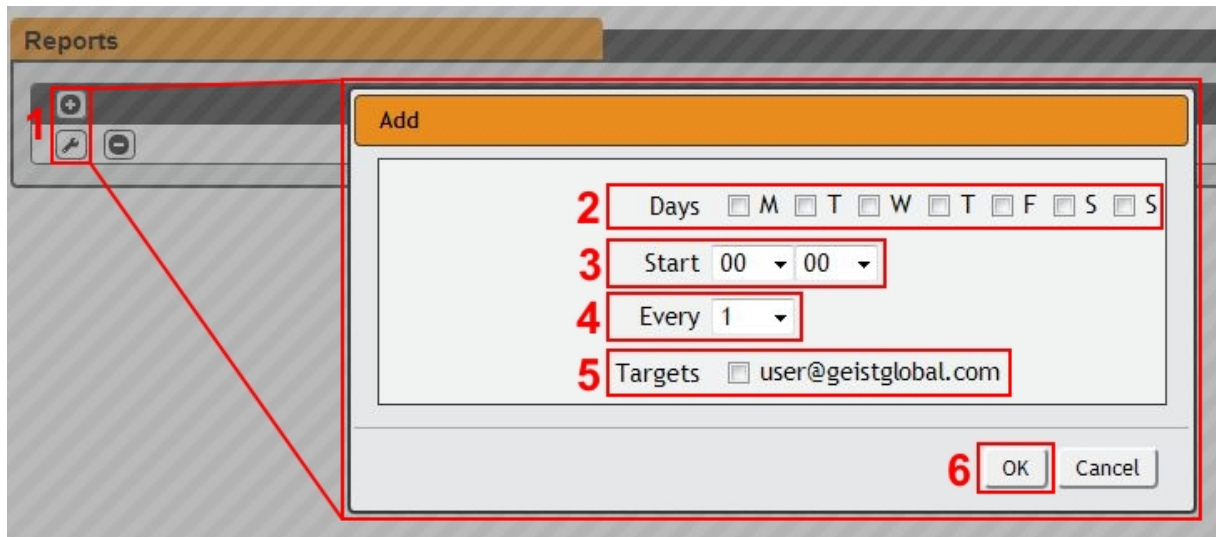
The **Reports** page allows the user to schedule the device to send recurring status reports.

Note: SMTP email must be set-up on the device via the Email page.

Reports				
⊕	Days	Start	Every	Targets
🔧 ⊖	M-W-F--	12:00	2	[1]

To Add or Modify a scheduled report:

1. Click the **Add** or **Modify** icon.

2. Select the **Days** the report is to be sent.
3. Select the time of the day to **Start** sending reports.
4. Set the interval (in hours).
5. Select the **Target** email address for the reports to be sent.
6. Click **OK** to save changes.

To Delete a scheduled Report:
1. Click on the **Delete** icon next to the report to delete.
2. Click the **OK** button on the pop-up window to confirm.

5.2.5 LDAP

The Lightweight Directory Access Protocol (LDAP) can be setup through this menu.

Enable: Enabling or Disabling LDAP

LDAP URI: LDAP Uniform Resource Identifier shall be formatted as: ldap:// HOST:PORT. The "HOST" can be an IPv4 address, an IPv6 address in brackets (ie. [2001:0DB8:AC10:FE01::]), or a host name. The default port for LDAP is 389.

Bind DN: Distinguished Name (DN) used to bind to the directory server.

Bind Password: Password used to bind to the directory server.

Base DN: DN to use for the search base.

The remaining fields come from the NIS schema, defined in RFC2307. They are used to authenticate users in LDAP. Leaving them blank will use the default value, which is shown in the picture, in orange.

User Filter: LDAP filter for selecting users.

"uid" Mapping: Name of the server attribute that corresponds to the "uid" attribute in the schema.

"uidNumber" Mapping: Name of the server attribute that corresponds to the "uidNumber" attribute in the schema.

Group Filter: LDAP filter for selecting groups

"gid" Mapping: Name of the server attribute that corresponds to the "gid" attribute in the schema.

"memberUid" Mapping: Name of the server attribute that corresponds to the "memberUid" attribute in the schema.

5.2.6 LCD Display

The LCD Display page allows the user to configure what measurements are scrolling on the local or remote LCD display.

To Add/Modify Measurements:

1. Click the Add/Modify button:
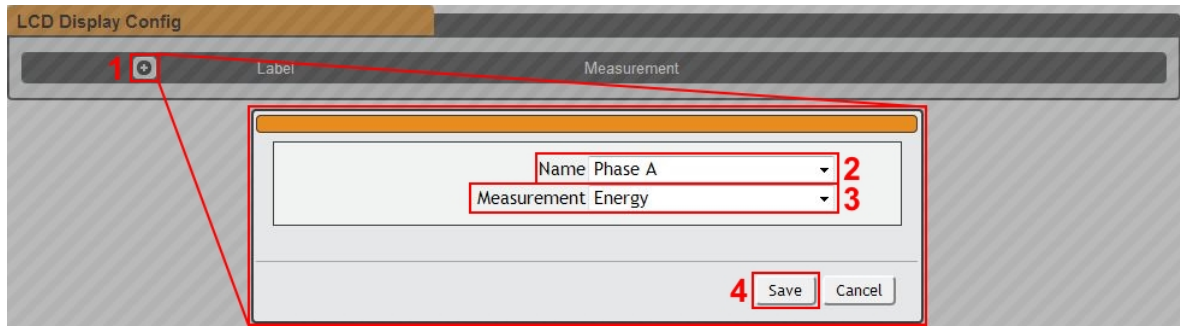
2. Select the **Name** of the desired phase or circuit to display a measurement from.

3. Select the type of **Measurement** to display.

4. Click Save.

5.2.7 Time

The unit's time and date are set on this page.
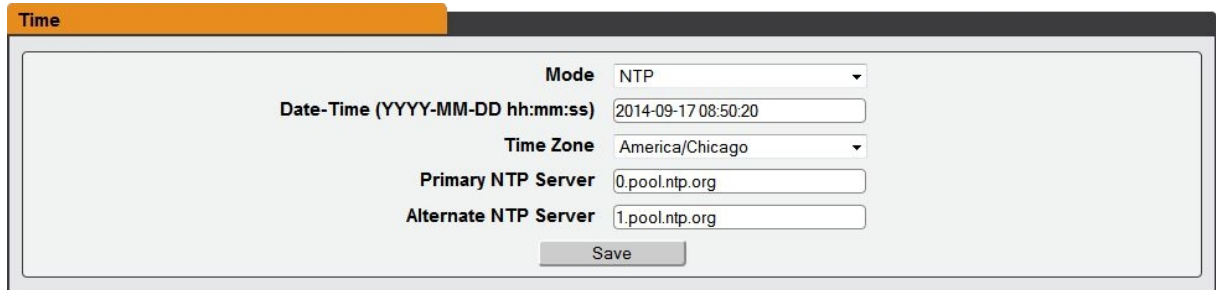
There are two mode available: **Network Time Protocol (NTP)** and **Manual**.

1. NTP synchronizes the unit's time and date to the specified time zone using listed NTP Servers. NTP servers can be reconfigured.

2. In Manual mode, the date and time must be typed as indicated on the left of the field.

5.2.8 Email

The unit is capable of sending e-mail notifications to up to five e-mail addresses when an Alarm or Warning Event occurs.

To send e-mails, the unit must be configured to access the mail server, as follows:

- **SMTP Server:** the name or IP address of a suitable SMTP or ESMTP server.

- **Port:** the TCP port which the SMTP Server uses to provide mail services. (Standard is port 25 for an unencrypted connection, or 465 for a TLS/SSL-encrypted connection.)

- **"From" Email Address:** the address the e-mails appear to come from. Note that many hosted e-mail services will require this to be the e-mail account of a valid user.

• *Username* and *Password:* the login credentials for the e-mail server. If your server does not require authentication (open relay), these can be left blank.

Set Microsoft Exchange servers to allow SMTP relay from the IP address of the unit and "Basic Authentication", so the PDU will log in with the AUTH LOGIN method of sending its login credentials. (Other methods, such as AUTH PLAIN, AUTH MD5 are not supported.)

Target e-mail addresses can be configured as follows:

Legend of icons/buttons:
1. **Add** new target email address.
2. **Modify** existing target email address.
3. **Delete** existing target email address.
4. Send **Test Email**.

To Add or Modify a Target Email address:
    1. Click on the **Add** or **Modify** icon.
    2. Type email address and then click *Save*.

To Delete a Target Email address:

1. Click on the **Delete** icon next to the address to delete.

2. Click the **Delete** button on the pop-up window to confirm.

To send a test e-mail:

1. Click on the **Test Email** icon next to the address to test.

2. A pop-up window will indicate that the test e-mail is being sent. Click *OK* to dismiss the pop-up.

5.2.9 SNMP

Simple Network Management Protocol (SNMP) can be used to monitor the unit's measurements and status, if desired. SNMP v1, v2c and v3 are supported. In addition, alarm traps can be sent to up to two IP addresses.

The *SNMP Service* can be enabled or disabled. The service will listen for data-read requests (a.k.a. "Get requests") on *Port* 161, which is the usual default for SNMP services; this can also be changed if desired.

The MIB is can be downloaded from the unit, via the link at the top of the page. Clicking this link will download a .ZIP archive containing both the MIB file and a CSV-formatted spreadsheet describing the available OIDs in a readable form to assist in setting up a SNMP manager.

The *Users* section allows users to configure the various Read, Write, and Trap communities for SNMP services, authentication types and encryption methods used for the SNMP v3 communities.
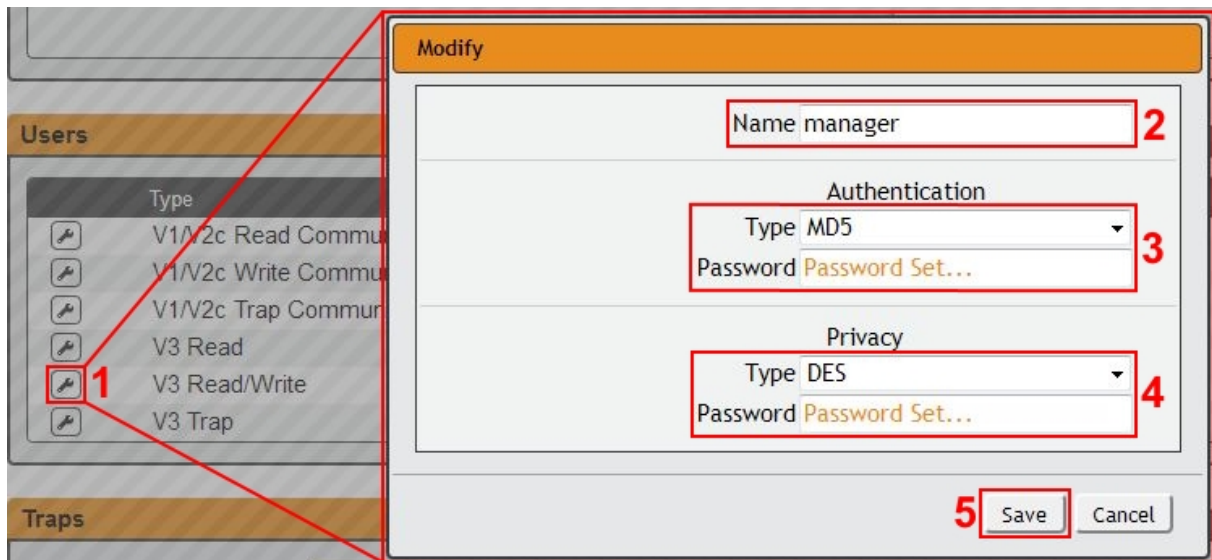
To configure:
1. Click the **Modify** icon.
2. Configure the **Name**.
3. Configure the **Authentication** type and assign a password.
4. Configure the **Privacy** type and assign a password.
5. Click **Save** to save changes.
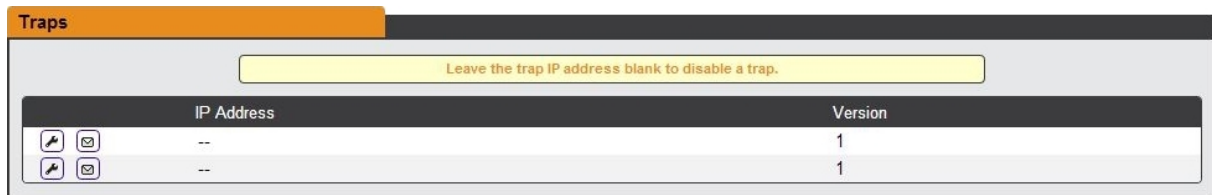
Traps allow users to define the IP address(es) and SNMP types.
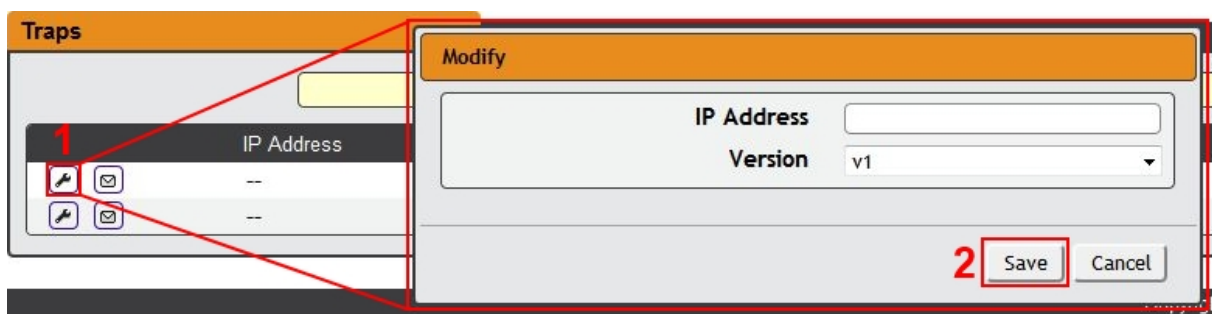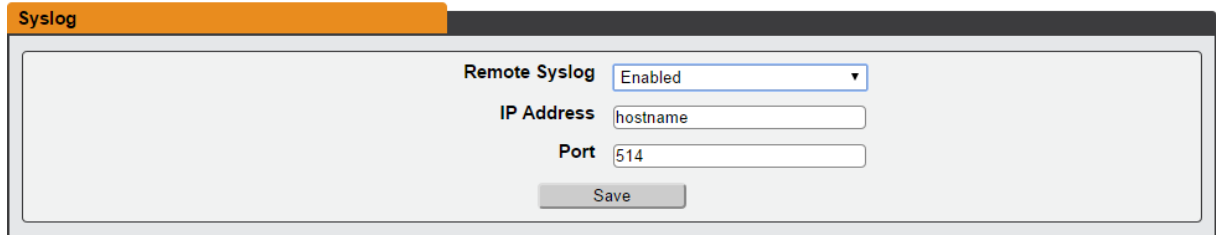
To configure a trap destination:

1. Locate the **Traps** section of the SNMP page, and click on the **Modify** icon.

2. Enter the **IP Address** which the trap should be sent to, select the trap **Version** to be used (v1, v2c, or v3), and click **Save**.

A test trap may be sent by clicking on the Test icon next to the trap destination.

5.2.10 Syslog
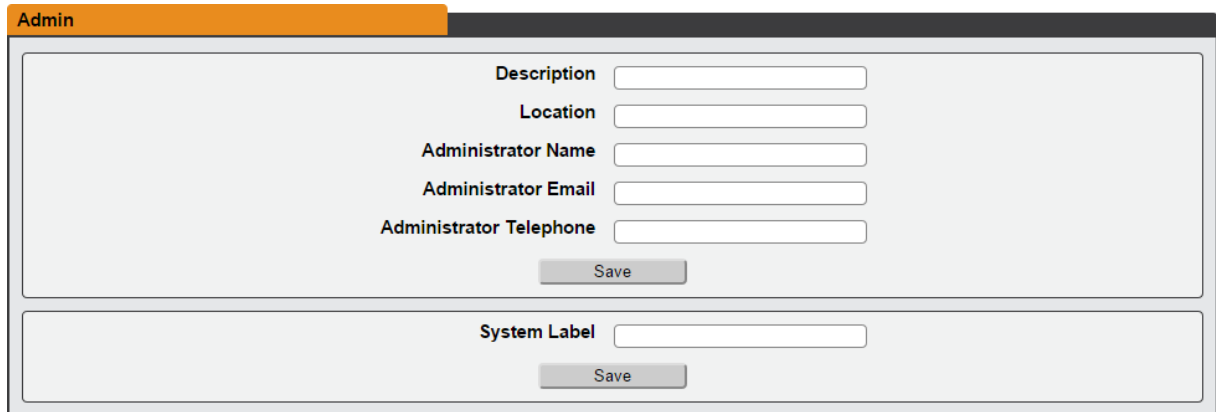
Syslog data can be relayed to a remote syslog server but must be setup and enabled via the *Syslog* page. Note that this function is to be used for diagnostic purposes.

Syslog	
Remote Syslog	Enabled ▼
IP Address	hostname
Port	514
	Save

5.2.11 Admin
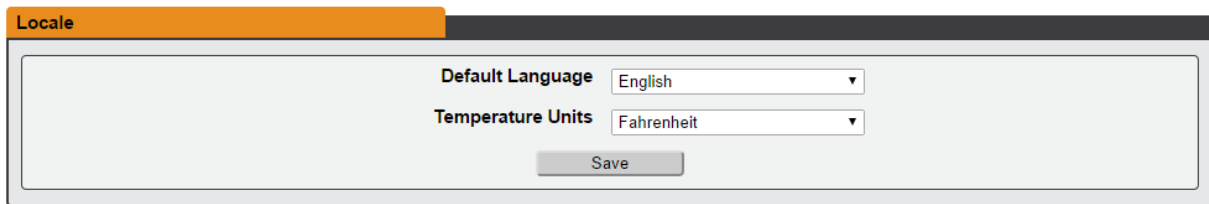
The Admin page allows the administrator of the device to save their contact information along with the device description and location. Once the info is saved by an administrator, other (non-administrator) users can view the information. The System Label can be modified on this page; this label is shown in the title bar of the web browser's window and on the browser tab currently viewing the device.

Note: This information is strictly for the users' and administrator's convenience; the unit will not attempt to send e-mails to the "Administrator Email" address, and this address cannot be chosen as the Target of an Event Action when configuring an Alarm or Warning Event, unless it is added as a target.

Admin	
Description	
Location	
Administrator Name	
Administrator Email	
Administrator Telephone	
	Save
System Label	
	Save

5.2.12 Locale

The Locale page sets the default Language and Temperature Units for the device. These settings will become the default viewing options for the device, although individual users can change these options for their own accounts. (The Guest account will only be able to view the device with the options set here.)

5.2.13 Utilities

The Utilities page can be used to restore settings to default values, reboot the PDU interface, perform firmware and enable/disable factory access.

Restore Defaults: allows the user to restore the unit's settings to the factory defaults. There are two options:

All Settings: Erases <u>all</u> of the unit's settings, including all Network and User Accounts settings, effectively reverting the entire unit back to its original out-of-the-box state.

All Non-Network Settings: Erases all settings <u>except</u> the Network and User Accounts.

Reboot: Reboot the PDU interface card

Firmware Update: Use the Firmware Update section to load firmware updates into the unit. Firmware updates can be found on the Geist website:

http://www.geistglobal.com/supportfirmware-updates/power-firmware

Users can subscribe to a mailing list, to be notified of when firmware updates become available.

Firmware updates will come in a .ZIP archive file containing several files including the firmware package itself, a copy of the SNMP MIB, a "readme" text file explaining how to install the firmware, and various other support files as needed.

Factory Access: Enabling Factory Access mode allows Geist support technicians

access to more in-depth diagnostic information. It is recommended that this option be set to Disabled unless a Geist support member   instructs you to enable it.

Restore Defaults

Restore to Default Settings   [All Settings ▾]

[Save]

Reboot

[Reboot]

Firmware Update

Firmware Package File   [   ] [Browse...]

[Submit]

Factory Access

Factory Access   [Enabled ▾]

[Submit]

5.3 Help

5.3.1 Info

The Info Page displays the unit's current configuration information, including the device name and ID, the PDU's current firmware versions, and network information.

Info

Device Name	RCU-OD
Device ID	020C6FE3851900C3
Device Type	Pow-Swi-250-DB
Version	4.2.0
GUI Version	1.0.7
MAC Address	00:19:85:E3:6F:0C
Hostname	192.168.116.118
Manufacturer	Geist Global
Manufacturer Site	www.geistglobal.com
Support Site	www.geistglobal.com/support/power
Support Email	support@geistglobal.com
Support Telephone	1-800-432-3219

5.3.2 Support Site

Technical support and documentation can be found at http://www.geistglobal.com/support/power

6 Communication

6.1 Web API

Geist's Web API is designed to provide developers and integrators an easy to use method to communicate with the device. All of the device's actions can be accessed through this API. It is all HTTP POST with JSON as the underlying data structure.

6.1.1 Definitions

__ACTION_ID__ : Action identifier. Unique across all actions on the system. A string representation of number (e.g. "1").

__CAMERA_ID__ : Camera identifier. Unique across all cameras on the system. A string representation of number (e.g. "1").

__CAMERA_INDEX__ : Index into the supported cameras table. A string representation of number (e.g. "1").

__DISPLAY_ID__ : Display source identifier. Unique across all actions on the system. A string representation of number (e.g. "1").

__EMAIL_REPORT_ID__: String representation of a unique number to refer to email report definitions.

__EMAIL_TARGET_ID__ : Email target identifier. Unique across all email targets on the system. A string representation of number (e.g. "1").

__GROUP_ID__ : Outlet group identifier. Unique in a outlet group block on a given device. A string representation of number (e.g. "1").

__LDAP_GROUP_NAME__: A unique group name (string) for use with LDAP

__LOG_ID__ : Datalog identifier. Unique across all actions on the system. A string representation of number (e.g. "1").

__MEASUREMENT_ID__ : Measurement identifier. Unique inside a measurement block for a device or component. A string representation of number (e.g. "1").

__OUTLET_ID__ : Outlet identifier. Unique in an outlet block on a given device. A string representation of number (e.g. "1").

__RELAY_ID__ : Relay identifier. Unique in a relay block on a given device. A string representation of number (e.g. "1").

__RETURN_CODE__ : A code that uniquely identifies the result of an operation. The number 0 is reserved for a success and other codes may express a authorization failure or a malformed JSON structure.

__RETURN_MESSAGE__ : Additional information that may be required to further detail the result of an operation.

__SERIAL_NUM__ : Device identifier. Unique across all devices on the system. A 16 character hex string (e.g. "1A0004A37971E9C3").

__SNMP_USER_ID__: String from "0" through "5". Range could change later.

__TRAP_TARGET_ID__ : Trap target identifier. Unique across all trap targets on the system. A string representation of number (e.g. "1").

__TRIGGER_ID__ : Alert trigger identifier. Unique across all alerts on the system. A string representation of number (e.g. "1").

__TYPE__ : Device type. Identifies the device as one of our supported sensors and determines what components can be expected in its JSON structure. Will also drive how this device is displayed on the GUI. A string (e.g. "remoteTemp").

__USER_ID__ : User identifier. Unique across all users on the system. An alpha-numeric string (e.g. "Dan42").

6.1.2 Error Codes

6.1.2.1 Success

0 - Success

6.1.2.2 Authentication Errors

- 1000 - No Admin user configured
- 1001 - Not Authorized
- 1002 - Not Authorized: Session expired
- 1003 - Not Authorized: Not enough permissions
- 1004 - Not Authorized: Invalid password
- 1005 - User not found
- 1008 - Must have at least one admin user

6.1.2.3 JSON Format Errors

- 2000 - Malformed JSON
- 2001 - Missing Field

6.1.2.4 Path Errors

- 3000 - Invalid path
- 3001 - Path not found
- 3002 - Identifier not found
- 3003 - Field not applicable

6.1.2.5 Validation Errors

- 4000 - Invalid input
- 4001 - Input too long
- 4002 - Invalid characters
- 4003 - Invalid serial
- 4004 - Invalid boolean
- 4005 - Out of range

- 4006 - Invalid integer
- 4007 - Invalid number
- 4008 - Invalid url
- 4009 - Invalid ip
- 4010 - Paths not allowed
- 4011 - Invalid username
- 4012 - Invalid email address
- 4013 - Invalid option
- 4014 - Invalid datetime
- 4015 - Out of bounds
- 4016 - Invalid week
- 4017 - Duplicate entry

6.1.2.6 Other Errors

- 5000 - Unknown error
- 5001 - Command not allowed
- 5002 - System busy

6.1.2.7 Consistency Errors

- 6000 - Inconsistent state
- 6001 - Syslog enabled requires target
- 6002 - NTP mode requires servers
- 6003 - Start time must come before end time

6.1.2.8 Firmware Errors

- 7000 - Invalid firmware package (bogus file)
- 7001 - Invalid file key (wrong OEM)
- 7002 - Invalid version (Version is too old or otherwise unsupported)
- 7003 - Invalid product (Blackbird has different FW for each product, this happens when you try to load a WD15 image on a WD100)

6.1.3 Usage

Requests:

```
HTTP POST path/to/object
{
  "token" : "access token"
  "cmd" : "get"/"set"/"special"
  "filter" : ["label", "measurement", ...]
  "data" : { ... }
}
```

Response:

```
{
  "retCode" : 0/__RETURN_CODE__
  "retMsg" : "__RETURN_MESSAGE__"
  "data" : { ... }
}
```

6.1.3.1 Get Operations

Note: GET operations are always available to enabled users including Guest.

```
HTTP POST path/to/object
{
  "token" : "access token"
  "cmd" : "get"
  "filter" : ["label", "measurement", ...]
}
```

In order to perform a get, the client sends a post to the desired path on the server. The path can be arbitrary as long as it can be resolved to an object or component in the API structures defined below. The get will return a JSON structure starting at the depth indicated by the path and traversing down to the leaf objects. The "filter" field is optional and can be used to fine tune the returned structure. Filters are composed of an array of leaf object names and any number of them can be specified. If a filter is present, the returned structure will only contain objects that match the name specified starting from the path requested.

Examples:

```
HTTP POST api/conf/contact
{
  "token" : "*****"
  "cmd" : "get"
}
Response:
{
  retCode : 0
  retMsg : ""
  data : {
    description : someplace over the rainbow
    location : way up high
    contactEmail : dorothy@oz.com
    contactName : dorothy
    contactPhone : 5558675309
  }
}

HTTP POST api/dev
{
  "token" : "*****"
```

```
    "cmd" : "get"
    "filter" : ["latching"]
  }
  Response:
  {
    retCode : 0
    retMsg : ""
    data : {
      "1A0004A37971E9C3" : {
        "measurement" : {
          "temperature" : {}
          "humidity" : {}
        }
        "relay" : {
          "1" : { "latching" : true }
        }
      }
    }
  }
```

6.1.3.2 Set Operations

Note: *SET operations must be performed by a user with the right access level.*

```
HTTP POST path/to/object
{
  "token" : "access token"
  "cmd" : "set"
  "data" : { ... }
}
```

In order to perform a set, the client sends a post to the desired path on the server. The path can be arbitrary as long as it can be resolved to a settable object or component in the API structures defined below. The data field of the post contains a JSON structure indicating which objects are to be changed and what the new values are. Any missing objects are left unmodified on the server side. Sets can only be performed at a given depth and sub-objects are not allowed. The response object indicates if there were any errors and no extra data is returned.

Example:

```
HTTP POST api/conf/contact
{
  "token" : "*****"
  "cmd" : "set"
  "data" : {
    description : someplace over the rainbow
    location : way up high
    contactPhone : 5558675309
  }
```

```
}
Response:
{
  retCode : 0
  retMsg : ""
}
```

6.1.3.3 Special Operations

Note: *Special operations must be performed by a user with the right access level.*

```
HTTP POST path/to/object
{
  "token" : "access token"
  "cmd" : "defaults"
  "data" : {...}
}
```

Special commands are used to perform other operations that are not covered by sets or gets. Each object may have a set of valid operations along with specific requirements for the data sent. The request and response format is the same as with the sets and gets. Special operations and their parameters are only valid on the path that defines them.

6.1.4 /api/dev

6.1.4.1 Top Level

Object

```
{
  __SERIAL_NUM__ : {...}
  __SERIAL_NUM__ : {...}
  ...
}
```

Operations
None

6.1.4.2 __SERIAL_NUM__

Object

```
{
  __SERIAL_NUM__ : {
    type: __TYPE__,
    state: normal/unavailable/degraded,
    *alarm : {
      *state: none/clear/acked/latched/tripped,
```

```
            *severity : ""/warning/alarm
        }
        name : default name
        label: user name,
        measurement : {...},
        analog: {...},
        outlet : {...},
        entity : {...},
        relay : {...},
        layout : {...}
        order : index
    }
    __SERIAL_NUM__ : {...}
    ...
}
```

Operations

delete:
Remove specified devices.

Access: Control
Parameters:

```
data : {}
```

6.1.4.2.1 Measurement

Object

```
measurement : {
  __MEASUREMENT_ID__ : {
    *type : measurement type
    *value : 42,
    *name : some official name
    label : some user name,
    *units : potatoes,
    *state : normal/unavailable,
    *alarm : {
      *state: none/clear/acked/latched/tripped,
      *severity : ""/warning/alarm
    }
    *note : some note,
    *min : 0,
    *max : 100,
  }
  __MEASUREMENT_ID__ : {...}
  ...
}
```

       *Not user-settable

Operations
None

6.1.4.2.2 Analog Inputs

Object

```
analog : {
  __ANALOG_ID__  : {
    *type : 5V/10V
    *value : 42,
    *name : some official name
    label : some user name,
    **units : potatoes,
    *state : normal/unavailable,
    *alarm : {
      *state: none/clear/acked/latched/tripped,
      *severity : ""/warning/alarm
    }
    **min : 0,
    **max : 100,
    mode : door/powerFailure/flood/waterSnake/smoke/
batVoltage/customVoltage/customCurrent/customBinary,
    **highLabel : "on",
    **lowLabel : "off",
  }
  __ANALOG_ID__  : {...}
  ...
}
```
*Not user-settable
**User-settable only in custom modes

Operations
None

6.1.4.2.3 Outlet

Object

```
outlet : {
  __OUTLET_ID__  : {
    *group : __GROUP_ID__, //maybe
    *name : official name,
    label : outlet name,
    url : asdasd,
    *state: on/off/on2off/off2on/rebootOn/rebootOff/
unavailable,
    *alarm : {
```

```
        *state: none/clear/acked/latched/tripped,
        *severity : ""/warning/alarm
      }
      *timeToAction : 30 //seconds,
      *relayFailure: true/false,
      onDelay : 60 //seconds,
      offDelay : 60 //seconds,
      rebootDelay : 60 //seconds,
      rebootHoldDelay : 5 //seconds,
      poaAction : on/off/last,
      poaDelay : 60 //seconds,
      measurement : {...}
    }
    __OUTLET_ID__ : {...}
    ...
}
```
*Not user-settable

Operations

control:
> Performs an action on the outlet. Used to turn it on or off or reboot. Should be called on a path to a particular outlet and may only affect a single one.
>
> Access: Control
> Path: `dev/__DEVICE_ID__/outlet/__OUTLET_ID__`
> Parameters:
>
> ```
> data : {
>   action : on/off/reboot/cancel
>   delay : true/false
> }
> ```

reset:
> Resets KWHr on an outlet. Should be called on a path to a particular outlet and may only affect a single one. Only applicable if the outlet has KWHr measurement.
>
> Access: Control
> Parameters:
>
> ```
> {
>   "target": "energy"
> }
> ```

6.1.4.2.4 Entity

Object

```
entity : {
   __ENTITY_ID__ : {
     name : Breaker 1
     label : Computer 1
     *alarm : {
        *state: none/clear/acked/latched/tripped,
        *severity : ""/warning/alarm
     }
     measurement : {...}
   }
   __ENTITY_ID__ : {...}
   ...
}
```

Operations

reset:
Resets certain parameters on an entity. Should be called on a path to a particular entity and may only affect a single one. Only applicable if the entity has the relevant capability. Targets can be energy (clears accumulated energy) or minmax (clears minimum and maximum values, i.e. voltage max and voltage min).

Access: Control
Parameters:

```
{
   "target": "energy"/"minmax"
}
```

control:
Performs an action on all outlets within the entity (if applicable)

Access: Control
Path: dev/__DEVICE_ID__/outlet
Parameters:

```
data : {
   action : on/off/reboot/cancel
   delay : true/false
}
```

6.1.4.2.5 Relay

Object

```
relay : {
  __RELAY_ID__ : {
    *name : relay 1
    label : some name,
    energizedLabel : Energized,
    deenergizedLabel : Deenergized,
    *state : on/off/latchedOn/latchedOff,
    *alarm : {
       *state: none/clear/acked/latched/tripped,
       *severity : ""/warning/alarm
    }
    *mode : alarmControl/overrideOn/OverrideOff/,
  }
  __RELAY_ID__ : {...}
  ...
}
```
*Not user-settable

Operations

control:
Sets the relay to a particular mode or performs an ack on it.

Access: Control
Parameters:

```
data : {
  action : forceOn/forceOff/alarmControl
}
```

6.1.4.2.6 Layout

Object

```
layout : {
  0 : [__ID__, __ID__, ...],
  __ID__ : [__ID__, __ID__, ...],
  ...
}
```

The layout object defines a hierarchical structure and groupings between elements of the device. A particular ID field (be it __OUTLET_ID__, __ENTITY_ID__ or any other kinds of ID available within this device) is mapped to a list of ID fields representing its children. A special 0 ID is used to declare the top level elements of the hierarchy. For example, if an entity with ID 1 contains two outlets with IDs 1 and 2, the object would

look as follows:

```
layout : {
  0 : [entity/1],
  "entity/1" : [outlet/1,outlet/2]
}
```

The order of the elements within the lists is relevant and will affect the order in which they are displayed on the GUI.

Operations
　None

6.1.5　/api/alarm

6.1.5.1　Top Level

Object

```
{
  trigger : {...}
  action : {...}
  target : {...}
  validTime : {...}
}
```

Operations
　None

6.1.5.2　trigger:

Object

```
{
  __TRIGGER_ID__ : {
   *state: clear/acked/latched/tripped/inactive,
    severity : alarm/warning,
    latching : true/false
    type : high/low/status
    path: __DEVICE_ID__/path/to/alarmed/object
    threshold : 40,
    clearDelay : 0-14400 (seconds. Translates to 240
minutes),
    tripDelay : 0-14400 (seconds. Translates to 240
minutes),
    validTime : __VALID_TIMES_ID_ //blank for always valid
    invertValidTime : true/false
    selectedActions : [__ACTION_ID__, __ACTION_ID__, ...,
__ACTION_ID__ ]
  }
```

```
      __TRIGGER_ID__ : {...}
      ...
}
```
*Not user settable

Operations

delete:
Removes the target alert from the system. Called on the `/api/alarm/trigger/__TRIGGER_ID__` path.

Access: Control
Parameters: None

ack:
Acknowledges the target alert. Called on the `/api/alarm/trigger/__TRIGGER_ID__` path. Acking causes actions to stop for this trigger until it clears and trips again.

Access: Control
Parameters: None

add:
Adds the target alert to the system. Must adhere to the maximum supported. Called on the `/api/alarm/trigger` path.

Access: Control
Parameters:

```
data : {
    type : high/low/unplugged
    severity : alarm/warning,
    path: __DEVICE_ID__/path/to/alarmed/object
    threshold : 40,
    clearDelay : 0-14400 (seconds. Translates to 240
minutes),
    tripDelay : 0-14400 (seconds. Translates to 240
minutes),
    validTime : __VALID_TIMES_ID_ //blank for always valid
    invertValidTime : true/false
    selectedActions : [__ACTION_ID__, __ACTION_ID__, ...,
__ACTION_ID__ ]
}
```

set:
Modifies the target alert on the system. Called on the `/api/alarm/trigger/__TRIGGER_ID__` path.

Access: Control
Parameters:

```
data : {
    severity : alarm/warning,
    path: __DEVICE_ID__/path/to/alarmed/object
    threshold : 40,
    clearDelay : 0-14400 (seconds. Translates to 240
minutes),
    tripDelay : 0-14400 (seconds. Translates to 240
minutes),
    validTime : __VALID_TIMES_ID_ //blank for always valid
    invertValidTime : true/false
    selectedActions : [__ACTION_ID__, __ACTION_ID__, ...,
__ACTION_ID__ ]
}
```

6.1.5.3 action:

Object

```
{
  __ACTION_ID__ : {
    target : __TARGET_ID__
    delay : 0-14400 (seconds. Translates to 240 minutes)
    repeat : 0-14400 (seconds. Translates to 240 minutes)
(Only on triggers supporting repeat. For now, these are
emails and traps)
  }
  __ACTION_ID__ : {...}
  ...
}
```

Operations

delete:
Removes the target action from the system. Called on the `/api/alarm/action/__ACTION_ID__` path.

Access: Control
Parameters: None

add:
Adds the target action to the system. Must adhere to the maximum supported. Called on the `/api/alarm/action` path.

Access: Control
Parameters:

```
data : {
    target : __TARGET_ID__
    delay : 0-14400 (seconds. Translates to 240 minutes)
    repeat : 0-14400 (seconds. Translates to 240 minutes)
}
```

set:

Modifies the target action on the system. Called on the `/api/alarm/action/__ACTION_ID__` path.

Access: Control
Parameters:

```
data : {
    target : __TARGET_ID__
    delay : 0-14400 (seconds. Translates to 240 minutes)
    repeat : 0-14400 (seconds. Translates to 240 minutes)
}
```

purge:

Removes any currently unassigned action from the system. Called on the `/api/alarm/action` path. Basically this is a quick way for the user to make room in their action table without having to go back and see if any actions are not currently being used and deleting them manually.

Access: Control
Parameters: None

6.1.5.4 target:

Object

```
{
  __TARGET_ID__ : {
    name : something@something.com
    group : email/trap/devName
    type : email/trap/buzzer/outlet/relay
    enabled : true/false
  }
  __TARGET_ID__ : {...}
  ...
}
```

Note: *Actions are arranged based on the group string. There are 2 special group names, trap and email. These can be localized. Otherwise, the group name is used as is.*

Operations

None

6.1.5.5 validTime:

Object

```
{
  __VALID_TIMES_ID__ : {
    start : 16:15 (00-24 hour number plus minutes. 00:00 to
24:00 means all day)
    stop : 06:15 (00-24 hour number plus minutes. 00:00 to
24:00 means all day)
    days : "MTWTFSS"/"M----S-" (The letter of the day is
present if that day is enabled or '-' if not)
  }
  __VALID_TIMES_ID__ : {...}
  ...
}
```

Operations

delete:
Removes the target valid time from the system. Called on the `/api/alarm/validTime/__VALID_TIMES_ID__` path

Access: Control
Parameters: None

add:
Adds the target valid time to the system. Must adhere to the maximum supported. Called on the `/api/alarm/validTime` path

Access: Control
Parameters:

```
data : {
    start : 16:15
    stop : 06:15
    days : M----S-
}
```

set:
Modifies the target valid time on the system. Called on the `/api/alarm/validTime/__VALID_TIMES_ID__` path

Access: Control
Parameters:

```
data : {
```

```
        start : 16:15
        stop : 6:15
        days : M----S-
}
```

purge:
Removes any currently unassigned valid time from the system. Called on the `/api/alarm/validTime` path. Basically this is a quick way for the user to make room in their valid time table without having to go back and see if any times are not currently being used and deleting them manually.

Access: Control
Parameters: None

6.1.6 /api/datalog

Object

```
{
    __LOG_ID__ : {
    "enabled": true/false,
    "path": "00001/measurements/1",
    "algorithm": "high/low/average",
    "interval": integer (seconds)
  }
}
```

Operations

set

Permissions: Control

add

Permissions: Control
Path: `/api/datalog`
Parameters:

```
{
   "path": "00001/measurements/1",
   "algorithm": "high/low/average", (optional: defaults to
average)
   "interval": integer (seconds) (optional: defaults to 60)
}
```

delete

Permissions: Control

Path: `/api/datalog/__LOG_ID__`
Parameters: none

6.1.7 /api/display

Object

```
{
  "source": {
    __DISPLAY_ID__ : {
      "path": "00001/measurements/1",
    }
  }
}
```

Operations

add

Permissions: Control
Path: `/api/display/source`
Parameters:

```
{
  "path": "00001/measurements/1",
}
```

delete

Permissions: Control
Path: `/api/display/source/__DISPLAY_ID__`
Parameters: None

6.1.8 /api/conf

6.1.8.1 Top Level

Object

```
{
  network : {...}
  contact : {...}
  system: {...}
  report: {...}
  email : {...}
  snmp : {...}
  http : {...}
  time : {...}
```

```
        syslog : {...}
        lcd : {...}
        ldap: {...}
        led : {...}
        locale : {...}
        camera : {...}
    }
```

Operations
None

6.1.8.2 network:

Object

```
{
  __IFACE_ID__ : {
    enabled : true/false
    macAddr : 00:04:A3:1E:99:D7,
    dhcpOn : true/false,
    dns : {...},
    address : {...},
    ip4GW : 192.168.123.1,
    ip6GW : fe::01
  }
}
```

Operations
None

6.1.8.2.1 network/addresses

Object

```
address : {
  __ADDR_ID__ : {
    address : 192.168.123.1 or fe::01
    prefix : 24
    mutable : true/false
  },
  __ADDR_ID__ : ...
  ...
}
```

Operations

add:
Adds the address to the system. Must adhere to the maximum supported.

Access: Admin

Parameters:

```
data : {
  address : 192.168.123.1 or fe::01
  prefix : 24
}
```

set:
    Sets the address to the new values. Must be called on `api/conf/network/__IFACE_ID__/address/__ADDR_ID__` path.

    Access: Admin
    Parameters:

```
data : {
  address : 192.168.123.1 or fe::01
  prefix : 24
}
```

delete:
    Deletes the address from the system. Must be called on `api/conf/network/__IFACE_ID__/address/__ADDR_ID__` path.

    Access: Admin
    Parameters: None

6.1.8.2.2 network/dns

Object

```
dns : {
  __DNS_ID__ : {
    address : 192.168.123.1 or fe::01
  },
  __DNS_ID__ : ...
  ...
}
```

Operations

add:
    Adds the address to the DNS list. Must adhere to the maximum supported.

    Access: Admin
    Parameters:

```
data : {
  address : 192.168.123.1 or fe::01
```

```
        }
```

set:
    Sets the address in the DNS list to the new value. Must be called on `api/conf/network/__IFACE_ID__/address/__DNS_ID__` path.

    Access: Admin
    Parameters:

```
data : {
   address : 192.168.123.1 or fe::01
}
```

delete:
    Deletes the address from the DNS list. Must be called on `api/conf/network/__IFACE_ID__/address/__DNS_ID__` path.

    Access: Admin
    Parameters: None

6.1.8.3 contact:

Object

```
{
  description : someplace over the rainbow
  location : way up high
  contactEmail : dorothy@oz.com
  contactName : dorothy
  contactPhone : 5558675309
}
```

Operations

set:

    Access: Admin
    Parameters:

```
data : {
  description : someplace over the rainbow
  location : way up high
  contactEmail : dorothy@oz.com
  contactName : dorothy
  contactPhone : 5558675309
}
```

6.1.8.4 system:

Object

```
{
   label: string
}
```

Operations

set:

Access: Admin
Parameters:

```
data : {
   label: string
}
```

6.1.8.5 report:

Object

```
report: {
   __EMAIL_REPORT_ID__ : {
      start: "12:00" //same rules as alarm/validTime/start
      days: "M-W-F--" //same rules as alarm/validTime/days
      targets: [__EMAIL_TARGET_ID__]
      interval: 1-24 //number of hours between reports
   }
}
```

Operations

set:

Access: Admin
Path: `config/email/report/__EMAIL_REPORT_ID__`

add:
Adds the report schedule to the system. Must adhere to the maximum supported.

Access: Admin
Path: `config/email/report`

delete:
Removes the report schedule from the system.

Access: Admin
Parameters: none
Path: `config/email/report/__EMAIL_REPORT_ID__`

6.1.8.6 email:

Object

```
{
  server : smtp.gmail.com
  port : 25
  sender : me@me.com
  username : rrosas@itwatchdogs.com
  passwordSet : true/false
  password : null
  sslEnabled : true/false //BB only
  target : {...}
  report : {...}
  status : {}
}
```

Operations

add:
Adds the target to the system. Must adhere to the maximum supported.

Access: Admin
Parameters:

```
data : {
  name : 111@me.com
}
```

6.1.8.6.1 email/target

Object

```
target : {
  __EMAIL_TARGET_ID__ : {
    name : 111@me.com
  },
  __EMAIL_TARGET_ID__ : ...
  ...
}
```

Operations

set:

Access: Admin
Parameters:

```
data : {
  name : 111@me.com
}
```

sendTest:
Sends a test email address to the targets. Returns a __JOB_ID__ to track the email operation.

Access: Admin
Parameters: None
Returns:

```
data : {
   id : __JOB__ID__
}
```

delete:
Removes the email target from the system.

Access: Admin
Parameters: None

6.1.8.6.2 email/status

Object

```
status : {
   __JOB__ID__ : {
    msg : "done, ok"
   },
   __JOB__ID__ : ...
   ...
}
```

Operations
None

6.1.8.7 snmp:

Object

```
{
  enabled : true/false
  port : 161
  readCommunity : "public"
  writeCommunity : "private"
  trapCommunity : "private"
```

```
        target : {...}
        user : {...}
    }
```

Operations

set:
  Modifies the snmp object.

  Access: Admin
  Parameters:

```
data : {
    enabled : true/false
    port : 161
    readCommunity : "public"
    writeCommunity : "private"
    trapCommunity : "private"
}

user : {
    __SNMP_USER_ID__ : {
        username: string
        privPasswordSet: true/false
        privPassword: null
        privType: none/des/aes
        authPasswordSet: true/false
        authPassword: null
        authType: none/md5/sha1
        type: read/write/trap*
    }
}
```

Operations

set:
  Modifies the snmp target object.

  Access: Admin
  Parameters:

```
data : {
    username: string
    privPassword: string
    privType: none/des/aes
    authPassword: string
    authType: none/md5/sha1
}
```

```
target : {
  __TRAP_TARGET_ID__ : {
    trapVersion : 1/2c/3
    name : 192.168.123.123
  },
  __TRAP_TARGET_ID__ : ...
  ...
}
```

Operations

set:
Modifies the address for a test trap.

Access: Admin
Parameters:

```
data : {
  name : 192.168.123.123
}
```

sendTest:
Sends a test trap to the targets.

Access: Admin
Parameters:

```
data : {}
```

Notes:
- *v1/v2c users do not support passwords (and are analogous to communities in legacy products).*
- *Users are used for v3 operations. The user type is set to read for user 0, write for user 1 and trap for user 2.*

6.1.8.8 http:

Object

```
{
  httpEnabled : true/false
  httpPort : 80
  httpsPort : 443
}
```

Operations

set:

Access: Admin

6.1.8.9 time:

Object

```
{
  mode : manual/ntp
  datetime : 2012-11-15 16:25:45
  zone : "africa/casablanca" //for Quetzals
  offset : -6:00              //for BB
  ntpSyncPeriod : 180         //for BB
  ntpServer1 : pool.0.ntp.org
  ntpServer2 : pool.1.ntp.org
}
```

Operations

set:

Access: Admin
Parameters:

```
data : {
  mode : manual/ntp
  datetime : 2012-11-15 16:25:45
  zone : "africa/casablanca" //for Quetzals
  offset : -6:00              //for BB
  ntpSyncPeriod : 180         //for BB
  ntpServer1 : pool.0.ntp.org
  ntpServer2 : pool.1.ntp.org
}
```

6.1.8.10 syslog:

Object

```
{
  enabled : true/false
  target : 192.168.123.123
  port : 512
}
```

Operations

set:

Access: Admin

Parameters:

```
data : {
  enabled : true/false
  target : 192.168.123.123
  port : 512
}
```

6.1.8.11ldap:

Object

```
{
  enabled: false
  host: host
  port: 389
  account:
  passwordSet: false
  password:
  baseDN:
  userFilter:
  userId:
  userIdNum:
  groupFilter:
  groupId:
  groupMemberUid:
}
```

Operations

set:

Access: Admin
Path: `config/ldap`

6.1.8.12locale:

Object

```
{
  defaultLang : en,
  units : metric/imperial
}
```

Operations

set:

Access: Admin

Parameters:

```
data : {
  defaultLang : en,
  units : metric/imperial
}
```

6.1.8.13camera:

Object

```
{
  __CAMERA_ID__ : {
    selection : __CAMERA_INDEX__
    url : 192.169.123.123
    username : bob,
    passwordSet : true/false,
    password : null,
    passwordEnc : 1234567 //Base 64 encoded
  }
  __CAMERA_ID__ : {...}
  ...
}
```

Operations

set:

Access: Control
Parameters:

```
data : {
    selection : __CAMERA_INDEX__
    url : 192.169.123.123
    username : bob
    password : bob
}
```

delete:
Removes the target camera from the system.

Access: Control
Parameters: None

add:
Adds the target camera to the system. Must adhere to the maximum
supported.

Access: Control
Parameters:

```
data : {
    selection : __CAMERA_INDEX__
    url : 192.169.123.123
    username : bob
    password : bob
}
```

6.1.9 /api/sys

6.1.9.1 Top Level

Object

```
{
  name : system name
  oem : platform
  platform : gmsm1
  label : System label
  state : {...}
  version : 1.1.1
  model : RCM
  modelNumber: 123
  partNumber: 123
  serialNumber": 123
  guestEnabled : true/false
  adminExists : true/false
  locale : {
    defaultLang : en,
    units : metric/imperial
  }
  contact : {
    description : someplace over the rainbow
    location : way up high
    contactEmail : dorothy@oz.com
    contactName : dorothy
    contactPhone : 5558675309
  }
  component : {...}
}
```

Operations

reset:

Access: Admin
Parameters:

```
{
    "target": "defaults"|"partialDefaults"|"logs"
}
```

reboot:
Reboot the system.

Access: Admin
Parameters: None

6.1.9.2 state:

Object

```
{
  *alarm : {
    *state: none/clear/acked/latched/tripped,
    *severity : ""/warning/alarm
  }
  warnCount : 1
  alarmCount : 2
  localTime: 2012-11-15 16:25:45
  systemTime : 123456789 [unix timestamp (UTC) seconds from
epoch]
  dirty : 35 [integer]
  uptime : 123456789 [seconds since last boot time]
  component : "ok" / "updating 1/2: gmsd 10%"
}
```

Operations
None

6.1.9.3 component:

Object

```
{
  __COMPONENT_ID__ : {
    *type : "boardTypeID"
    *version : "1.2.3"
    *sn : "123456789ABC"
    *state : "active"/"inactive"
  }
}
```

Operations
None

6.1.10 /api/auth (Users and User Authentication)

Object

```
{
  __USER_ID__ : {
    passwordSet : true/false,
    password : null,
    language: "en",
    enabled: true,
    control: true,
    admin: true,
    source: "local"|"ldap"
  }
  __USER_ID__ : {...}
  ...
}
```

Operations

get:

   Access: Enabled accounts

add:

   Access: Admin/Any if no admin exists
   Parameters:

```
{
  username : admin
  password : password,
  [language: en,]
  [enabled: true,]
  [control: false,]
  [admin: false,]
}
```

User object operations

get:

   Access: Enabled accounts

set:

Access: Admin for any field/Authenticated as target user for anything other than
permission changes.
Parameters:

```
{
  password : *****,
```

```
            [language: en,]
            [enabled: true,]
            [control: false,]
            [admin: false,]
        }
```

delete:

Removes the target user from the system. One admin level user must always exist. Guest account cannot be deleted.

Access: Admin
Parameters: None

login:

Access: Guest

Login Request (`/api/auth/__USER_ID__`)

```
        {
            token: "",
            cmd: "login",
            data: {
                password: "xxxxxxxx"
            }
        }
```

Login Response

```
        {
            retCode: 0,
            retMsg: "",
            data: {
                token: "abc345efd298e",
                control: true/false,
                admin: true/false,
                language: "eo"
            }
        }
```

logout:

Access: Authenticated as target user

Logout Request (`/api/auth/__USER_ID__`)

```
        {
            token: "abc345efd298e",
            cmd: "logout"
            data: {}
        }
```

Logout Response

```
{
  retCode: 0,
  retMsg: ""
}
```

6.1.11 /firmware

Note: No 'get' object

Operation

upload:
    Update device firmware.

    Access: Admin

    Requires query string with token on the URL, e.g. /firmware?token=...
    Input is a multipart/form-data with one named part called 'file'
    Output is a normal JSON response, with error code 0 or 7000-7999

6.2   Serial Interface

The R-Series PDUs provide an out-of-band, serial monitoring interface. The unit provides a RJ-45 port for RS-232 serial communication, providing support for Telnet and SSH via command line.

6.2.1   Setup

The following describes how to wire a cable for communicating with the serial port on a RC Series PDU.
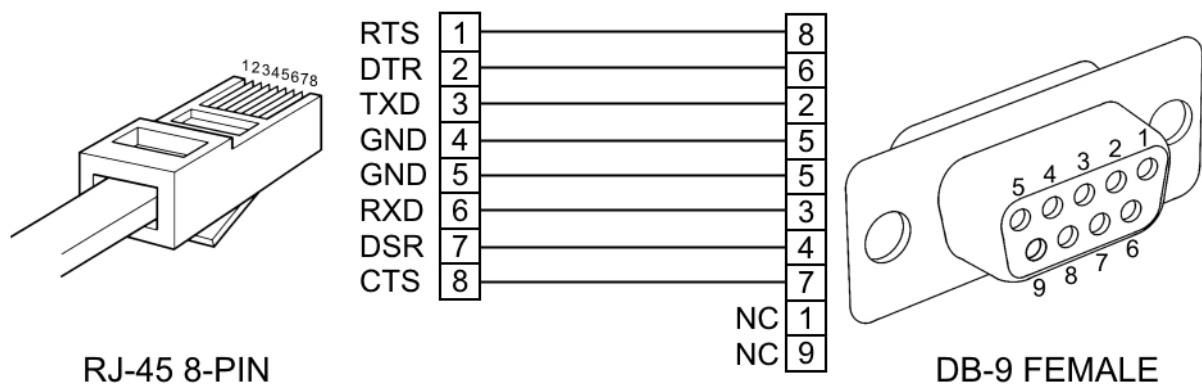
The following describes the parameters for serial communication with a R-Series PDU:

- Baud Rate: 9600

- Data Bits: 8
- Parity: N
- Stop Bits: 1
- Flow Control: None

6.2.2 Communication

Serial communication is the same as the Web API commands, but using the following syntax:

```
COMMAND (FILTERS) PATH = ARGUMENT
```

Command is the only required part. It is a single word from the following list: get, set, logout, add, delete, control, ack, sendTest, reset, and reboot.

Filters are offset from the rest of the message by parentheses and are separated from each other by spaces. This is only used with the "get"

command and is used to limit irrelevant information to the branches of the response tree that contain keys that match the filter.

Path is the location in the tree that you want to apply the Command. Starting at the root, each child key is separated by spaces.

Argument if present, is always preceded by an equal sign and is in JSON or YAML format. It is only used with the following Commands: set, add, control, and reset.

To see what the tree looks like, simply type in the following command:

```
get
```

The entire data tree is returned in YAML format. You will see some top-level keys like dev, alarm, sys, conf, etc.
To see the system configuration, you could type:

```
get conf
```

And, paying attention to the keys returned, go any number of levels deeper:

```
get conf network ethernet dhcpOn
```

To turn DHCP off you'll use an argument:

```
set conf network ethernet dhcpOn = false
```

"set" commands are special like "get" commands in that they can be applied at any level:

```
set conf network ethernet = {dhcpOn: true, ip4GW:
192.168.123.1}
```

Many commands require a device ID, a 16 character string, which can be obtained by calling:

```
get dev
```

Turn on outlet 1 with no delay (note outlets are 0-indexed)

```
control dev 0EC359E3851900C3 outlet 0 = {action: "on",
delay: "false"}
```

Turn off outlet 1 with no delay

```
control dev 0EC359E3851900C3 outlet 0 = {action: "off",
delay: "false"}
```

Note: *Be sure to use quotes in the parameter values.*

7   Technical Support

7.1   Resetting PDU

Should the PDU lose communication, the following reset/reboot buttons are available to help with troubleshooting:

1. **Network-Reset Button (○)**: Located under the Ethernet port, users will need to use a small pin or paper clip to contact this button. Holding the Network-Reset button for 5 seconds during normal operation will restore the default IP address and reset the user accounts.

2. **Hard-Reboot Button (↻)**: Pressing the Hard-Reboot button reboots the monitoring device. This acts as a power-cycle for the device, and does not change or remove any user information. *Note: This will NOT affect power to the connected devices*.

7.2   Service and Maintance

- No service or maintenance is required.
- There are no serviceable parts inside the PDU.
- **Do not attempt to open the PDU or the warranty will be void.**

7.3   More Technical Support

http://geistglobal.com
1 (800) 432-3219
1 (402) 474-3400
Email: support@geistglobal.com
or contact your distributor

7.4   Using Microsoft Exchange as an SMTP server

If your facility uses a Microsoft Exchange e-mail server, it can be used by the PDU to send Alarm and Warning notification e-mails if desired. However, the Exchange server may need to be configured to allow SMTP connections from the unit first, as later version of Exchange often have SMTP services or basic authentication disabled by default. If you encounter difficulties in getting your PDU to send e-mails through your Exchange server, the following notes may be helpful in resolving the problem.

Note: These suggestions only apply if you are using your own, physical Exchange server! Microsoft's hosted "Office365" service is not compatible with the PDU at this time, as Office365 requires a Start-TLS connection rather than a fully-encrypted connection, and the PDU does not currently support Start-TLS connections.

First, since the PDU cannot use IMAP or Microsoft's proprietary MAPI/RPC Exchange/Outlook protocols to send messages, you will need to enable SMTP by setting up an "SMTP Send Connector" in the Exchange server. More information on setting up an SMTP Send Connector in Exchange can be found at this Microsoft TechNet article: **http://technet.microsoft.com/en-us/library/aa997285.aspx**

Next, your Exchange server may also need to be configured to allow messages to be "relayed" from the monitoring unit. Typically, this will involve turning on the "***Reroute incoming SMTP mail***" option in the Exchange server's ***Routing*** properties, then adding the PDU's IP address as a domain which is permitted to relay mail through the Exchange server. More information about enabling and configuring SMTP relaying in Exchange can be found at this Microsoft TechNet article: **http://technet.microsoft.com/en-us/library/dd277329.aspx**

The SMTP "AUTH PLAIN" and "AUTH LOGIN" authentication methods (also known as "Basic Authentication) for logging in to the server are often no longer enabled by default in Exchange; only Microsoft's proprietary NTLM authentication method is enabled. The AUTH LOGIN method which the PDU requires can be re-enabled as follows:
1. In the Exchange console under ***server configuration***, select ***hub transport***.
2. Right-click the client server, and select ***properties***.
3. Select the ***authentication*** tab.
4. Check the ***Basic Authentication*** checkbox.
5. Uncheck the ***Offer Basic only after TLS*** checkbox
6. Apply or save these changes, and exit. Note that you may need to restart the Exchange service after making these changes.

Finally, once you have enabled SMTP, relaying, and the AUTH LOGIN Basic Authentication method, you may also need to create a user account specifically for the PDU to log into. If you have already created an account prior to enabling the SMTP Send Connector, or you are trying to use an already-existing account created for another user, and the PDU still cannot seem to connect to the Exchange server, the account probably did not properly inherit the new permissions when you enabled them as above. (This tends to happen more often on Exchange servers that have been upgraded since the account(s) you are trying to use were first created, but can sometimes happen with accounts when new connectors and plug-ins are added regardless of the Exchange version.) Delete the user account, then create a new one for the monitoring unit to use, and the new account should inherit the SMTP authentication and mail-relaying permissions correctly.

If none of the above suggestions succeed in allowing your Geist PDU to send mail through your Exchange server, then you may need to contact Microsoft's technical support for further assistance in configuring your Exchange server to allow SMTP e-mails to be sent from a 3rd-party, non-Windows device through your network.