
Siemon Power Distribution Unit
Instruction Manual

7M, 7N, 7S, 7T and 7W Series

Firmware Version 4.x

Table of Contents

Specifications	4
Overview	4
Environmental	4
Temperature	4
Humidity	4
Elevation	4
Electrical	4
Receptacle Ratings	4
Networking	5
Ethernet Link Speed	5
Protocols	5
User Interfaces	5
EMC Verification	5
Installation	6
Guidelines	6
Mounting	7
Full Length Brackets	7
Toolless Mounting Hardware	7
Flush Mount Brackets	8
Adjustable Mount Brackets	8
19" Horizontal/Panel Mount Brackets	9
Hardware	10
Interface	10
Network Setup	10
Windows	11
Mac	13
Serial Communication	14
Setup	15
Communication	15
Web Interface	18
Sensors	18
Overview	18

Alarms & Warnings.....	23
Logging	27
System.....	29
User Accounts.....	29
Network.....	30
Email.....	31
Reports.....	33
LDAP.....	33
LCD Display.....	34
Time.....	35
SNMP.....	35
Syslog.....	36
Admin.....	37
Locale.....	37
Restore Defaults.....	37
Firmware Update.....	38
Help.....	38
Info.....	38
Support Site.....	38
Technical Support.....	38
Resetting PDU.....	38
Service and Maintenance.....	39
More Technical Support.....	39
Using Microsoft Exchange as an SMTP server.....	39

Specifications

Overview

The Intelligent PDUs 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. Intelligent PDUs support optional external sensors. These units can be built for installation in single-phase, three-phase Delta or Wye building wiring configurations. There are four families; Monitored, Smart, Switched & Managed

	Input Power Monitoring	Outlet Level Power Monitoring	Outlet Level Switching
Monitored	●		
Smart	●	●	
Switched	●		●
Managed	●	●	●

Environmental

Temperature

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

Humidity

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

Elevation

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

Electrical

See nameplate for unit ratings.

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

Type	Ratings
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)

Networking

Ethernet Link Speed

10/100 Mbit; full-duplex

Protocols

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

User Interfaces

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

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, and (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.

Installation

Guidelines

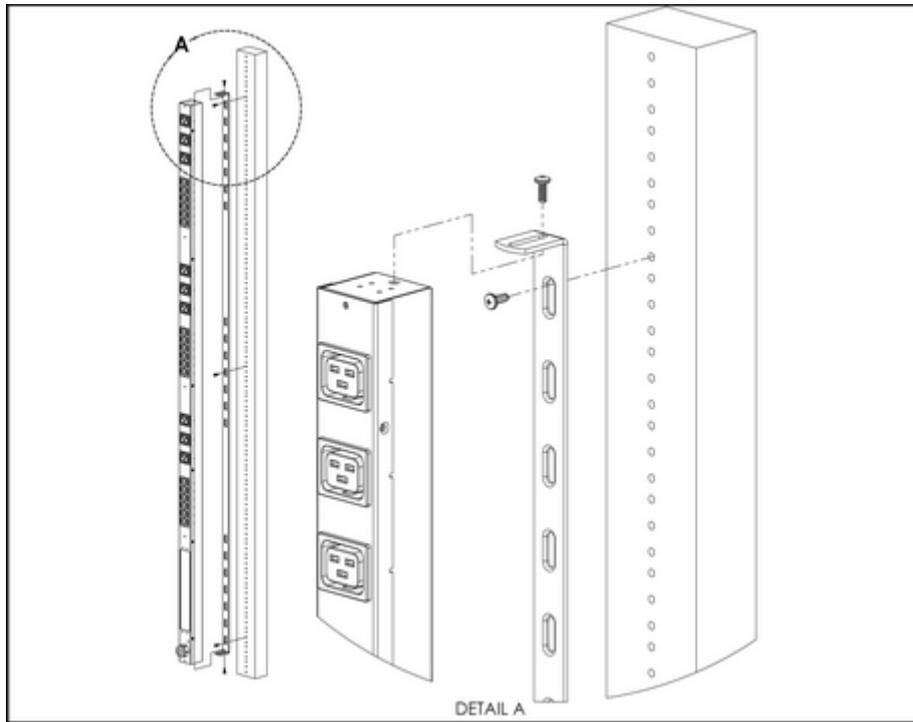
- The ambient temperature of the rack should be no greater than 45°C.
- Install the PDU such that the amount of airflow required for safe operation of equipment is not compromised.
- Mount the PDU so that a hazardous condition is not achieved due to uneven mechanical loading.
- Follow nameplate ratings 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 earthing 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 socket 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.

Installation

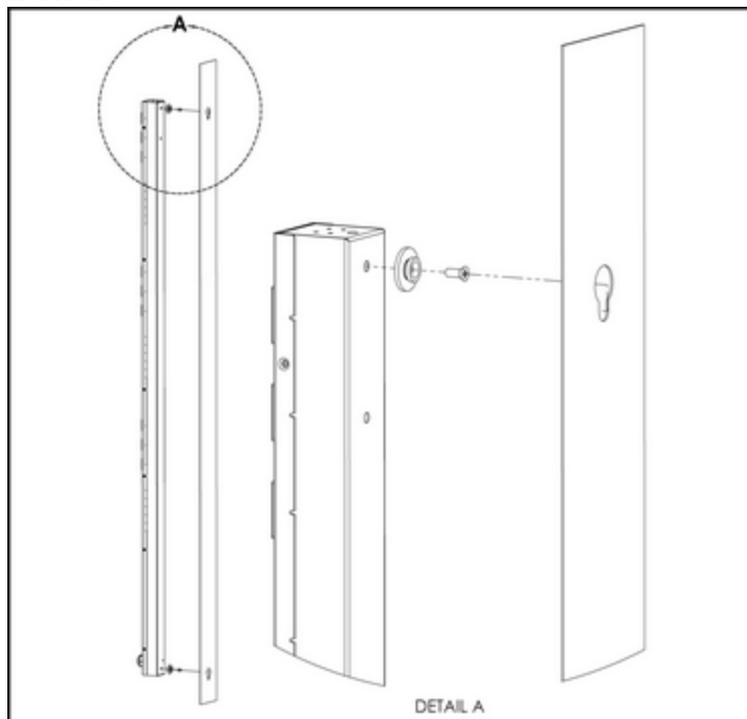
1. Using appropriate hardware, mount unit to rack. (See next section for examples.)
2. Plug PDU into an appropriately-rated and protected branch-circuit receptacle.
3. Plug in the devices to be powered by the PDU.
4. Turn on each device connected to the PDU. Sequential power-up is recommended to avoid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

Mounting

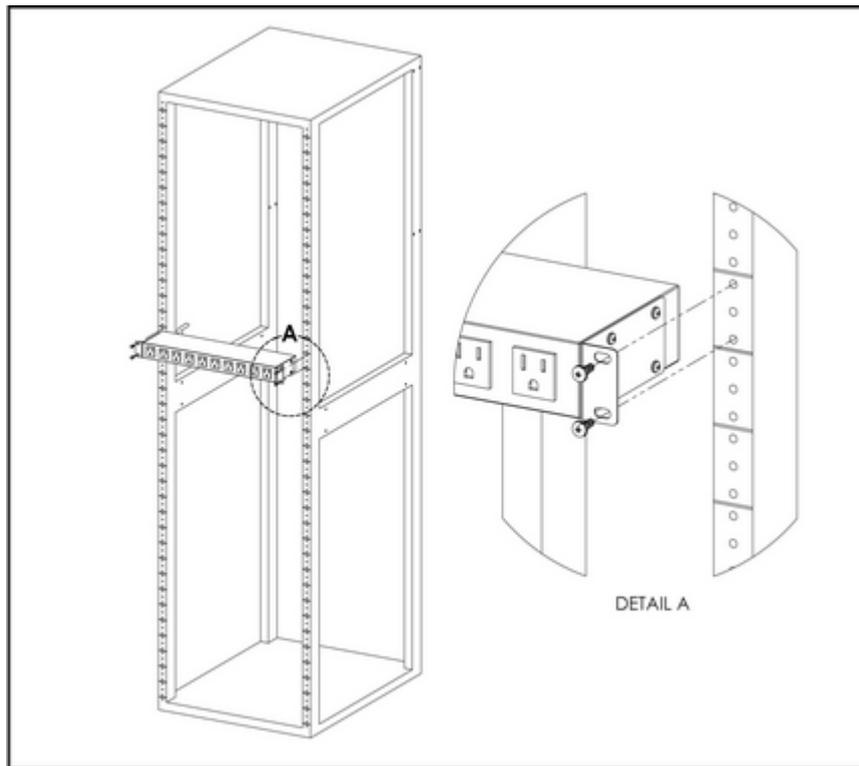
Full Length Brackets



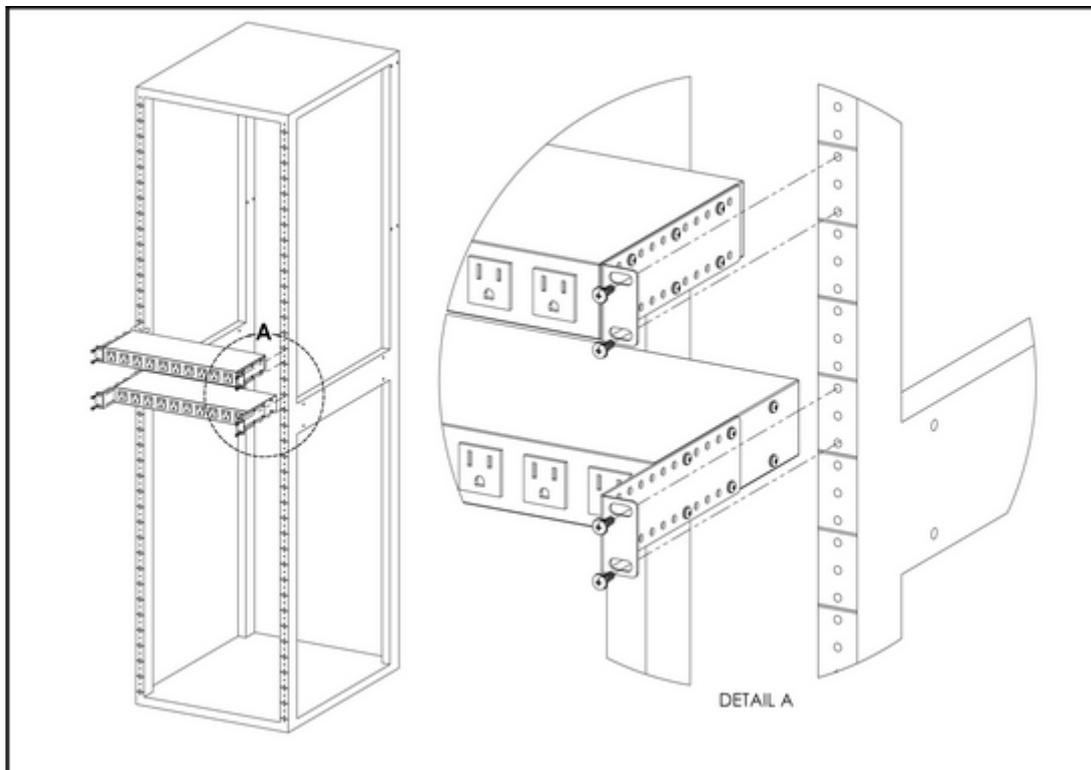
Toolless Mounting Hardware



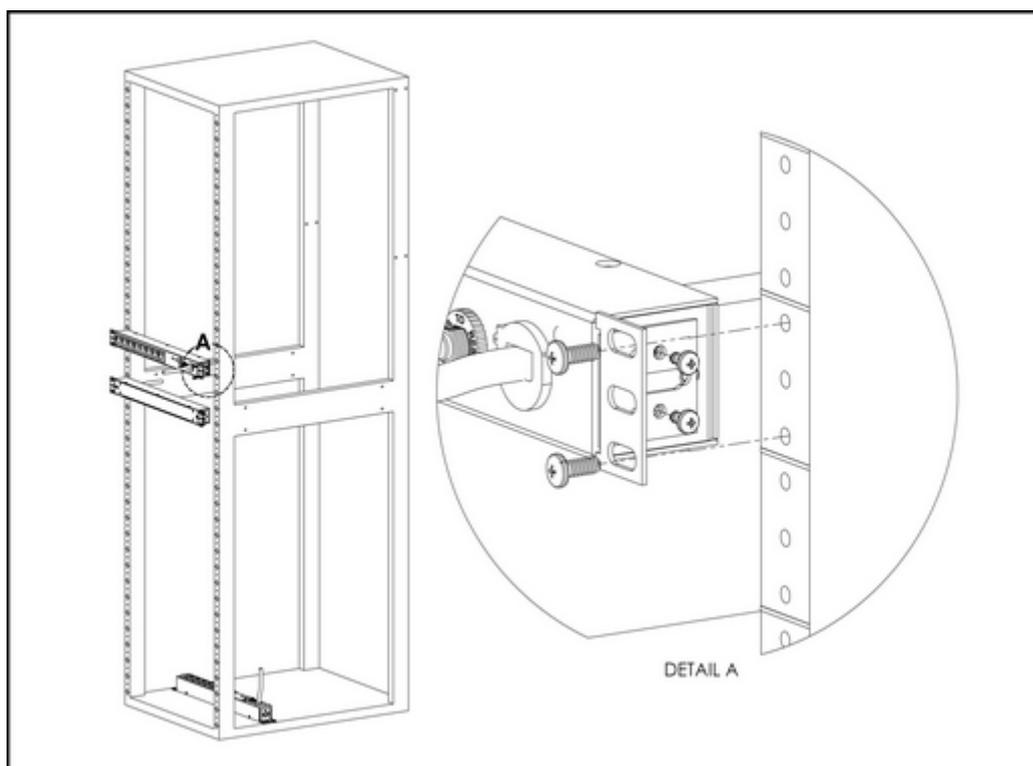
Flush Mount Brackets



Adjustable Mount Brackets



19" Horizontal/Panel Mount Brackets



Hardware

Interface

Intelligent 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 Siemon 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. Intelligent PDUs support up to sixteen sensors.
2. **Serial Communication Port** (📡): Intelligent 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. **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** (🔄): 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. **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 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.

Network Setup

Siemon Intelligent 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. 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).

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**.

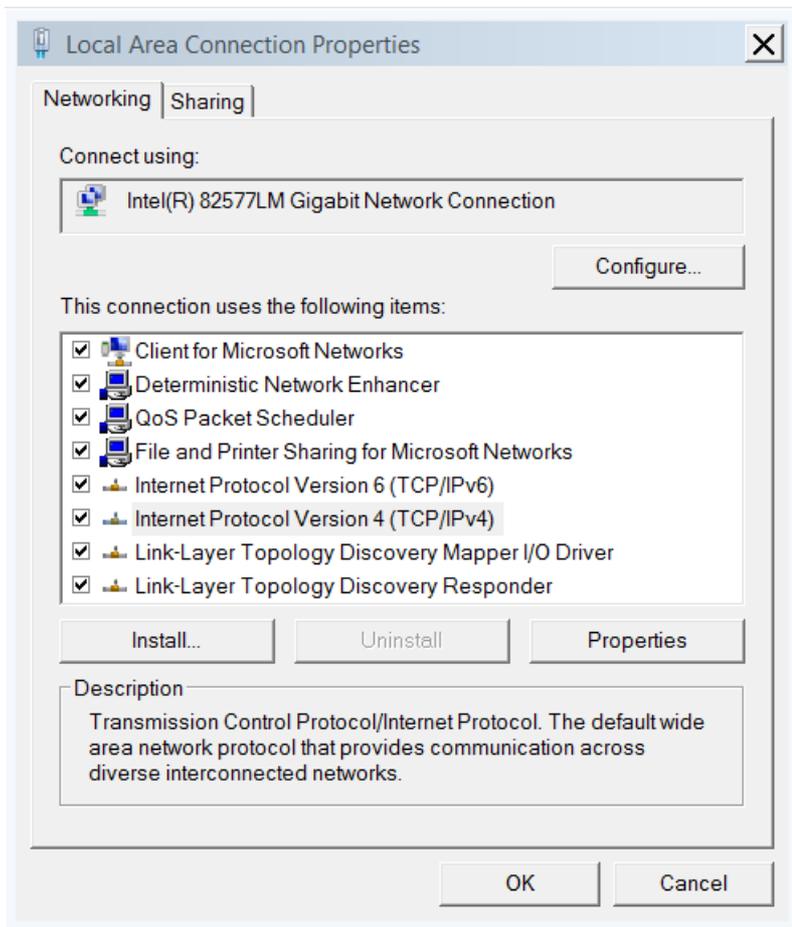
(Alternatively, on some Windows 7 machines, this may be **Start**, then **Settings >> Control Panel >> Network and Sharing Center >> Change Adapter Settings**.)

- **Windows 8 / Server 2012:**

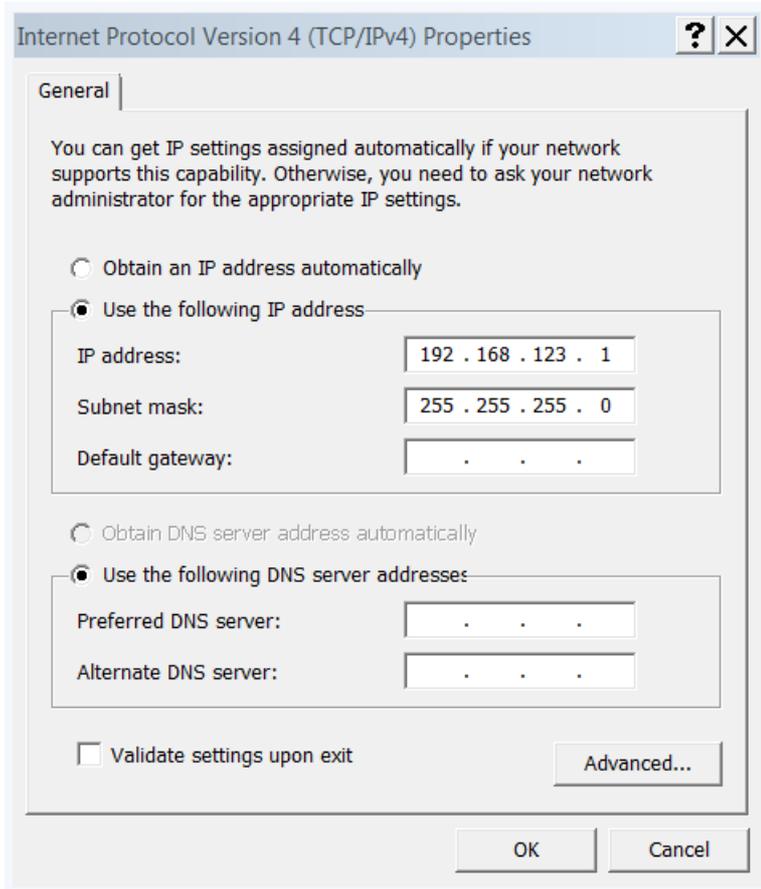
Move the mouse cursor to the bottom or top right corner of the screen, click the **Settings** icon, then select **Control Panel**. Change the view type from **Category** to **Large** or **Small Icons** if necessary, then select **Network and Sharing Center**, then **Change Adapter Settings**.

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.

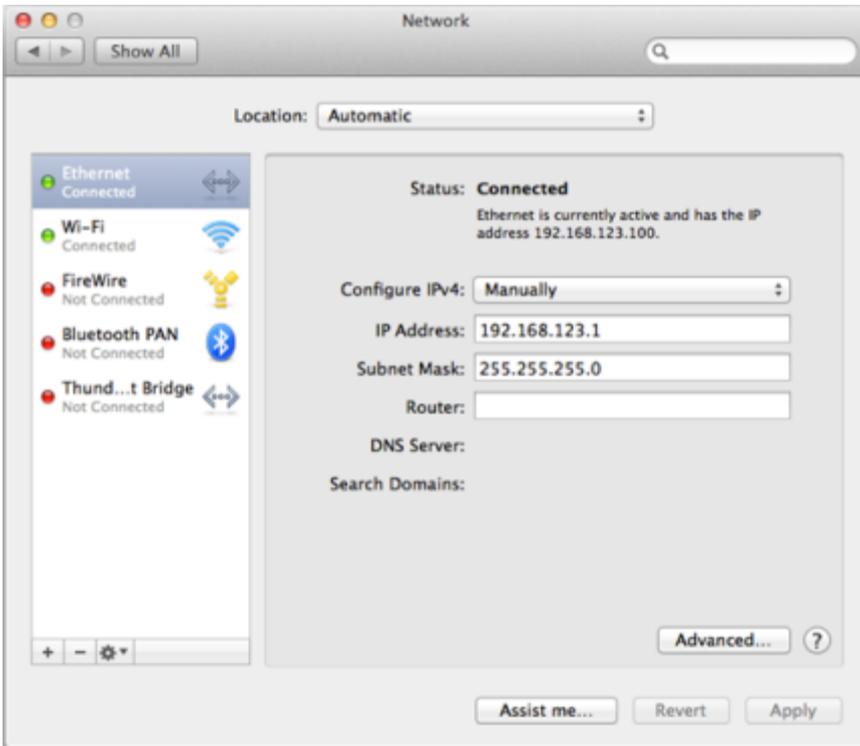
Once the NIC settings are configured properly, you should be able to access the unit by typing "http://192.168.123.123" into the address bar of your web browser. If you are setting up the unit for the first time, or if the unit has been reset back to factory defaults via the network-reset button, the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

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.

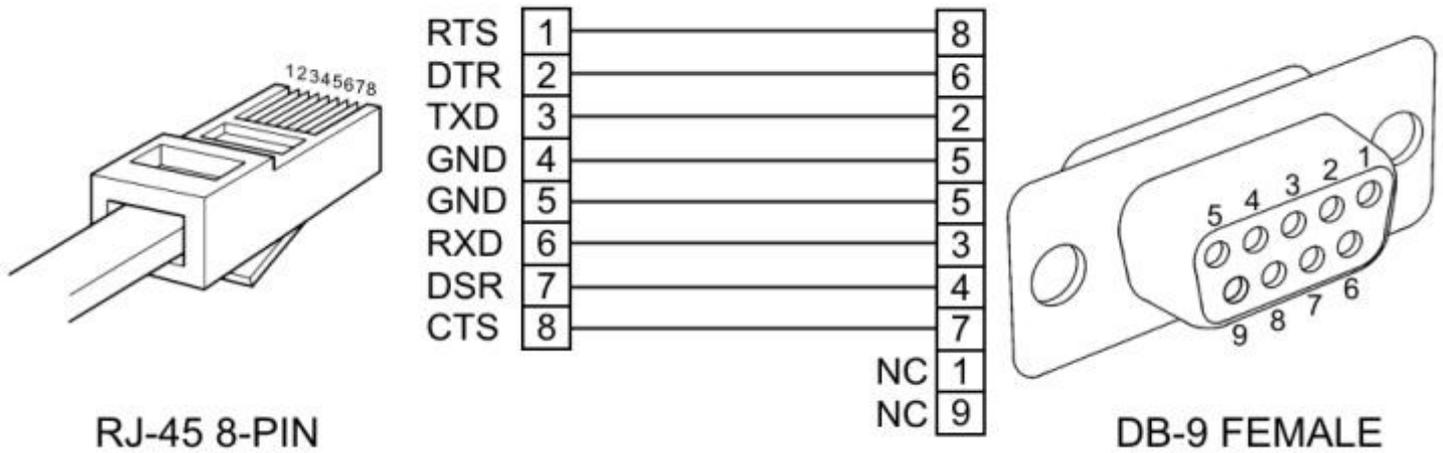
Note: Changes to settings will take effect instantly when the **Save** button is clicked, so the browser will no longer be able to reload the web page from the default/previous address. Once you have finished configuring the unit's IP address, simply repeat the steps above, and change the computer's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

Serial Communication

The Intelligent 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.

Setup

The following describes how to wire a cable for communicating with the serial port on an intelligent PDU.



The following describes the parameters for serial communication with an intelligent PDU:

- Baud Rate: 9600
- Data Bits: 8
- Parity: N
- Stop Bits: 1
- Flow Control: None

Communication

Serial communication is done with commands 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.

- **get** - 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.
- **set** - 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. Set operations 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.

The rest of the Commands are considered special commands and 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, and can only be called by users with correct permissions.

- **logout**
- **add**
- **delete**
- **control**
- **ack**
- **sendTest**
- **reset**
- **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.*

Web Interface

Siemon Intelligent 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.

Sensors

Overview

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



- 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	Sensors			Help
Overview	User	LCD Display	Locale	Info
Alarms & Warnings	Network	Time	Restore Defaults	Support Site

Camera	Email	SNMP	Firmware Update	
Logging	Report	Syslog		
	LDAP	Admin		

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.



Configuration Icon



Operation Icon

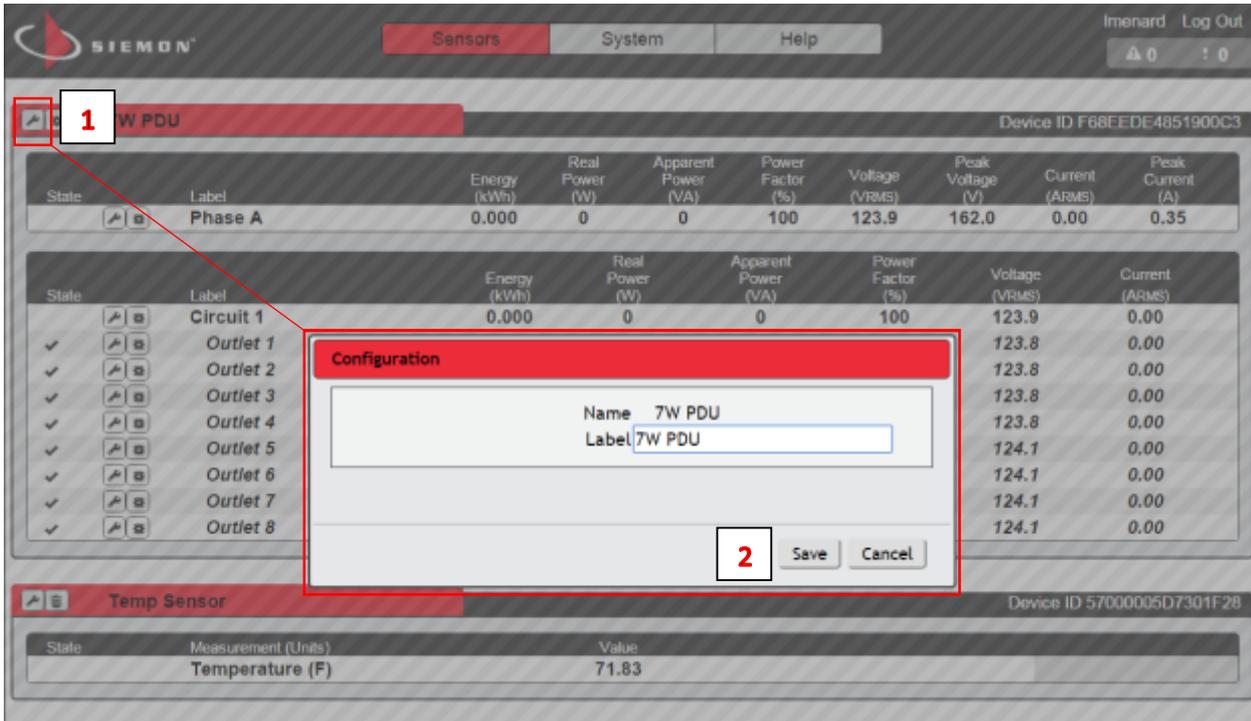
Configuration and Operation

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

Device, Phase and Circuit Configuration:

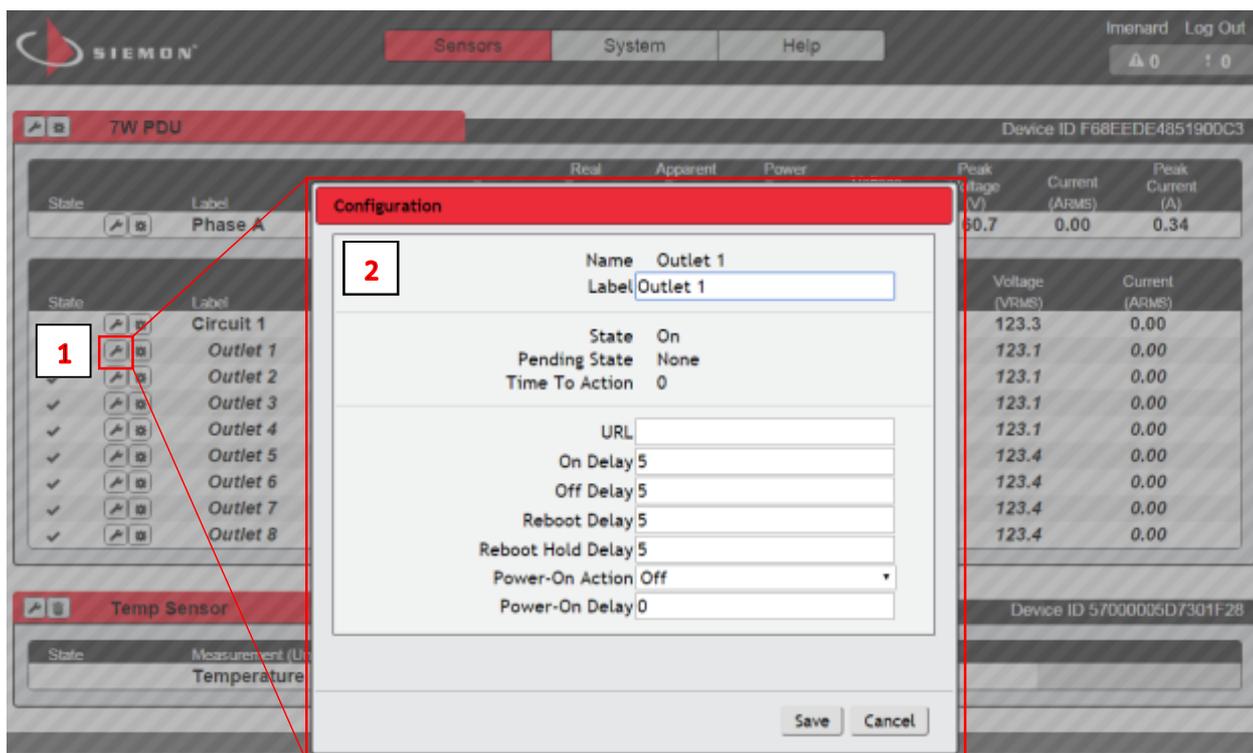
1. Click the desired Configuration icon to change the device's **Label**. (**Name** is the PDU's factory name or model, and cannot be changed.)

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:

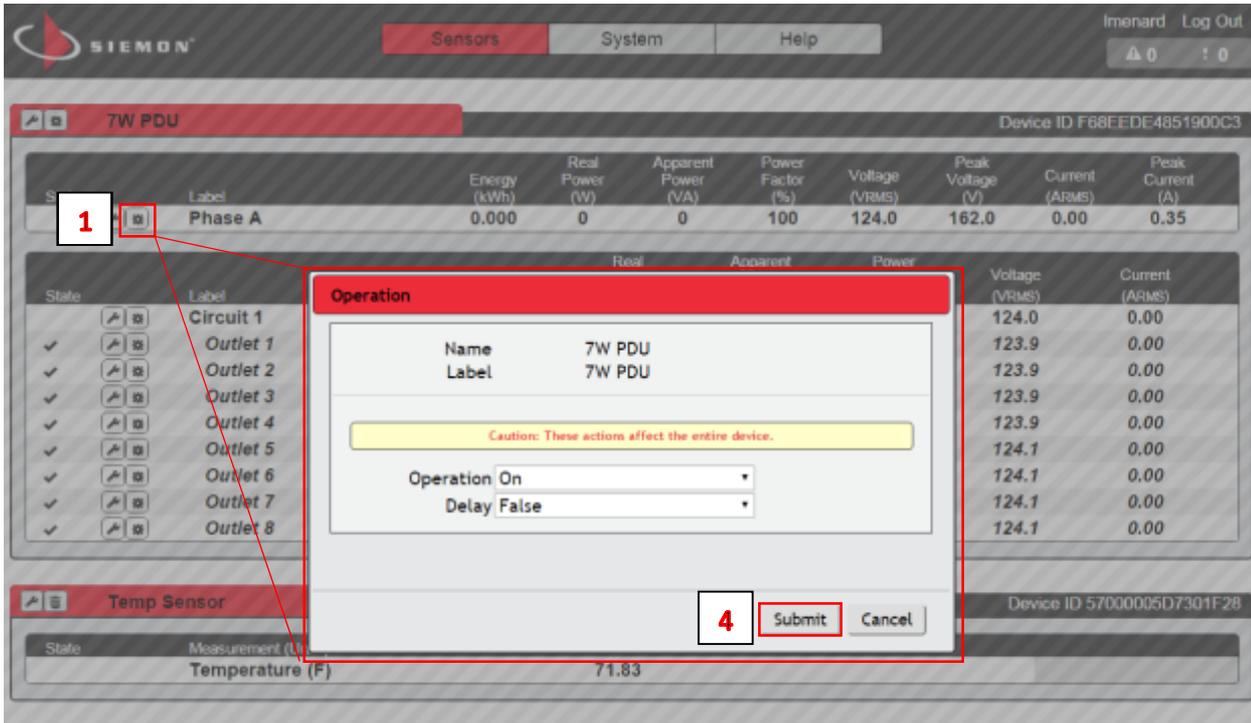
- **State** describes the outlet's current state (On/Off).
- **Pending State** describes the state the outlet is currently transitioning to, if it is in the process of switching.

- **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.

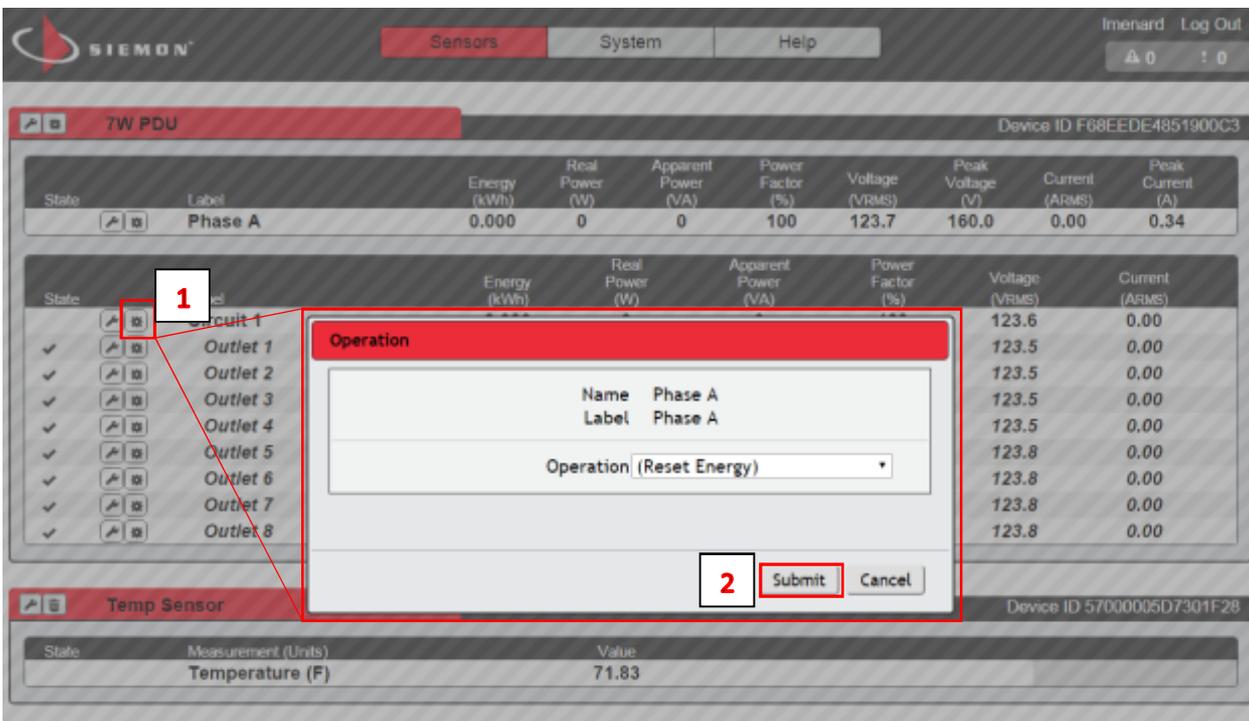
4. Select **Submit** to issue the action.



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.

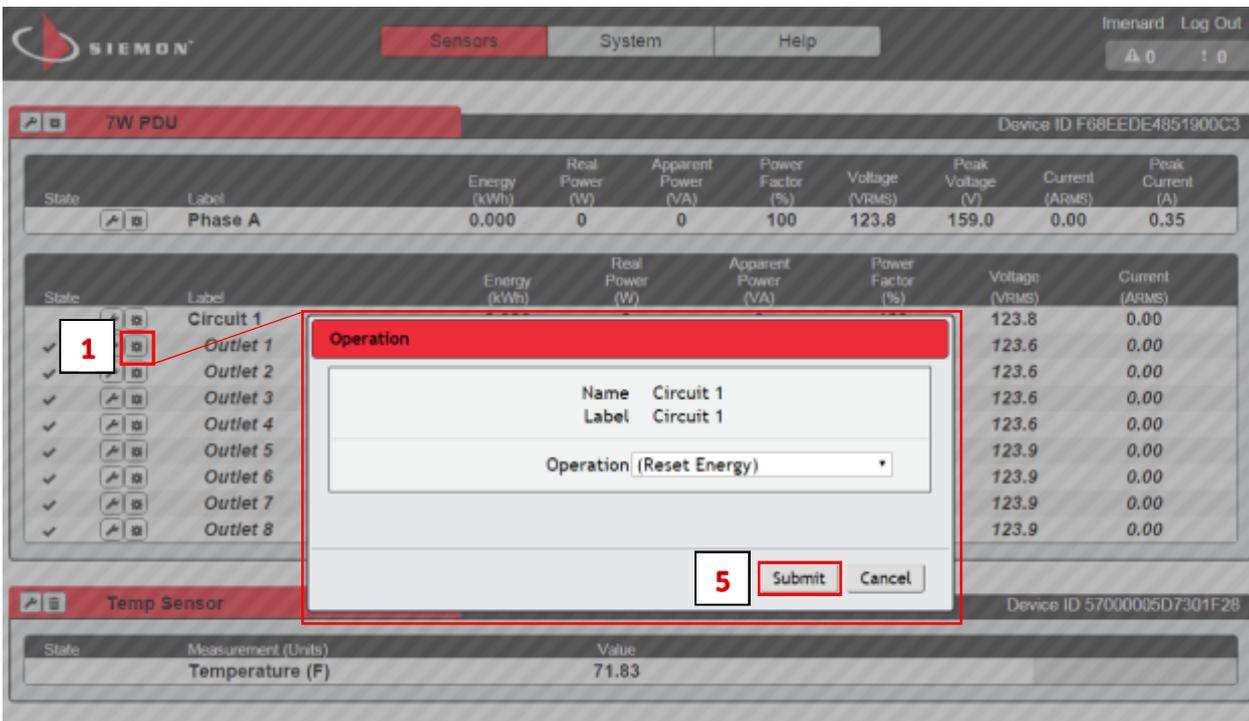
Phase/Circuit Operation:

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.

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.

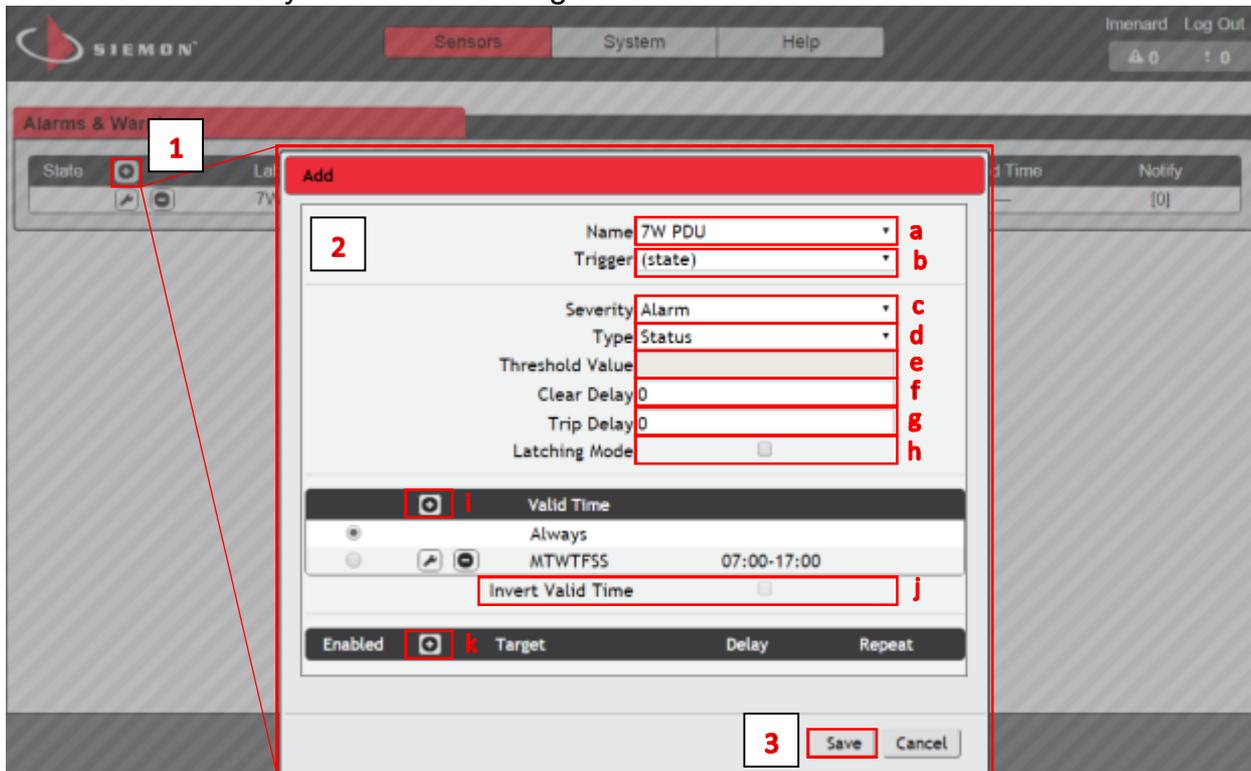
Alarms & Warnings									
State			Label	Trigger	Severity	Type	Value	Valid Time	Notify
1	2	3	4	7W PDU	—	Alarm	Status	—	[0]

- 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.)
- Configuration:** Add/Delete/Modify Alarms & Warnings.
 - ⊕ : Add new Alarms & Warnings.
 - 🔧 : Modify existing Alarms & Warnings.
 - ⊖ : Delete Existing Alarms & Warnings.
- 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.)
- The actual conditions for the various Alarms & Warnings settings are shown here.

Alarms & Warnings Configuration

To add a new Alarm or Warning Event:

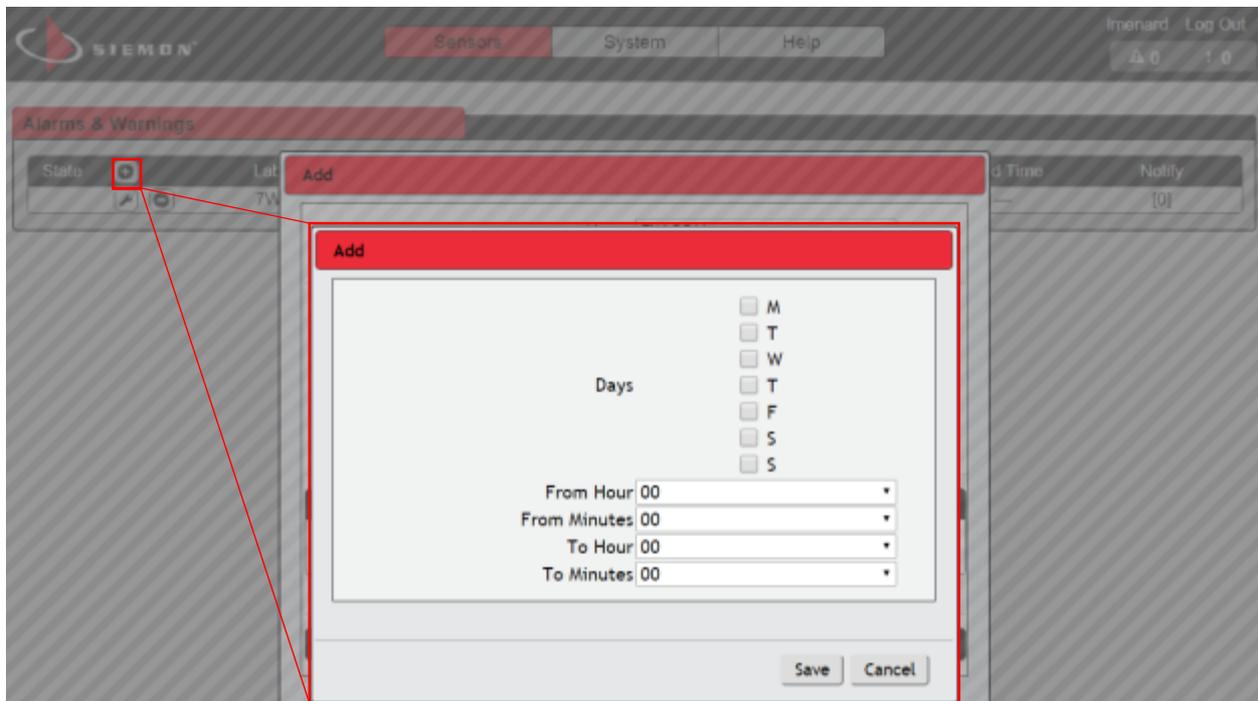
1. Click the Add/Modify Alarms & Warnings button:



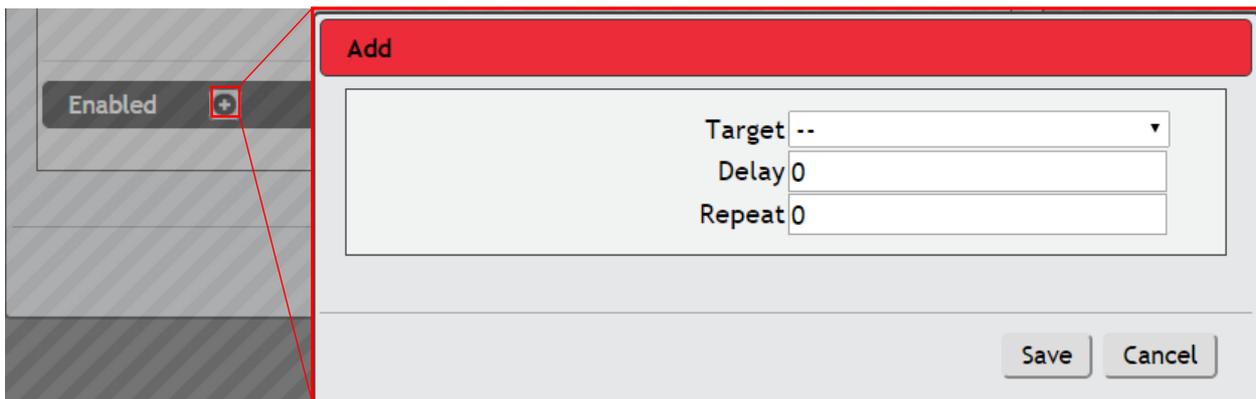
2. Set the desired conditions for this Event as follows:

- 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:



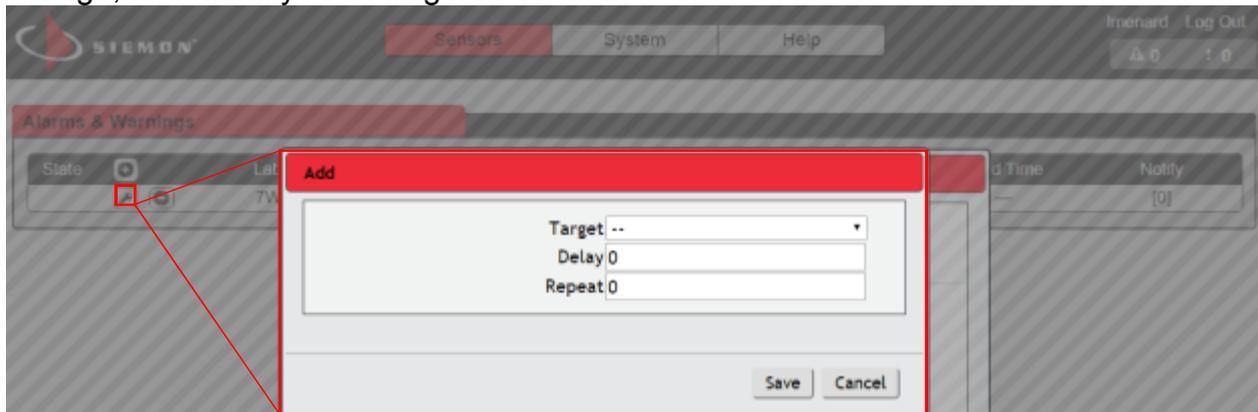
- **Target** is the e-mail address or SNMP manager to which notifications should be sent when the Event is tripped. Other options, such as "buzzer", may be available depending on your Intelligent PDU.
- **Delay** determines how long this Event must remain tripped before this Action's first notification is sent. (Note that this is different from the *Trip Delay*, above; *Trip Delay* determines how long the threshold value has to be exceeded before 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

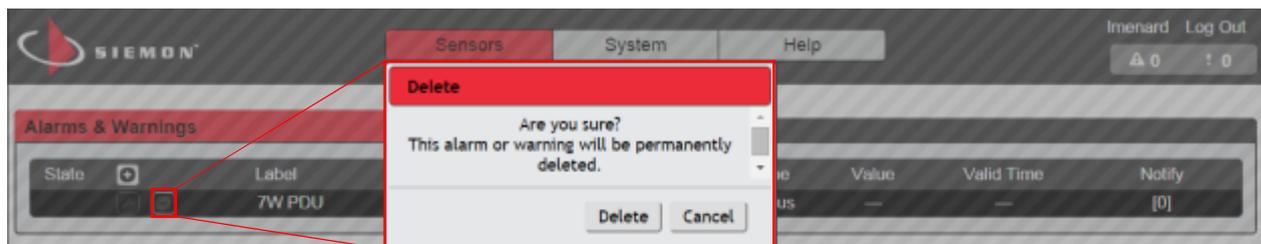
associated with it.

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.

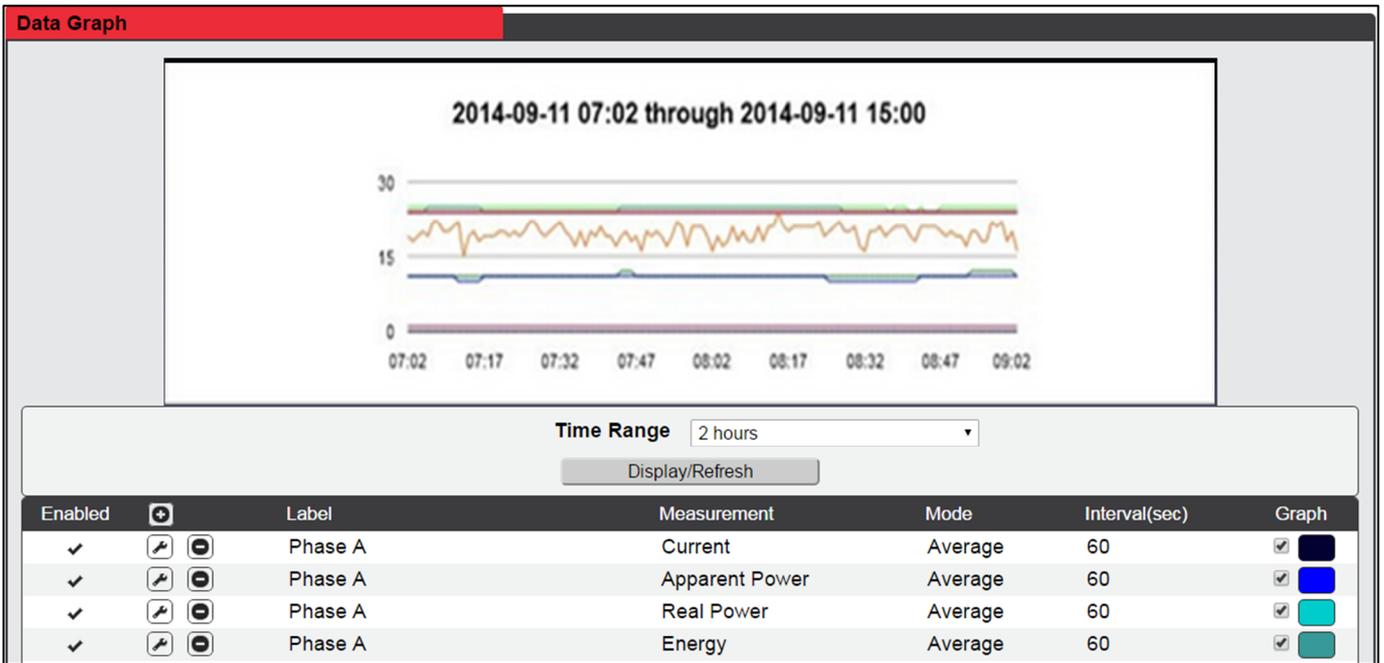
To delete an existing Alarm or Warning Event:

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

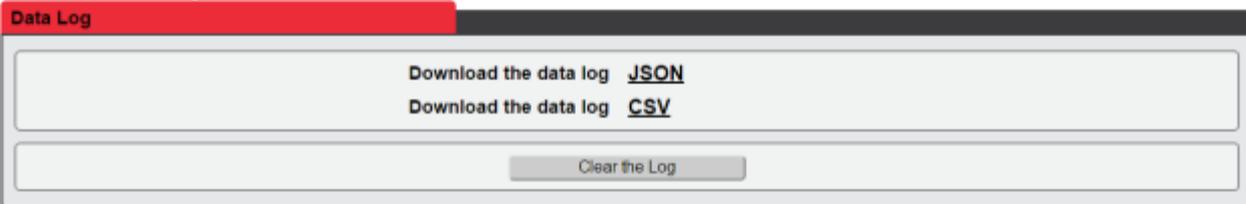
Logging

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.



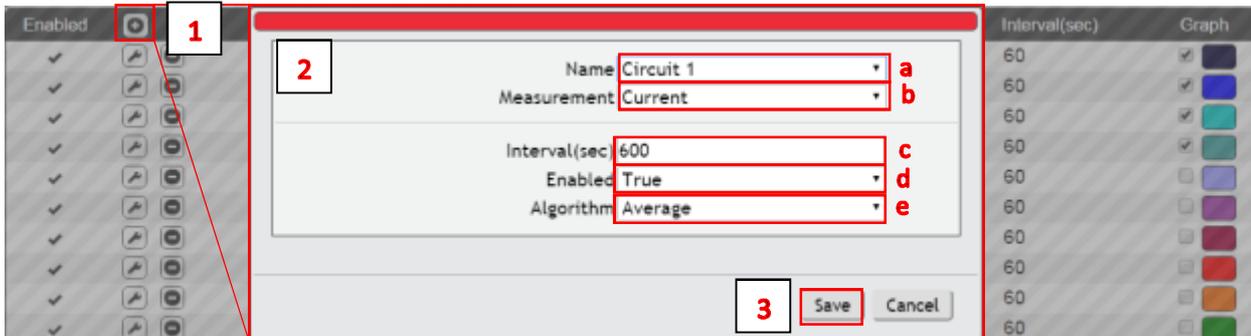
Recorded data is available for download in CSV and JSON file formats. To reset the logs click the "Clear the Log" button.



Logging Configuration

To add a new Measurement for logging:

1. Click the Add Measurement button:



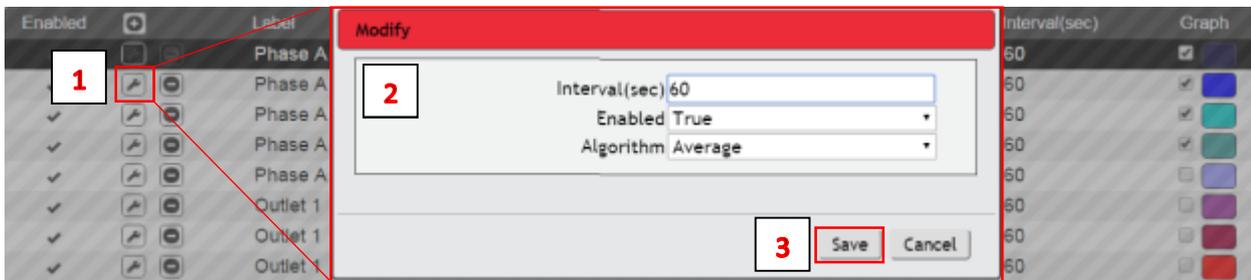
2. Set the desired conditions for this Measurement as follows:

- Select the **Name** of the phase or circuit you wish to measure.
- Select the **Measurement** (current, voltage, etc.) you want to record.
- Set the **Interval**, in seconds, for this Measurement.
- Enable/Disable** the Measurement.
- 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:

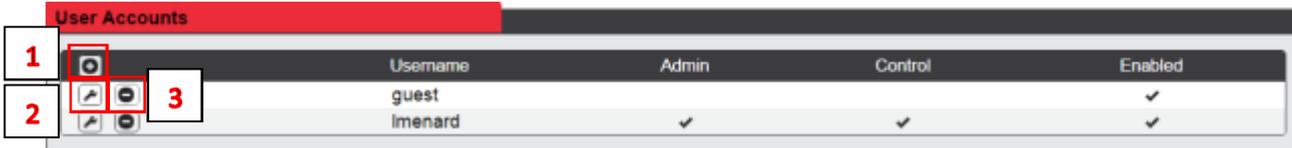


2. Set the desired conditions for this Measurement as follows:
 - a. Set the **Interval**, in seconds, for this Measurement.
 - b. **Enable/Disable** the Measurement.
 - c. Choose the **Algorithm** the device will use to record. Options are High, Low or Average.
3. Click **Save**.

System

User Accounts

The **User Accounts** page allows you to manage or restrict access to the unit's features by creating accounts for different users.

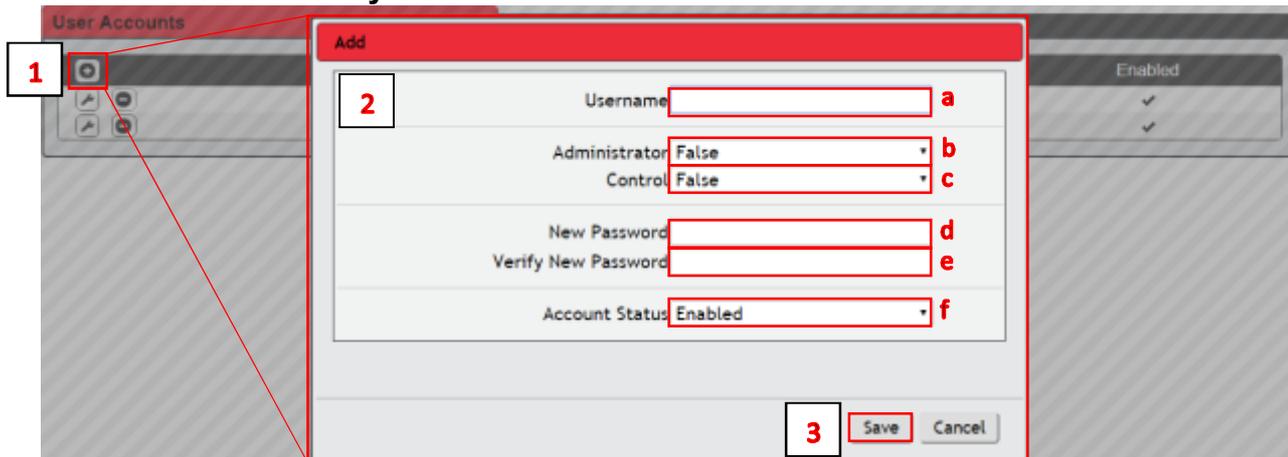


There are three buttons available on the User Accounts page:

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.



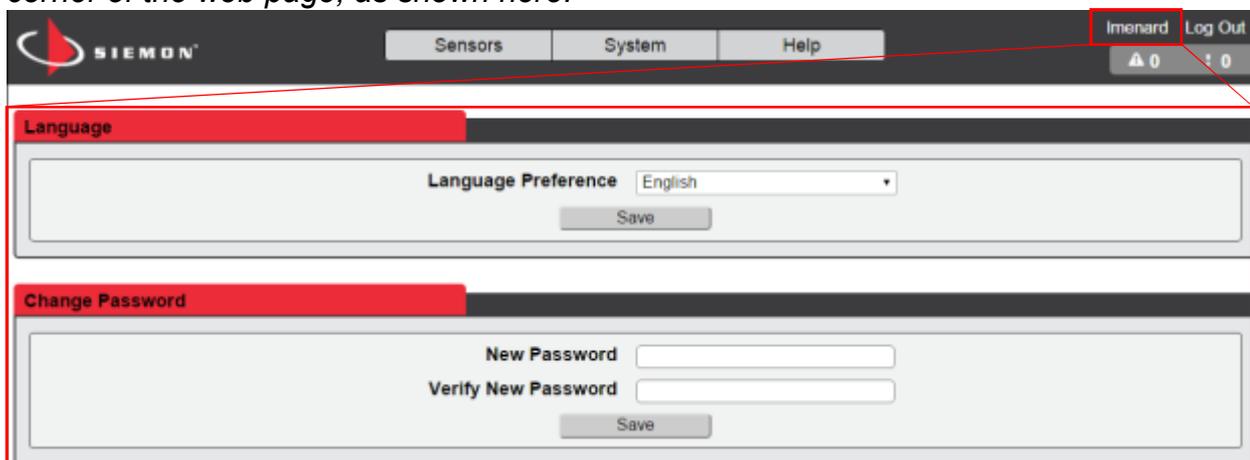
2. Create or modify the account information as follows:
 - a. **Username**: the name of this account. User names may be up to 24 characters long, are case-sensitive, and may not contain spaces or any of these prohibited characters: \$&`<>[] { }"+%@/ ; =?^\|~', Note that an account's username cannot be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



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:

- **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.

IP Address	Prefix (Netmask)
172.17.6.32	/ 24 (255.255.255.0)
172.17.10.1	/ 16 (255.255.0.0)
fe80::219:85ff:fee4:ed8e	/ 64

DNS Server Address: 172.17.1.10

- **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.

HTTPS is always enabled.

HTTP Interface: Enabled

HTTP Port: 80

HTTPS Port: 443

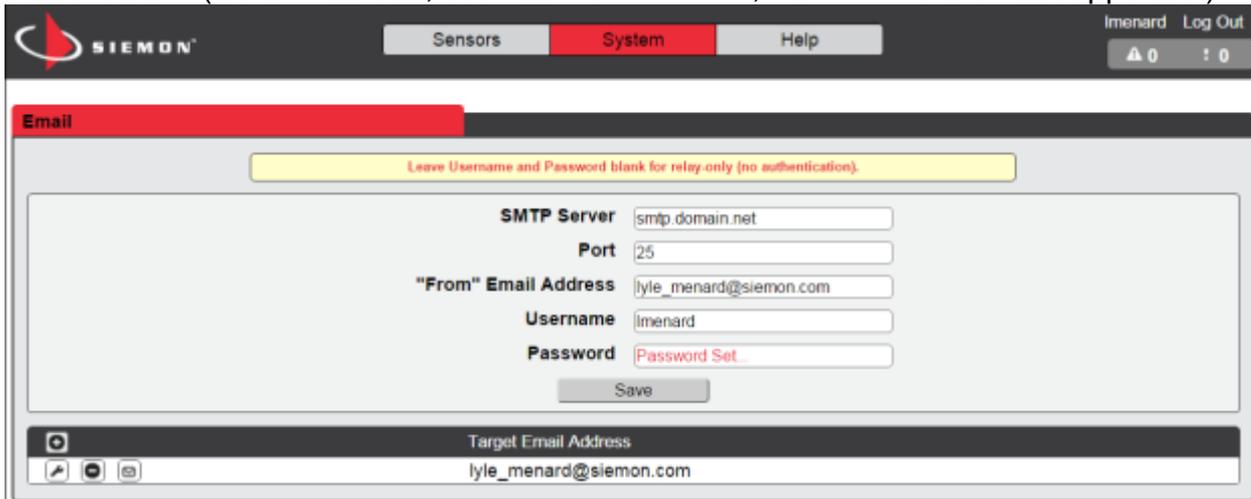
Email

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.)

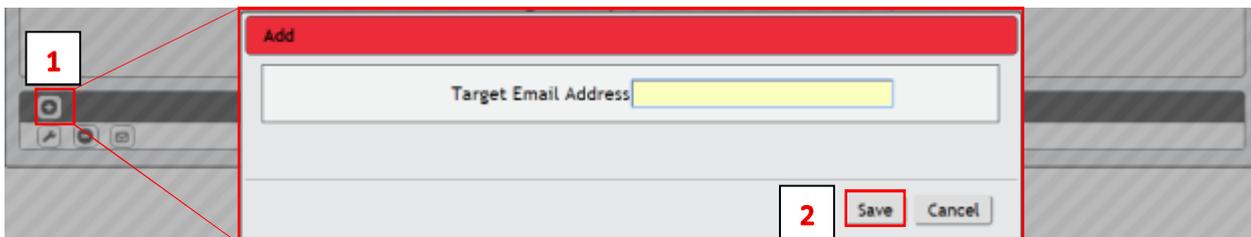


Target e-mail addresses can be configured as follows:



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.

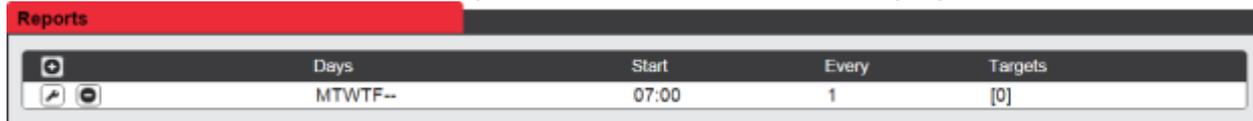
To send a test e-mail:

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.

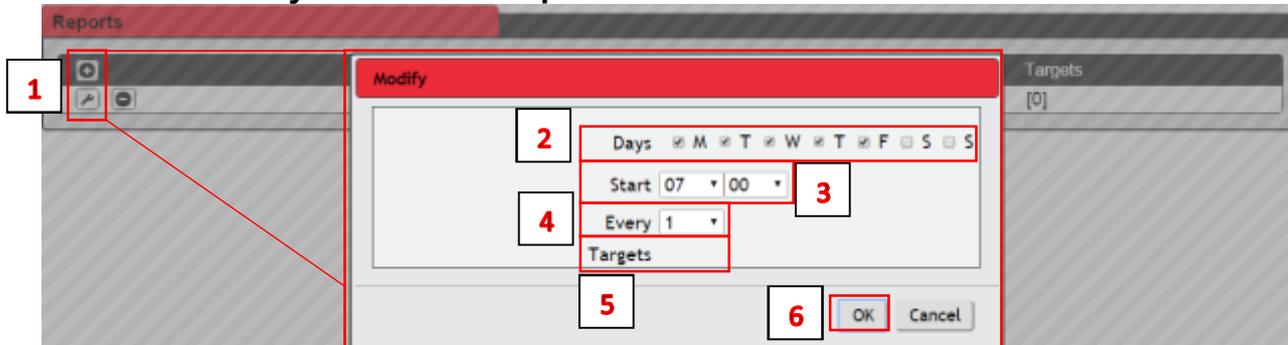
Reports

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.



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

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

Enable	Disabled
LDAP URI	ldap://host
Bind DN	
Bind Password	No Password...
Base DN	
User Filter	(objectClass=posixAccount)
"uid" Mapping	uid
"uidNumber" Mapping	uidNumber
Group Filter	(objectClass=posixGroup)
"gid" Mapping	gidNumber
"memberUid" Mapping	memberUid

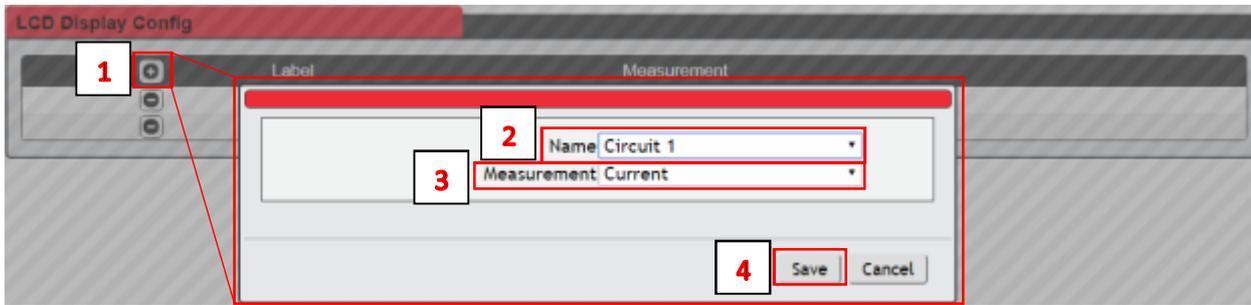
LCD Display

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

	Label	Measurement
<input type="checkbox"/>	Temp Sensor	Temperature
<input type="checkbox"/>	Circuit 1	Voltage

To Add/Modify Measurements:

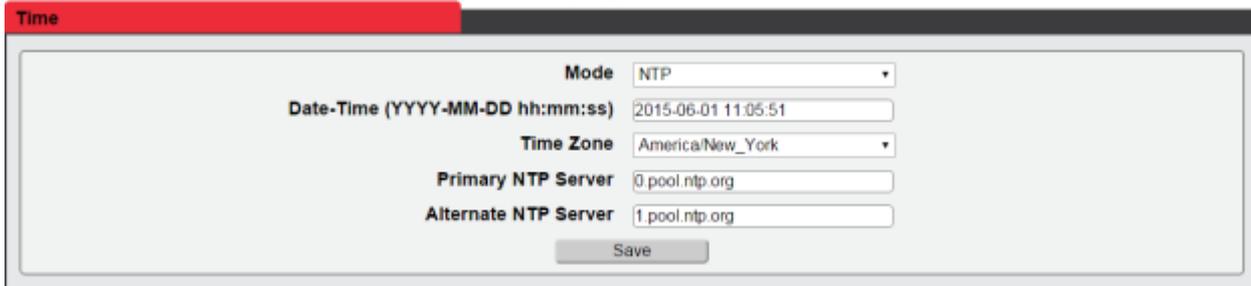
1. Click the Add/Modify button:



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.

Time

The unit's time and date are set on this page.

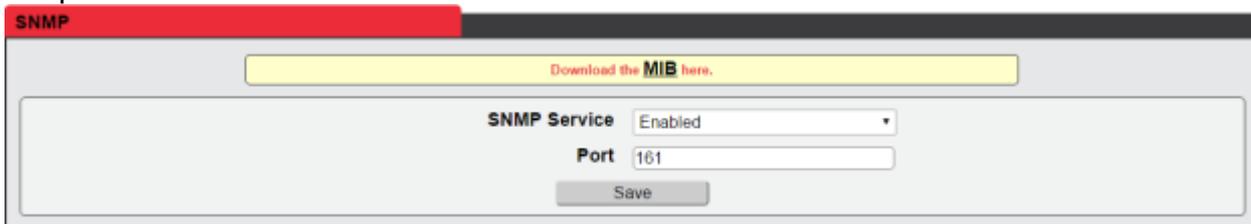


There are two mode available: **Network Time Protocol (NTP)** and **Manual**.

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.

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.

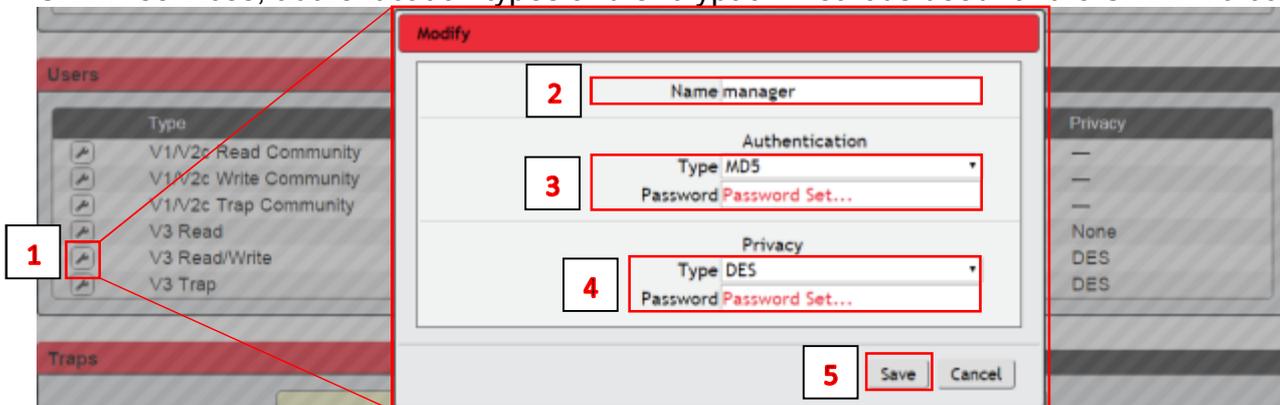


The **SNMP Service** can be enabled or disabled. The service will listen for data-read requests (a.k.a. "Get requests") on **Port** 161, which is the usual default for SNMP services; this can also be changed if desired.

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.

Type	Name	Authentication	Privacy
V1/V2c Read Community	public	—	—
V1/V2c Write Community	private	—	—
V1/V2c Trap Community	private	—	—
V3 Read	initial	None	None
V3 Read/Write	manager	MD5	DES
V3 Trap	trap	MD5	DES

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.

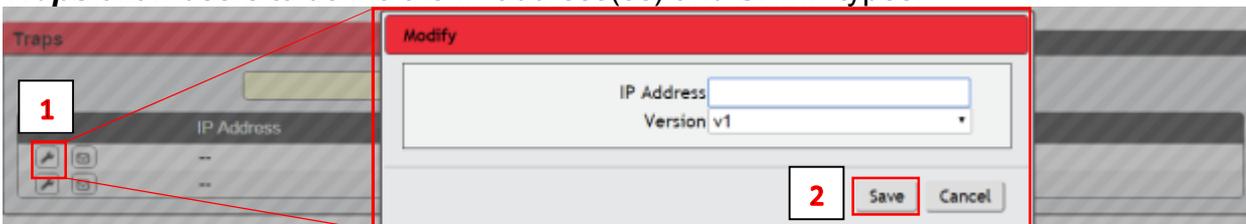


To configure:

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.

IP Address	Version
--	1
--	1

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.

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.

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.

Locale

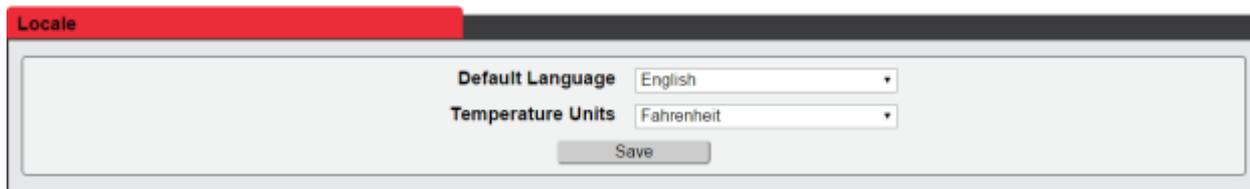
The Locale page sets the default Language and Temperature Units for the device. These settings will become the default viewing options for the device, although individual users can change these options for their own accounts. (The Guest account will only be able to view the device with the options set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

Restore Defaults

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

All Settings: Erases all 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.

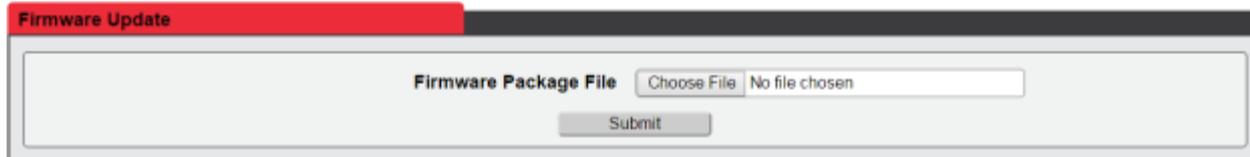
All Non-Network Settings: Erases all settings except the Network and User Accounts.



Firmware Update

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

<http://www.siemon.com/ipdu/updates>

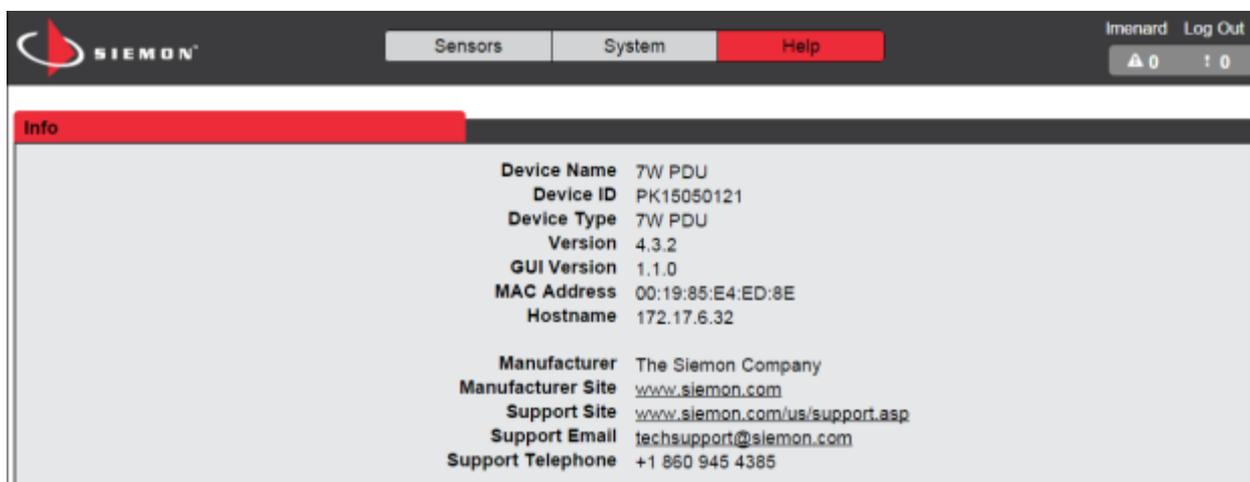


Firmware updates will come in a .ZIP archive file containing several files including the firmware package itself, a copy of the SNMP MIB, a "readme" text file explaining how to install the firmware, and various other support files as needed.

Help

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.



Device Name	7W PDU
Device ID	PK15050121
Device Type	7W PDU
Version	4.3.2
GUI Version	1.1.0
MAC Address	00:19:85:E4:ED:8E
Hostname	172.17.6.32
Manufacturer	The Siemon Company
Manufacturer Site	www.siemon.com
Support Site	www.siemon.com/us/support.asp
Support Email	techsupport@siemon.com
Support Telephone	+1 860 945 4385

Support Site

Technical support and documentation can be found at <http://www.siemon.com/ipdu/updates>

Technical Support

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.*

Service and Maintenance

- 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.**

More Technical Support

If you have any questions pertaining to this this instruction manual or other related issues, please contact your regional Technical Services Group.

Worldwide Headquarters – North America

Watertown, CT USA
Phone (1) 860 945 4200

Regional Headquarters – EMEA

Europe/Middle East/Africa
Surrey, England
Phone (44) 0 1932 571771

Regional Headquarters – Asia/Pacific

Asia/Pacific
Shanghai, P.R. China
Phone (86) 21 5385 0303

Regional Headquarters – Latin America

Latin America
Bogota, Columbia
Phone (571) 657 1950

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 Intelligent 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.