POWER INNOVATIONS INTERNATIONAL

LITEON GROUP

# *UPQ-NetAgent9™*

## Remote and Local Management for Uninterruptible Power Quality™ Systems

# Installation and Operation Manual

**MNL116**

*Rev 4.2*

**Export Classification EAR99**

**READ THIS MANUAL CAREFULLY**
**SAVE ALL INSTRUCTIONS**

This manual contains important information needed to operate the NetAgent9™ safely and efficiently. Please read all instructions carefully before installing or operating equipment.

Keep this manual handy for easy reference.

## FCC Information

This equipment has been tested and found to comply with the limits for a class A/B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is used in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference with radio communications.

## FCC Caution

To ensure continued compliance, use only shielded interface cable when connecting to computer or peripheral devices. Any changes or modifications not expressly approved by the party responsible for compliance could void this compliance to the FCC rules.

# Table of Contents

# Table of Figures

# Table of Tables

*This page intentionally left blank.*

# 1—Introduction

Congratulations on purchasing Power Innovations International, Inc.'s UPQ-NetAgent9 network interface device. Power Innovations prides itself on its superior product quality and hopes that the NetAgent and the system of which it is a part will serve you well for a long time.

Manual Helps

For warranty and customer service information for this product, please refer to **9—Warranty and Copyright**.

For information about how to find specific information located within this manual see **Table of Contents**. For an explanation of manual contents, see **1.2—Using this Manual**.

## 1.1—Product Overview

The UPQ-NetAgent9™ is an optional accessory that provides tools for remote monitoring and management of a Power Innovations Uninterruptible Power Quality™ (UPQ™) power management and battery backup system. With a NetAgent installed, use a computer on the local network or over the internet to view real-time status reports or logs for events such as AC power loss, battery charge status, or system load.

There are two main models of NetAgent, the BX (BX505 and BX506) and BY (BY505 and BY506) models as well as the NetAgent Mini with a similar interface but smaller hardware.

### 1.1.1—Remote Notification and Management

The NetAgent can send system event notifications via SNMP trap notifications; email; an optional USB GPRS/GSM wireless modem (connected directly to the NetAgent or monitoring server); MODBUS TCP; or SMS text messages.

With the NetAgent, the UPQ can be configured and managed remotely, allowing tasks such as testing the batteries or putting the system into sleep mode.

Manual Helps

For definitions of technical terms, see **Appendix A—Glossary**.

### 1.1.2—e-Alert Sensor™

The optional e-Alert Sensor™ environmental monitor can add temperature, humidity, and flood sensors to the UPQ-NetAgent9. A wireless smoke/gas detector and up to seven wireless door/window alarm sensors can also connect to the e-Alert Sensor to provide additional security monitoring.

### 1.1.3—Customizable Interfaces

All of the UPQ-NetAgent9 features, including the e-Alert Sensor, are accessible using the included monitoring application or the web-based management interface. Users can set alarm triggers and actions, including event notifications and clean system shutdowns for machines connected to the UPQ. The management interfaces also provide several tools for remotely testing the condition of the batteries and backup systems.

Real-time status reports, events, and logs can also be provided automatically, or on a schedule-based need.

### 1.1.4—Remote Management

The NetAgent also includes an auto-configuring RJ45 Ethernet adapter or has built-in support for an external USB 802.11b/g wireless adapter.

The NetAgent can be managed from any computer with a web browser and network access. Initial configuration can be done with or without server a local DHCP auto-configuring wired (RJ45 Ethernet) network. Management software that can detect and configure the NetAgent if the NetAgent is connected to the same network segment as the computer running the configuration software (Netility). The software is available for Windows, MacOS, Linux, and other operating systems.

### 1.1.5—Specifications and Applications

| Feature | | Specification |
|---|---|---|
| CPU | | ARM9 180 MHz 32 Bit |
| Ports | Front | RJ45 (LAN Internet) |
| | | RJ45 (e-Alert Sensor) |
| | | 2x USB (GPRS/GSM Modem, 802.11 wireless adaptor) |
| | Back | RS232 (UPQ) |
| | | Coaxial power (9-12 V / 500 mA) |
| Flash Memory | | 8 MB |
| SDRAM | | 32 MB |
| DC Input | | 9–12 V / 500 mA |
| Display | | 3 LED Status lights, LCD Panel |
| Dimensions | | 158 cm x 80 cm |

***Table 1—Features and Specifications***

| Program | Compatible with | Function |
|---|---|---|
| **Netility** | Windows, MacOS, Linux | Identify NetAgent devices on the local network |
| | | Modify network configuration |
| | | Apply firmware upgrades |
| **SNMPView** | Windows only | Monitor and manage multiple NetAgents from a single SNMP application |
| **ClientMate** | Windows, MacOS, Linux, FreeBSD, VMWare | Perform clean system/server shutdown tasks when UPQ goes on battery power or when battery reaches critical levels |
| **SMS Server** | Windows only | Send SMS messages through a GPRS/GSM cellular modem connected to a computer |
| | | Send notifications from multiple NetAgent devices using a single GPRS/GSM cellular modem |

***Table 2—Programs and Compatibility***

## 1.2—Using this Manual

This manual will show how to install Power Innovations International, Inc.'s UPQ-NetAgent9. Often, the NetAgent has already been installed in a system when it arrives.

Read and understand this manual to make installing and operating the NetAgent as easy as possible.

## 1.3—Conventions Used in this Manual

To make this manual easier to read, several formatting conventions have been adopted.

### 1.3.1—Additional Advice

This manual will occasionally provide additional advice. When it is provided, this information will be enclosed by a set of lines to separate it from the rest of the text, like this:

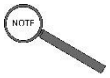
---

This text does not belong with the rest.

---

Some of the information is very important, while other information may be good to know. To show the importance of each piece of information, the following symbols are used:

Notes




Offers practical advice that may be helpful but can be disregarded.

Manual Helps

Offers a reference to another section of the manual that may be helpful.

Additional Manuals

Offers a reference to another manual that may be helpful.

Usually these symbols will be listed in order of importance.

### 1.3.2—Type Conventions

Menu options will be formatted in bold. If the menu options consist only of symbols, they will be placed in quotation marks.

Filenames will be placed in italics.

*This page intentionally left blank.*

# 2—Installation

## 2.1—Hardware Installation

The UPQ-NetAgent9™ (both internal and external) is an auto-configuring, hot-swappable device. It is not necessary to turn OFF or reboot the UPQ in order to install and use the UPQ-NetAgent9.

***Figure 1—Green Serial Cable***

***Figure 2—Ports on Front of NetAgent***

### 2.1.1—Installing an External (BX/BY505) UPQ-NetAgent9

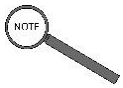
1. Unpack the UPQ-NetAgent9 and included accessories;
2. Connect the male end of the included serial cable to the serial adapter on the back of the UPQ-NetAgent9;
3. Connect the female end of the included serial cable to the serial adapter on the back of the UPQ;
4. Connect the power adapter DC plug to the power supply jack on the back of the NetAgent;
5. Connect a live Ethernet (RJ45) cable to the Ethernet port (far left) on the front of the NetAgent;
6. Plug the AC converter end of the power adapter into one of the power outlets on the back of the UPQ.

### 2.1.2—Installing an Internal (BX506) UPQ-NetAgent9 (Mini/MiniGo)

1. Unpack the NetAgent;
2. Locate the module cover plate on the back of the UPQ;
3. Remove and keep the screws that hold the cover plate in place;
4. Remove the cover plate;
5. Slide the NetAgent into the opening, making sure that the connector seats properly in the slot;
6. Place the provided cover plate (with cutouts for the ports) over the opening;
7. Use the original screws to secure the new cover plate in place;
8. Connect a live Ethernet (RJ45) cable to the Ethernet port (far left) on the front of the NetAgent.

---

Note




The NetAgent with a Q-LS uses a special connection for power. The serial cable connects to CNR21 on the communications & display PCB (3R). The power also connects to this PCB. No external power source from the Q-LS is necessary.

---

## 2.2—Software Installation

The included software provides tools for configuring and managing the UPQ-NetAgent9.

Manual Helps

**Chapter 3—UPQ-NetAgent9 Management** provides information about how to install and use the individual software applications, as well as the built-in web management interface.

# 3—UPQ-NetAgent9 Management

## 3.1—Managing the NetAgent

The NetAgent is managed and configured remotely using a management application or the web interface.

The first time the NetAgent is turned ON, it will attempt to negotiate a connection with the local DHCP server over the wired Ethernet connection. Even if an IP connection isn't established, it is possible to use *Netility*, user interface to configure different connection options, including a permanently assigned IP address or use of a USB wireless 802.11 network adapter; once an appropriate IP configuration is set on the NetAgent, the device can be further configured through the Web interface.

Manual Helps

For help installing or configuring the NetAgent on a wireless network, see **8.2—USB 802.11 Wireless Adapter**.

Although a network connection is necessary to connect to the NetAgent or to send email or SNMP trap notifications, it is not necessary for automated management or SMS notifications using a GPRS/GSM cellular modem. Additionally, a standard USB drive can be connected to the NetAgent to do local event and data logging on the UPQ system. This USB drive can then be disconnected when desired and have data downloaded to a computer in CSV format.

Manual Helps

For definitions of technical terms, see **Appendix A—Glossary**.

## 3.1.1—Using Netility

Netility provides an easy tool for identifying, configuring network settings, and upgrading the firmware of all NetAgent devices on a network. The application automatically discovers any NetAgent devices on the local network, then lists the serial number, MAC address, and IP address of all devices.

Netility is available for Windows, MacOS, and Linux computers.

### 3.1.1.1—Installing Netility on Windows, MacOS, or Linux

To install Netility on Windows download the installer file from the Power Innovations website (see the **Contacting Power Innovations** at the back of this manual.

1. Run Netility.exe;
2. If prompted, click **Yes** to allow Netility.exe to make changes to the computer;
3. Follow the installer on-screen instructions to complete the installation process.

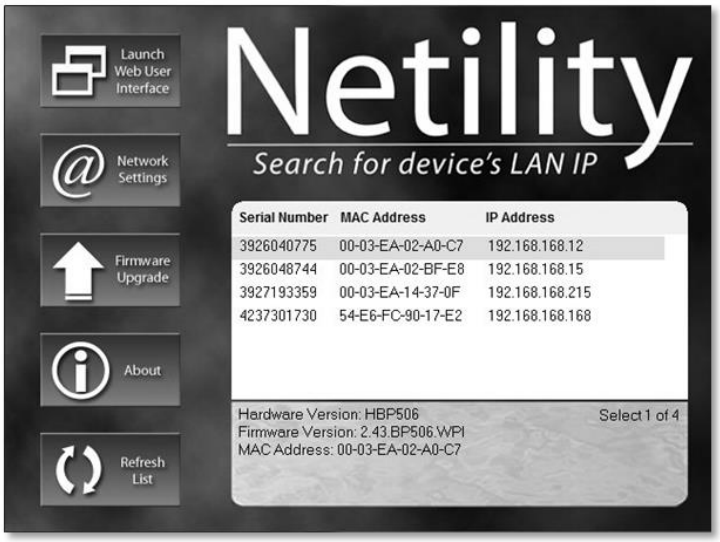



***Figure 3—Netility Opening Screen***

### 3.1.2—Managing a NetAgent Using Netility

1. Launch Netility:
   a. In Windows, go to **Start (All Programs)**>**NetAgent**>**Netility** and click **Netility**;
   b. In Linux, go to **Applications**>**Internet** and click **Netility**;
   c. In MacOS, go to **Applications** and click **Netility**;
2. If the desired NetAgent is not listed, click **Refresh List** to force Netility to search for the device again;
3. If the desired NetAgent is still not listed, make sure both the NetAgent and the computer running Netility are on the same network segment with no traffic restricting appliances in-between.
4. Select the NetAgent from the list of devices on the local network;
5. Click **Launch Web User Interface** to open the web interface for the selected NetAgent;
6. See **3.2—Using the Web Interface** for more information about managing the NetAgent through the web interface.

### 3.1.3—Using Netility to Modify Network Settings

1. Launch Netility. In Windows, go to **Start** > **(All Programs)** > **NetAgent** > **Netility** and click **Netility**;
2. If the desired NetAgent is not listed, click **Refresh List** to ask Netility to search for the device again;
3. If the desired NetAgent is still not listed, make sure both the NetAgent and the computer running Netility are on the same network segment with no traffic restricting appliances in-between.
4. Select the NetAgent from the list of devices on the local network;
5. Click **Network Settings**;
6. Select the radio button to indicate whether the NetAgent should obtain an IP address automatically from the DHCP server or be assigned a static IP address;
7. If the NetAgent will use a static IP address, enter the **IP address**, **Subnet Mask**, and **Gateway** that the NetAgent should use when connecting to the network;

---

Manual Helps

For definitions of technical terms (such as static IP address, IP address, Subnet Mask, and Gateway), see **Appendix A—Glossary**.

---

8. Click the **Advanced** tab;
9. Select the network protocols (**HTTP**, **HTTPS**, **Telnet**, **SSH**) the NetAgent should run. The **HTTP** or **HTTPS protocol** *must* be checked to use the web interface;

10. Enter an alternate port, if desired, for the selected protocol to listen on. If an alternate port is used, the alternate port number must also be specified in the client request (to use port 81 for HTTP, the address of the NetAgent in a browser must also specify port 81. e.g.: *http://192.168.168.168:81/*)

---

Manual Helps

For definitions of technical terms used in **Steps 8** and **9**, see **Appendix A—Glossary**.

---

To require a password to modify the network settings using Netility:

1. Click the **Password** tab;
2. Check the **Enable password setting** box;
3. Enter the desired password in the **New password** field;
4. Enter the same password in the **Confirm password** field;
5. Click **OK**;
6. If a password is required, enter the password and click **OK**.

### 3.1.4—Upgrading NetAgent Firmware with Netility

1. Obtain the firmware image from Power Innovations;

---

**Caution**

Do not attempt to install older versions of the firmware on a NetAgent. Always install every individual upgrade in order and note that firmware versions are hardware type specific. (do versions).

---

2. Save a copy of the firmware image in a location accessible to the computer running Netility;
3. Launch Netility. In Windows, go to **Start** > **(All Programs)** > **NetAgent** > **Netility** and click **Netility**;
4. If the desired NetAgent is not listed, click **Refresh List** to force Netility to search for the device again;
5. Select the NetAgent from the list of devices on the local network;
6. Click **Firmware Upgrade**;
7. Click the **"…"** button to browse for and select the firmware image;
8. Click **Download**. The NetAgent red and yellow status lights will blink alternately while the firmware is being downloaded and installed;
9. Wait for the NetAgent to complete installing the upgrade. Reboot.
10. If the desired NetAgent is still not listed, make sure both the NetAgent and the computer running Netility are on the same network segment with no traffic restricting appliances in-between.
11. If the update fails to power cycle the NetAgent, start the update process over.

---

**Caution**

Do not interrupt the upgrade by shutting down power or attempting to view or modify settings on the NetAgent while the firmware upgrade is in progress.

# 3.2—Using the Web Interface

The NetAgent web interface provides complete reporting and control for the NetAgent, the UPQ, and any other connected accessories. It is best to interface using Internet Explorer, but other fully functional web browsers such as Firefox, Chrome, or Opera may also be used. Limited functionality browsers, such as those on mobile devices, may not display the web interface properly.

Note

The web interface is accessible through the NetAgent's built-in web server. If the web interface is not working, ensure the NetAgent is fully booted and check that the HTTP and HTTPS functions are enabled in the Netility **Network Settings**>**Advanced settings**.

Manual Helps

See **3.1.3—Using the Web Interface to Modify Network Settings** for more information.

## 3.2.1—Connecting Using Netility

1. Launch Netility (see **Using Netility**) on a computer connected to the same network as the NetAgent;
2. Select the desired NetAgent from the list of devices;
3. Click **Launch Web User Interface**—the web interface will open in the default browser;

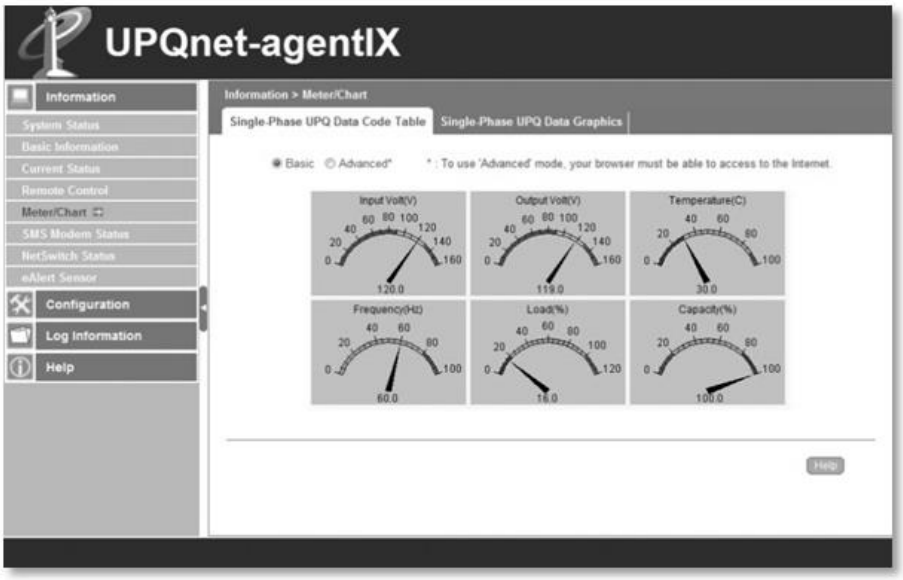



***Figure 4—One Netility Screen***

### 3.2.2—Connecting Directly

1. Open a web browser on a computer connected to the same network as the NetAgent;
2. Enter the NetAgent **IP address**;

---

Manual Helps

For definitions of technical terms, see **Appendix A—Glossary**.

---

3. Press **Enter**. The web interface will open in the browser window.

## 3.3—Notes about the User Interface

The NetAgent web user interface is divided into four sections: **Information**, **Configuration**, **Log Information**, and **Help**. Information about the screens in each section is outlined below.

Due to differences between single-phase and 3-phase systems, the screens for the systems are different. Screens that are different are indicated as being specific to single-phase or 3-phase systems.

## 3.4—Information Screens

The **Information** section of the interface provides access to real-time status information about the NetAgent, the UPQ, and any other devices connected to the NetAgent. This screen is for information only. Configurations are made from other screens.

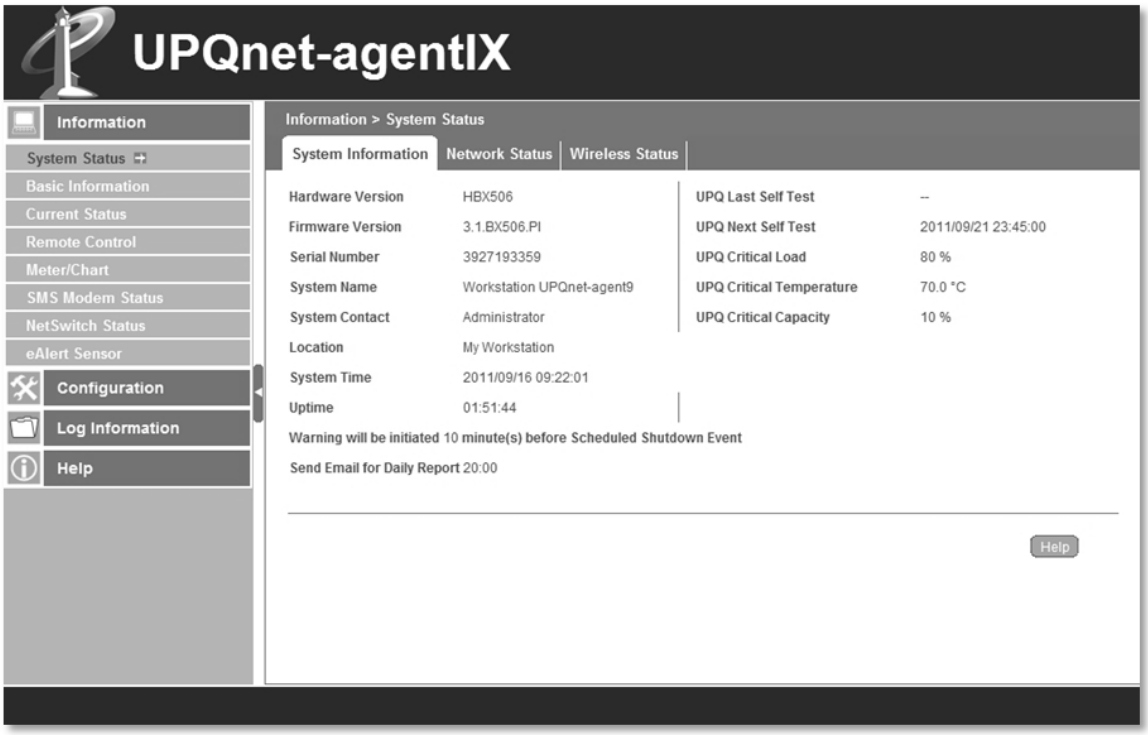



***Figure 5—Information→System Status screens***

### 3.4.1—System Status

The **System Status** screen provides overviews of information about the NetAgent device and network connections, such as:

- **Hardware Version**, **Firmware Version**, and **Serial Number** as sent from the NetAgent.
- **System Name**, **System Contact**, and **Location** as obtained from the **Configuration**>**SNMP**> **MIB System settings**.
- **System Time** configured on the **Configuration**>**System Time** screen.
- **Uptime** based off of the current system time and the system time when the NetAgent came online.
- **Warning time** settings before a scheduled shutdown event, as configured on the **Configuration**>**UPQ ON/OFF Schedule** screens.
- **Email for daily report** setting, as configured on the **Configuration**>**Email** settings.
- **Last Self-Test** and **Next Self-Test**, as scheduled on the **Configuration**>**UPQ Configuration**>**Test UPQ** screen.
- **Critical Load**, **Critical Temperature**, and **Critical Capacity** as set on the **Configuration**>**UPQ Configuration**>**Warning Threshold** screen.

The NetAgent will beep and send an event notification via email, SMS, or SNMP. It will also beep if the measured value goes beyond the specified critical limit.

#### 3.4.1.1—Network Status

This tab displays the wired (Ethernet) network settings:


***Figure 6—Information→System Status→Network Status***

By default, the NetAgent uses DHCP to configure the network connection. Network settings can be modified on the **Configuration**>**Network** screens.

Manual Helps

For definitions of technical terms, see **Appendix A—Glossary**.

### 3.4.1.2—Wireless Status

The Wireless Status tab displays the wireless (802.11 b/g) network settings:

By default, the NetAgent uses DHCP to configure the wireless network. Wireless network settings are configured on the **Configuration**>**Wireless** screens.


***Figure 7—Information→System Status→Wireless Status***

Manual Helps

For definitions of technical terms, see **Appendix A—Glossary**.

### 3.4.2—Basic Information

Both single-phase and 3-phase screens provide basic information about the UPQ. On the 3-phase system monitoring software, the **Basic Information** screen content is contained on one single screen.

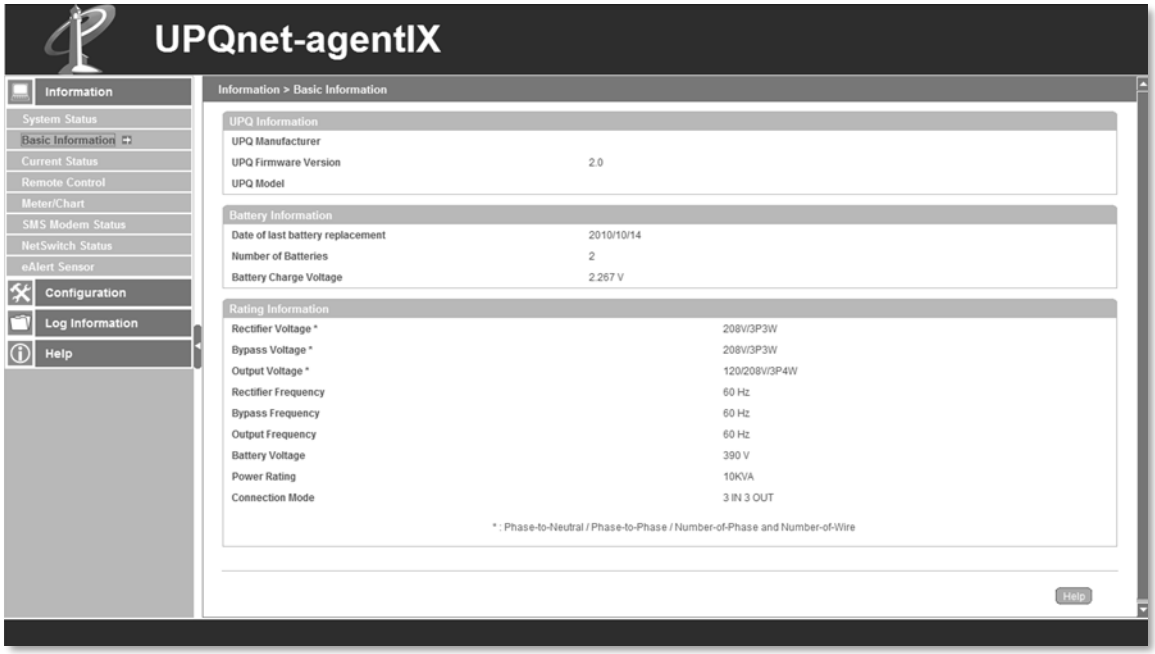



***Figure 8—Information→Basic Information***

#### 3.4.2.1—UPQ Information

Displays information about the UPQ. This information is obtained from the UPQ and cannot be changed.

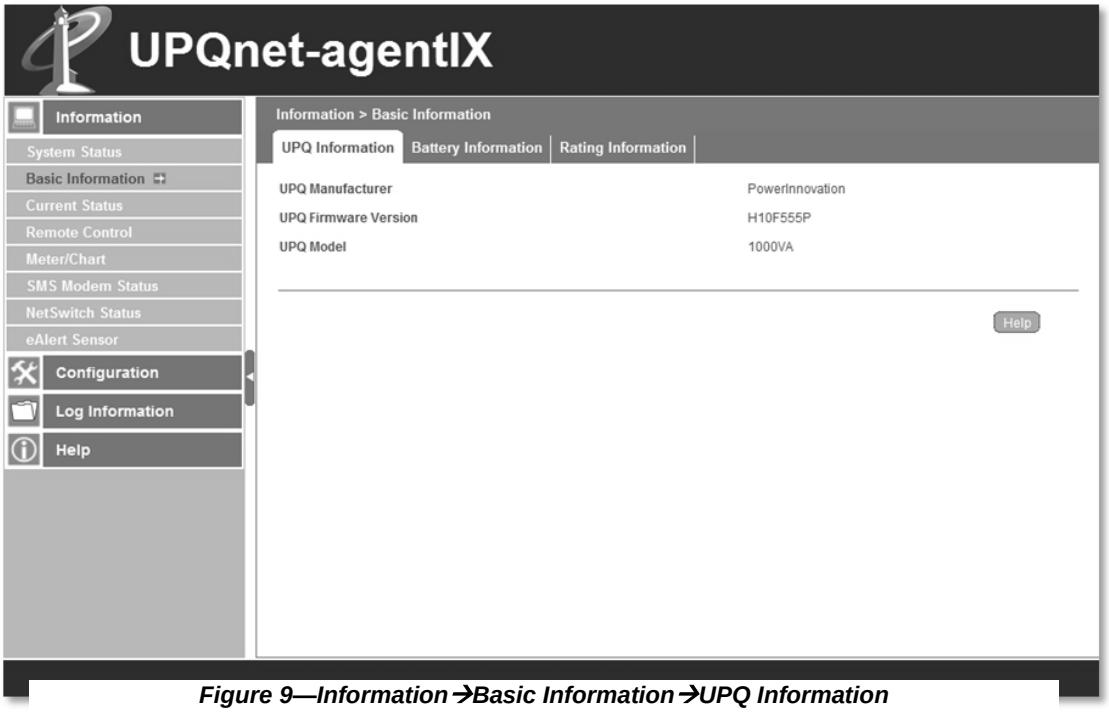



***Figure 9—Information→Basic Information→UPQ Information***

### 3.4.2.2—Battery Information

Displays basic information about the batteries in the UPQ.

Battery information can be configured on the **Configuration**>**UPQ Configuration**>**UPQ Properties** screen.


***Figure 10—Information→Basic Information→Battery Information***

### 3.4.2.3—Rating Information (3-Phase)

Single-phase: Displays basic information about UPQ voltage ratings.

3-phase: Displays information about the input, output, and DC rail.


***Figure 11—Information→Basic Information→Rating Information***

### 3.4.3—Current Status

Current Status screens provide a real-time view of UPQ operating status. Three single-phase screens are used: **Input Status, Output Status, and Battery Status**.

Five tabs for 3-phase screens are used: **Rectifier Status, Bypass Status, Output Status, Inverter Status, and Battery Status.**

#### 3.4.3.1—Input Status (Single-Phase)

Displays a real-time view of the UPQ's AC input.


***Figure 12—Information→Current Status→Input Status (Single-Phase)***

**Refresh status every—**This value determines how frequently the screen will be refreshed with new readings from the NetAgent. The display update interval can be shortened for diagnostic and calibration or can be extended for general use.

### 3.4.3.2—Output Status (Single-Phase)

Displays a real-time view of AC output from the UPQ.

**Refresh status every—**This value determines how frequently the screen will be refreshed with new readings from the NetAgent. The display update interval can be shortened for diagnostic and calibration or can be extended for general use.

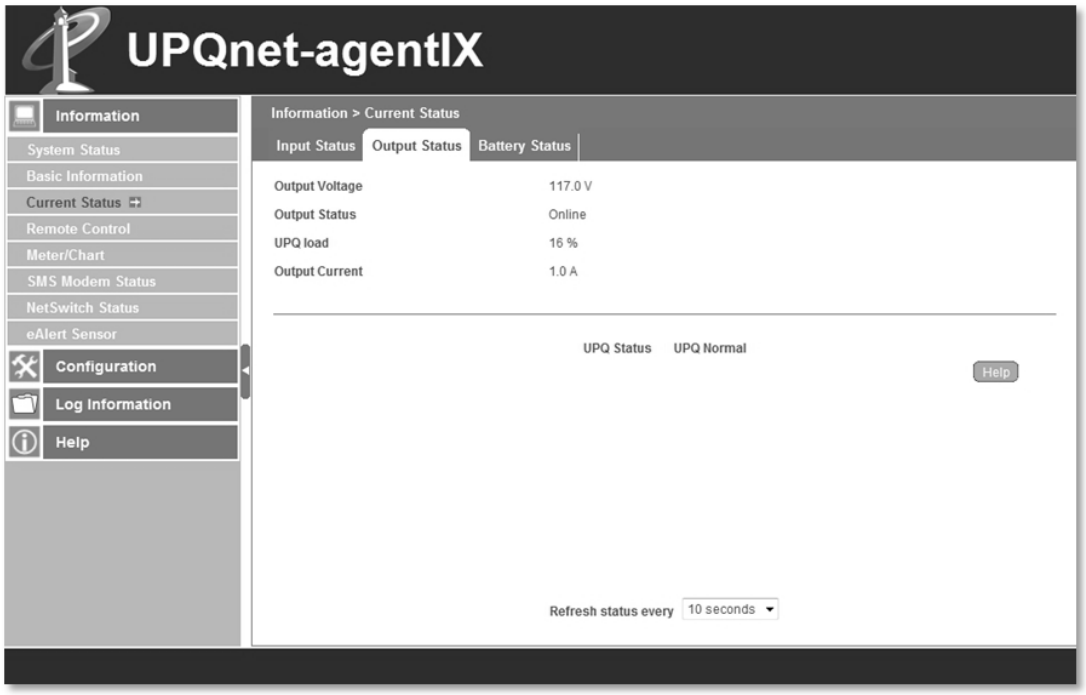



***Figure 13—Information→Current Status→Output Status (Single-phase)***

### 3.4.3.3—Battery Status (Single-Phase)

Displays a real-time view of UPQ battery status.

**The Battery Capacity value**—Determined from the difference between the actual battery voltage reading and the configured full battery voltage.

---

Manual Helps

See **3.9—Calibrating Battery Capacity Voltage** to calibrate this reading for the most accuracy.

---

**Refresh status every—**This value determines how frequently the screen will be refreshed with new readings from the NetAgent. The display update interval can be shortened for diagnostic and calibration or can be extended for general use.


***Figure 14—Information→Current Status→Battery Status (Single-phase)***

### 3.4.3.4—Rectifier Status (3-Phase)

Displays a real-time view of the rectifier input line.

**Refresh status every ___—**This value determines how frequently the screen will be refreshed with new readings from the NetAgent. The display update interval can be shortened for diagnostic and calibration or can be extended for general use.

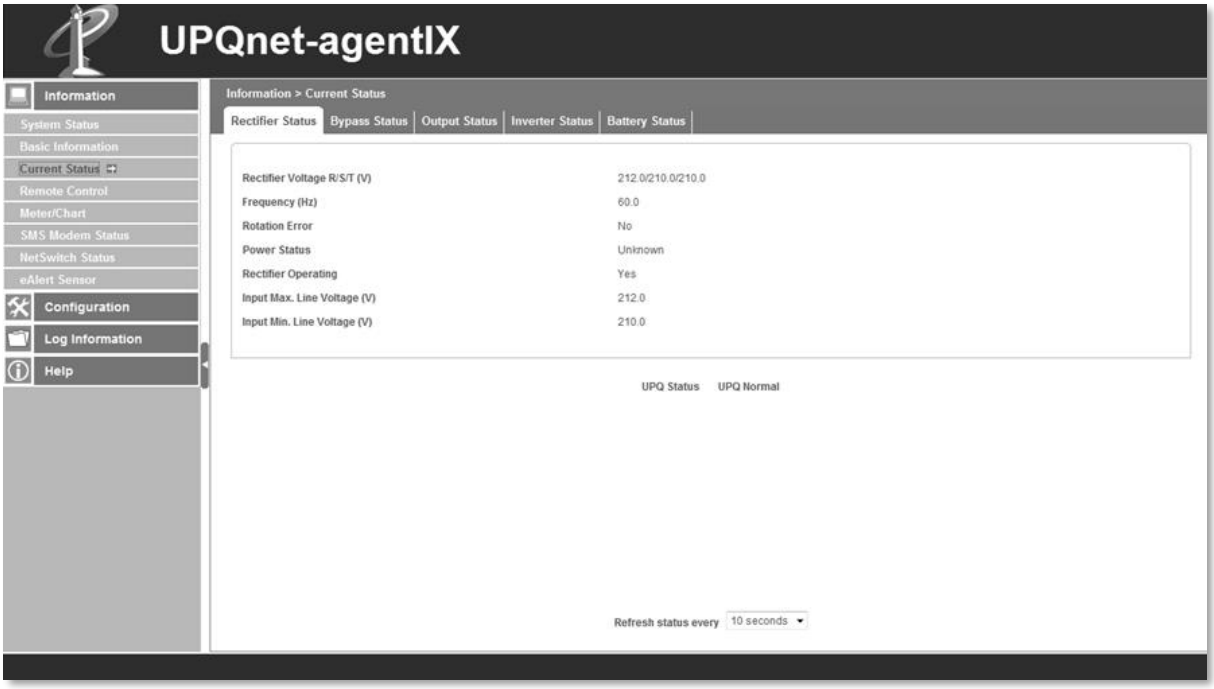



***Figure 15—Information→Current Status→Rectifier Status (3-phase)***

### 3.4.3.5—Bypass Status (3-Phase)

Displays a real-time view of the bypass input line.

**Refresh status every____—**This value determines how frequently the screen will be refreshed with new readings from the NetAgent. The display update interval can be shortened for diagnostic and calibration or can be extended for general use.

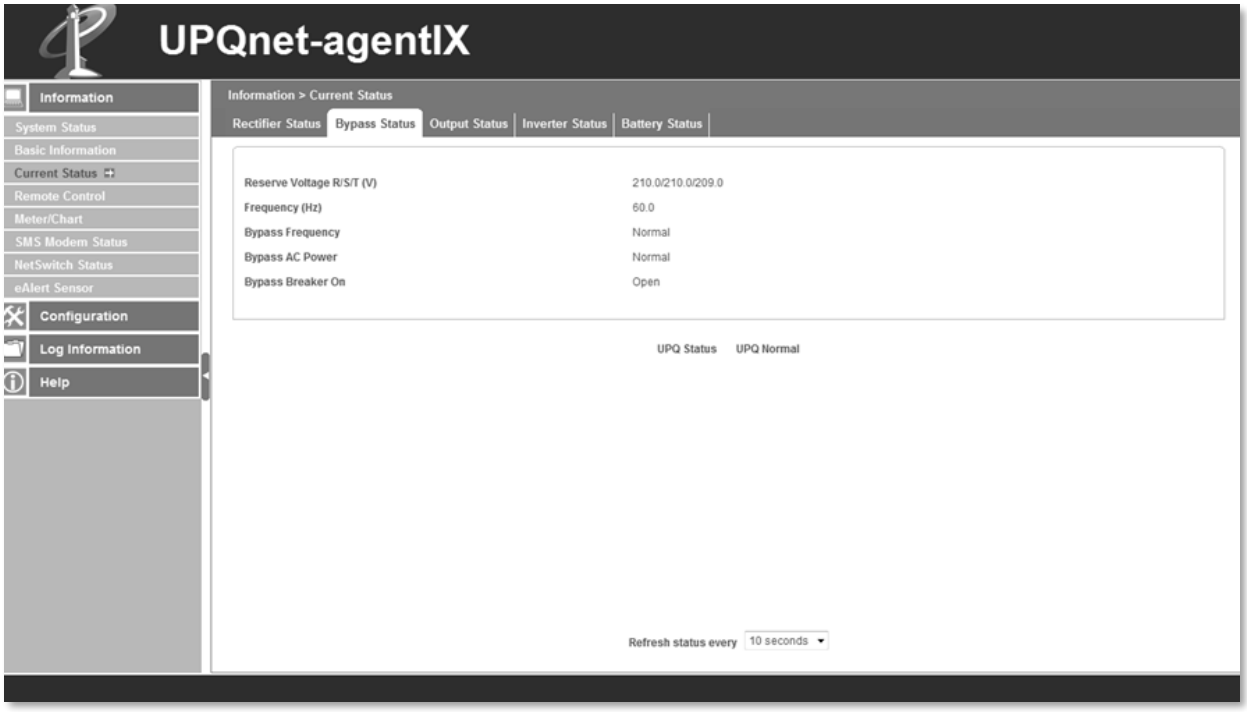



***Figure 16—Information Current Status Bypass Status (3-phase)***

### 3.4.3.6—Output Status (3-Phase)

Displays a real-time view of the AC output from the UPQ.

**Refresh status every—**This value determines how frequently the screen will be refreshed with new readings from the NetAgent. The display update interval can be shortened for diagnostic and calibration or can be extended for general use.


***Figure 17—Information→Current Status→Output Status (3-Phase)***

### 3.4.3.7—Inverter Status (3-Phase)

Displays a real-time view of the inverter operational status.

**Refresh status every—**This value determines how frequently the screen will be refreshed with new readings from the NetAgent.

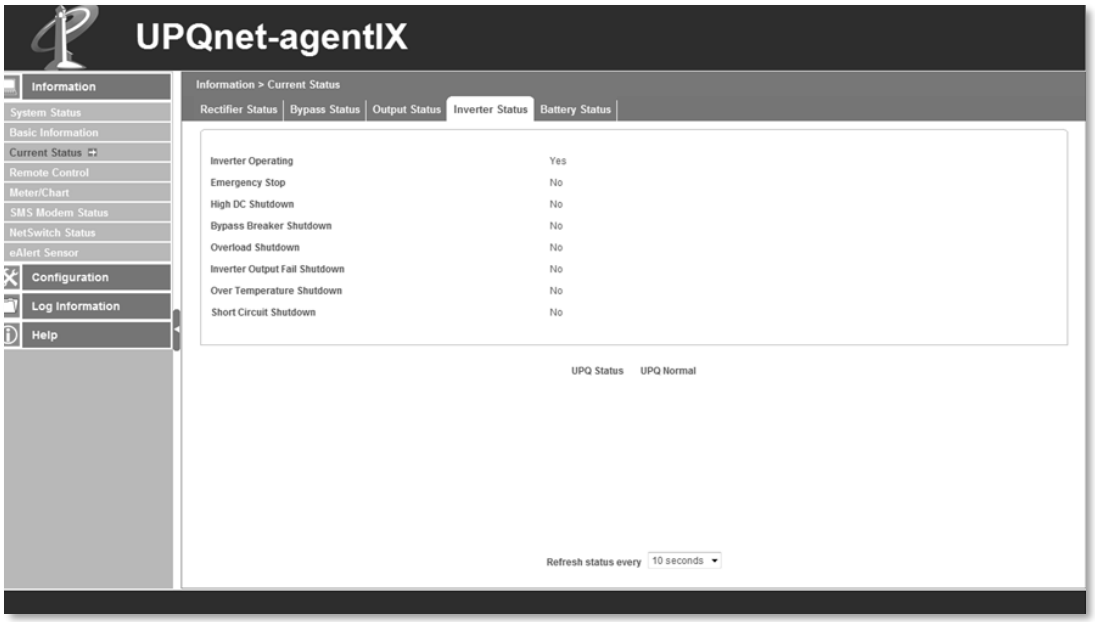



***Figure 18—Information→Current Status→Inverter Status (3-Phase)***

### 3.4.3.8—Battery Status (3-Phase)

Displays a real-time view of the status of the connected batteries.

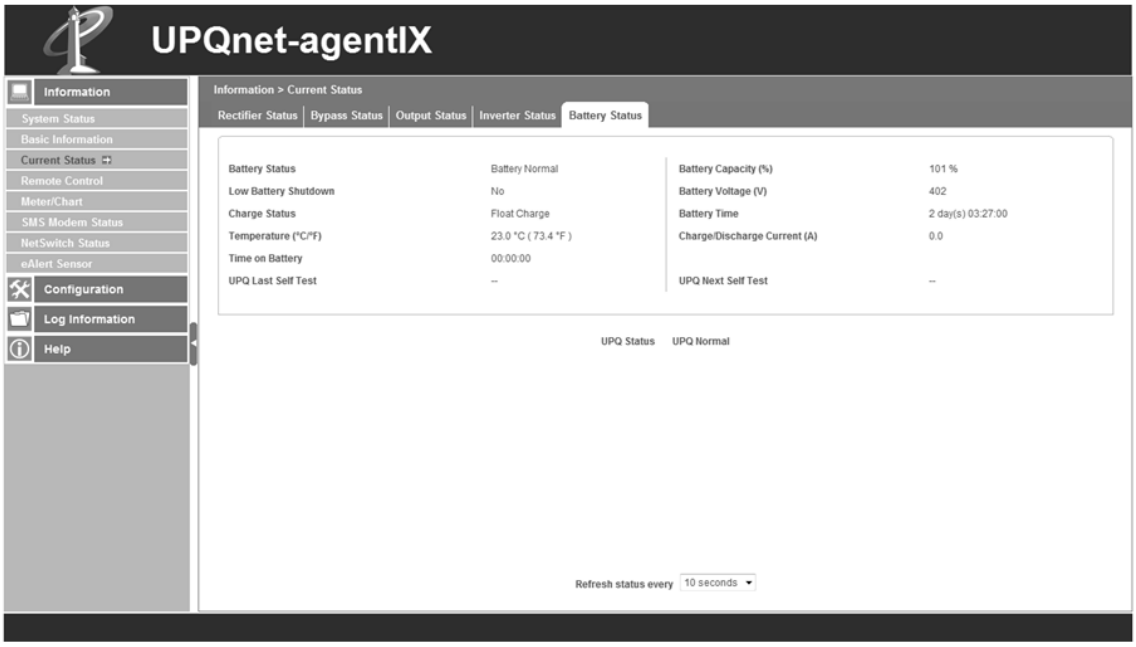



***Figure 19—Information→Current Status→Battery Status (3-Phase)***

**Battery Capacity—**Determined from the difference between the actual battery voltage reading and the configured full battery voltage.

Manual Helps

See **3.9—Calibrating Battery Capacity Voltage** to calibrate this reading for the most accuracy.

**Refresh status every—**This value determines how frequently the screen will be refreshed with new readings from the NetAgent. The display update interval can be shortened for diagnostic and calibration or can be extended for general use.

## 3.4.4—Remote Control

This section provides tools for testing and managing power status.

### 3.4.4.1—UPQ Testing

Each test will be performed when the **Apply** button is pressed. Provides the following options for testing UPQ power backup and batteries:


***Figure 20—Information→Remote Control→UPQ Testing***

**10-Second Test**—Simulates a 10-second interruption in main UPQ AC power source to verify the UPQ will successfully switch over to battery backup and back to AC without interrupting critical functions.

**Deep Battery Test for ____ minutes**—Simulates an interruption in UPQ AC power source for the specified time. This test is good for ensuring that the batteries will sustain the system for the time necessary to perform a clean shutdown during AC power loss. The battery test log (**Log Information**>**Battery Test Log**) will operate on battery power, based on the current load and battery charge level.

**Test until Battery Capacity below ____ %**—Simulates an interruption in the UPQ's AC power source until the UPQ battery level reaches a specified threshold, at which time the test will end. A useful test for determining the actual longevity of the UPQ batteries during AC power loss. To get accurate longevity estimates, it is a good idea to run tests that drain the battery to 50% or less.

**Test until Battery Low**—Simulates an interruption in AC input power until the battery reaches the preset **Critical Capacity** (see **3.9—Calibrating Battery Capacity Voltage**). Useful for ensuring that automated system shutdown software (like ClientMate) will be able to complete a system shutdown prior to battery failure.

**Cancel Test**—Discontinue a test at any time.

### 3.4.4.2—Miscellaneous

Provides a tool for modifying various UPQ settings. These functions are selected during the radio buttons and will be performed when the **Apply** button is pressed.


***Figure 21—Information Remote Control Miscellaneous***

**Turn OFF UPQ when AC Power Fails**—Disables battery backup function and causes UPQ to shut down immediately when power fails.

**Wake up UPQ**—Sends an immediate wake-up call to a UPQ that has been put to sleep. A sleeping UPQ does not send power to the AC output. An internal NetAgent does not lose power and will remain operational if the UPQ is asleep.

**UPQ Buzzer ON/OFF**—Turns the UPQ alert buzzer ON or OFF. If the buzzer is OFF, the UPQ will continue to function normally but will not sound audible alerts during AC power loss.

**Put UPQ in Sleep mode for ___ minutes**—Puts the UPQ into sleep mode (producing no output) for the specified time. The internal NetAgent will remain powered while the system is sleeping.

**Reboot UPQ**—Causes the UPQ to perform a complete shutdown and restart. AC power output will not be available while the UPQ is rebooting.

## 3.4.5—Meter/Chart

Uses a Java applet (requires Java) to display the real-time status of critical UPQ functions.

### 3.4.5.1—UPQ Data Code Table

Displays the real-time status using a series of virtual gauges.

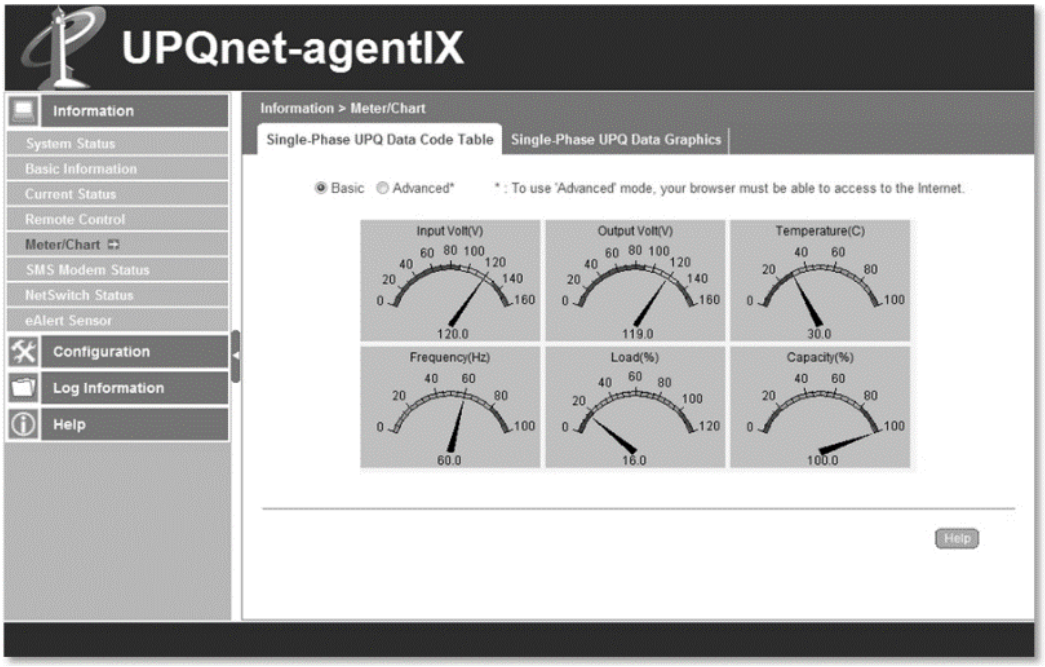



***Figure 22—Single-Phase Display***

*Figure 23—3-Phase Display*

**Advanced radio button**—Switches the display to a version with more graphically advanced gauges. Advanced mode requires an Internet (WAN) connection.

### 3.4.5.2—UPQ Data Graph

Displays the real-time status and a 2-minute history of the UPQ, using a line graph.

**Advanced radio button**—Switches the view to an interactive graph that can be zoomed in and out and display measured readings for a selected duration.

In the lower table, view statistics for a specific time by clicking on that time on the graph.

Zoom in the graph to view an exclusive time range by clicking the earliest time to view, then dragging the mouse right and releasing the button on the latest time.

When the graph has been zoomed in, zoom it out by clicking on a time and dragging the mouse left before releasing the button.


*Figure 24—Single-Phase Basic*

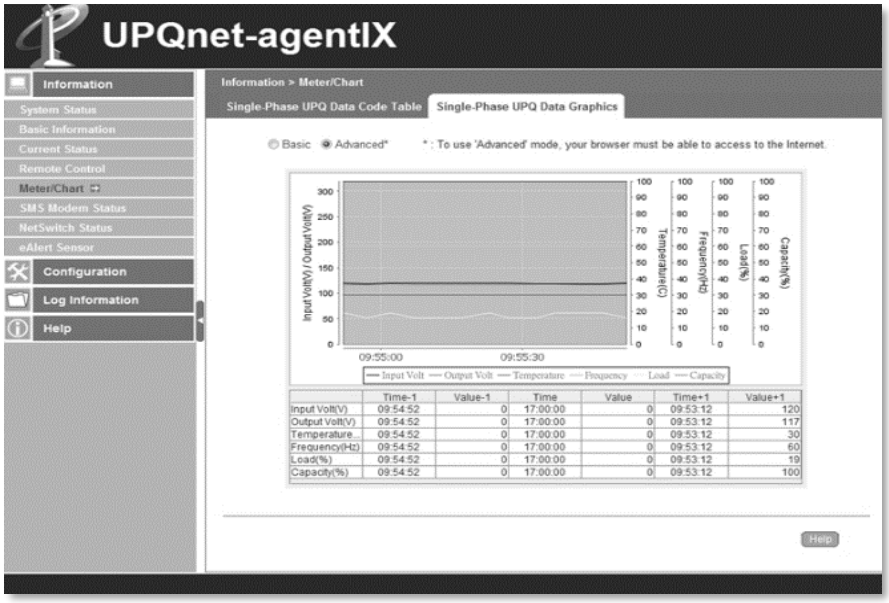



***Figure 25—Single-Phase Advanced***


***Figure 26—Information→Meter/Chart→UPQ Data***

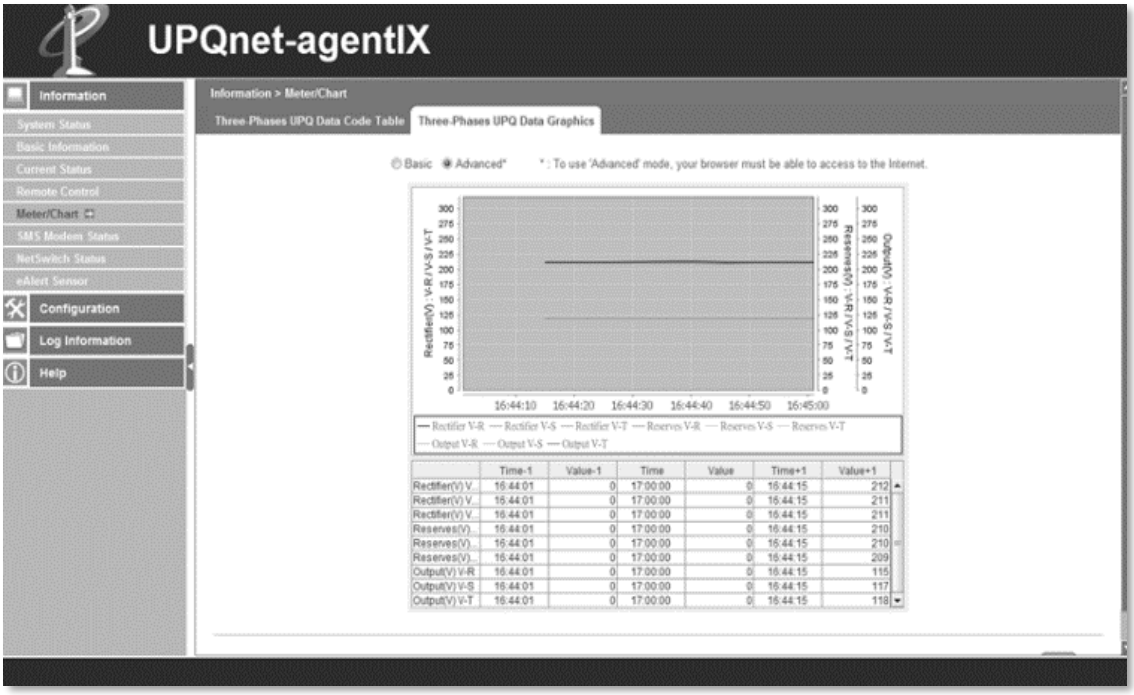



***Figure 27—Information→Meter/Chart→UPQ Data Graphics***

## 3.4.6—SMS Modem Status

These screens display status information about the optional GPRS cellular modem.

### 3.4.6.1—Modem Information

Displays information about the GPRS modem connected to the NetAgent.

Information about the GPRS modem is obtained from the actual modem. This information cannot be configured.

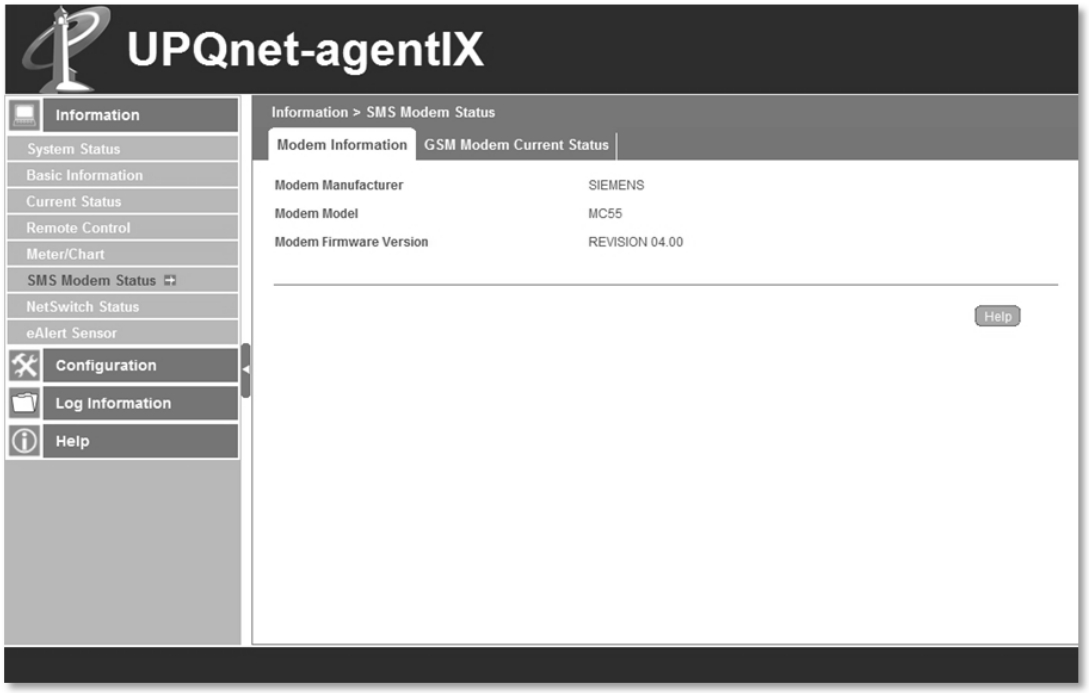



***Figure 28—Information→SMS Modem Status→Modem Information***

---

Manual Helps

For definitions of technical terms, see **Appendix A—Glossary**.

---

### 3.4.6.2—GSM Modem Current Status

Displays information about the GPRS cellular connection status.

**Service Provider, Central number of SMS service, and Signal Strength**—Determined by the SIM card inserted in the GPRS modem and the proximity of a compatible cellular service tower.

**SIM card PIN is correct (or incorrect)**—Displays “SIM card PIN is correct” if the SIM card has been configured properly and the modem is able to send messages. If the modem cannot send message, “no PIN configured” will display.


***Figure 29—Information→SMS Modem Status→GSM Modem Current Status***

---

Manual Helps

For definitions of technical terms, see **Appendix A—Glossary**.

---

## 3.4.7—NetSwitch Status

Displays information about any NetSwitch devices (remotely controlled AC power outlets) connected to the NetAgent.

### 3.4.7.1—NetSwitch Status and Control

Displays the status and provides power switching controls for any NetSwitch devices connected to the NetAgent.

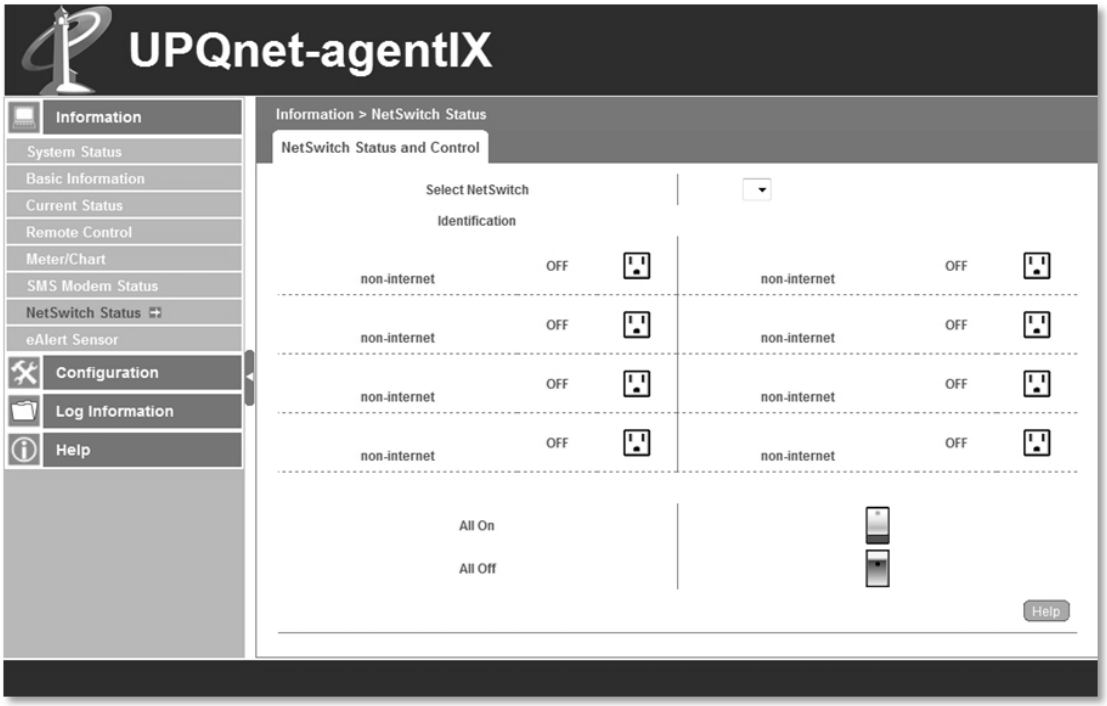



***Figure 30—Information→NetSwitch Status→NetSwitch Status and Control***

## 3.4.8—e-Alert Sensor

Displays status information about the optional e-Alert Sensor environmental monitor.

### 3.4.8.1—e-Alert Sensor Status

Displays the current sensor readings for the e-Alert Sensor connected to the NetAgent.

The sensor readings are obtained from the e-Alert Sensor and will display in red if there is an alert status.

The names of security sensors (in the right-hand column) are customizable under **Configuration** > **e-Alert Sensor** > **Security Label**.

**Refresh status every**—This value determines how frequently the screen will be refreshed with new readings from the NetAgent. The display update interval can be shortened for diagnostic and calibration or can be extended for general use.

**Reset Alarm**—Can be used to clear an alarm status.

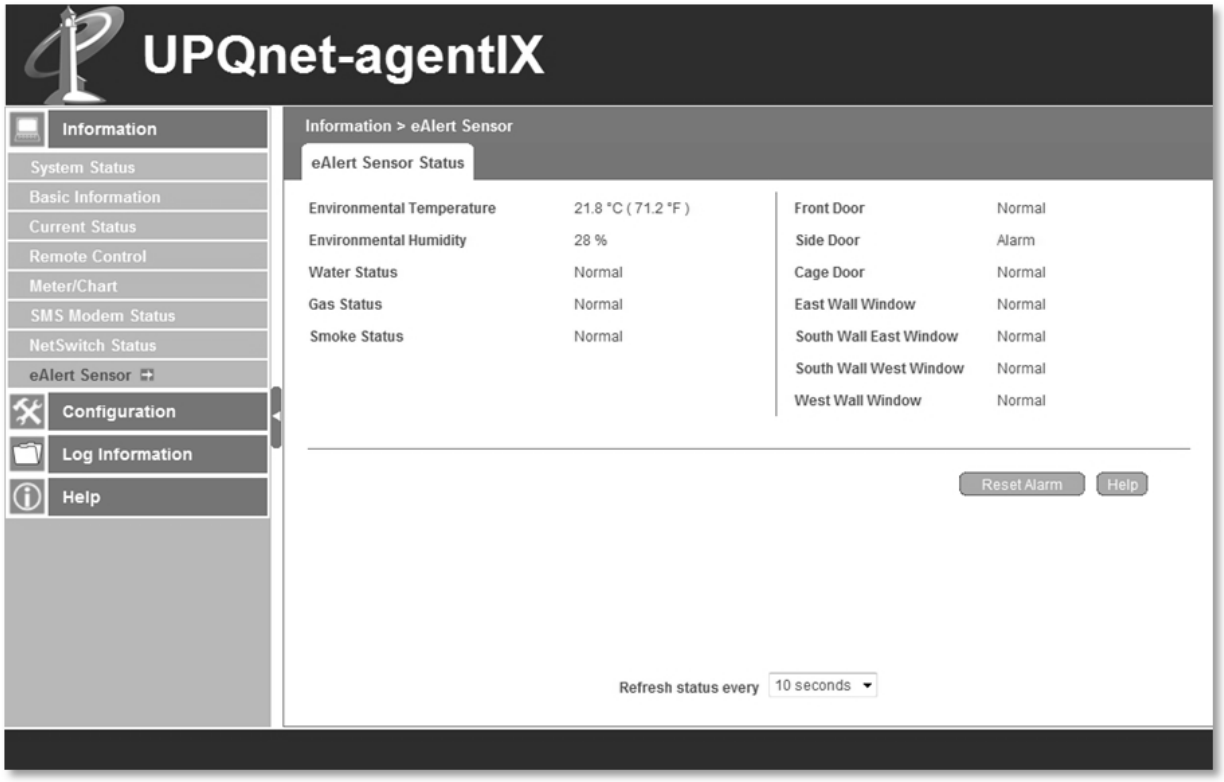



***Figure 31—Information→e-Alert Sensor→e-Alert Sensor Status***

# 3.5—Configuration

The **Configuration** section of the interface provides tools to configure and modify settings for the NetAgent, the connected UPQ, and any other connected accessories.

## 3.5.1—UPQ Configuration

These screens provide tools for modifying UPQ settings.

**3.5.1.1—UPQ Properties** Allows specific information about the connected UPQ to be entered.

**Single-Phase Screen**


**3-Phase Screen**

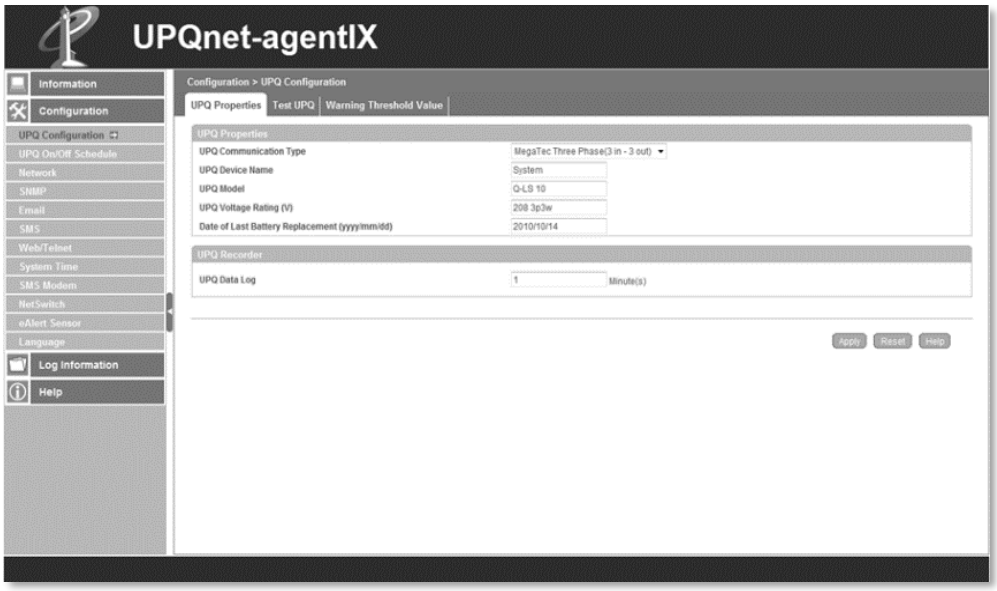



***Figure 32—Configuration→UPQ Configuration→UPQ Properties***

*Single-Phase:* The UPQ Communication Type should be set to **MegaTec**.

*3-Phase:* The UPQ Communication Type should be set to **MegaTec 3-phase**.

**Number of Batteries** should be set based off the number of batteries in the UPQ battery module.

**Battery Full Charge Voltage** should be calibrated using the instructions in **3.9—Calibrating Battery Capacity Voltage**.

**Battery Exhausted Charge Voltage** should be 1.667 V.

The **Date of Last Battery Replacement (yyyy/mm/dd)** should be set to the date the UPQ was first commissioned if the batteries have never been replaced. If the batteries have been replaced, this field should be set to the most recent battery replacement date.

Changes made on the screen are saved by clicking **Apply**.

**The Date of Last Battery Replacement (yyyy/mm/dd)** should be set to either the date the UPQ was first commissioned or the most recent battery replacement.

**UPQ Data Log** default interval is 1 minute. The interval can be changed by entering a new value.

Save all changes made on the screen by clicking **Apply**.

### 3.5.1.2—UPQ Recorder

Allows for a specific time interval to be entered between UPQ status updates in the **UPQ Data Log**.


***Figure 33—Configuration→UPQ Configuration→UPQ Recorder***

The **UPQ Data Log** default interval is 1 minute. The interval can be changed by entering a new value and clicking **Apply**.

### 3.5.1.3—Test UPQ

Schedule regular, automatic tests for the UPQ and batteries.

Testing can be scheduled by entering an interval, date, start time, and test type in the appropriate fields.

Save changes made on the screen by clicking **Apply**.


***Figure 34—Configuration→UPQ Configuration→Test UPQ***

### 3.5.1.4—Warning Threshold Value

Specify warning thresholds for power loss and battery state.

The NetAgent will beep every second. It will also send out any configured notifications (SMS, e-mail, SNMP) when one of the warning thresholds has been exceeded.

**Time out after loss of connection**—Time the NetAgent will wait after losing a connection with the connected UPQ before sending an alert (SMS, e-mail, or SNMP).

**Critical Load (%)—**Minimum power capacity allowed before the NetAgent sends a low-battery alert (SMS, e-mail, or SNMP).

**Critical Temperature (°C)—**Maximum temperature (from the e-Alert Sensor) that will be allowed before the NetAgent sends a low battery alert via SMS, email, or SNMP.

**Critical Capacity (%)—**Minimum battery capacity allowed before the NetAgent sends a low-battery alert via SMS, email, or SNMP.


***Figure 35—Configuration→UPQ Configuration→Warning Threshold Value***

Save changes made on this screen by clicking **Apply**.

### 3.5.1.5—UPQ ON/OFF Schedule

These screens provide tools for scheduling when the UPQ will be online and when it will be offline. When a shutdown time is set, the UPQ will go into sleep mode until the next scheduled wake time. An internal NetAgent will remain powered and operational while the UPQ is in sleep mode.

**Weekly Schedule**—Allows the UPQ to be turned ON and OFF on specified days of the week.


***Figure 36—Configuration→UPQ ON/OFF Schedule→Weekly Schedule***

**Warning will be Initiated—**Allows connected system with a monitoring service (such as ClientMate) to be shut down cleanly before UPQ shutdown.

Save changes made on this screen by clicking **Apply**.

### 3.5.1.6—Date Schedule

Specifies specific dates when the UPQ is set to turn ON and OFF.

The UPQ can be turned ON or OFF (or both) on a specific date. Specify this date by entering the **Date (yyyy/mm/dd)**. The UPQ power state will be changed at the appropriate **Turn ON (hh:mm)** or **Turn OFF (hh:mm)** times.

**Warning will be initiated**—Allows connected systems with a monitoring service (such as ClientMate) to be shut down cleanly before UPQ shutdown.

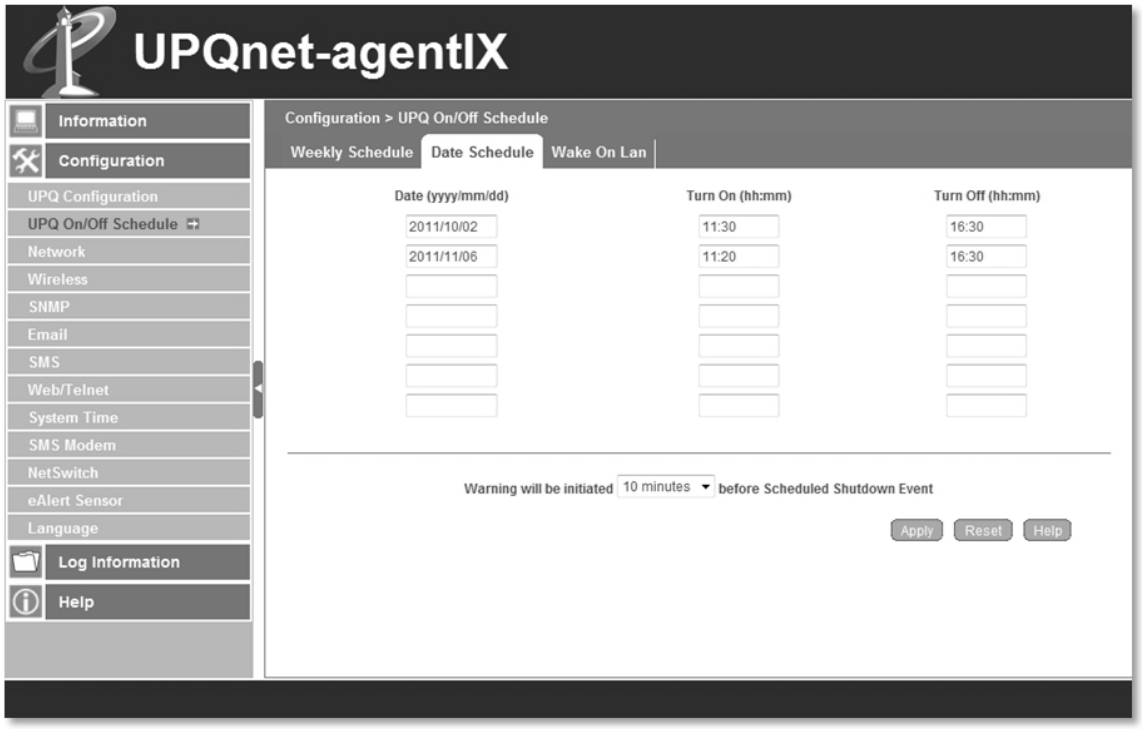



***Figure 37—Configuration→ON/OFF Schedule→Date Schedule***

Save all changes made on this screen by clicking **Apply**.

### 3.5.1.7—Wake on LAN

Set specific computers that will receive a Wake on LAN signal to turn ON or OFF when the UPQ is scheduled to turn ON or OFF (the computer must support and be configured for Wake on LAN):

Using the **Wake on LAN** function, turn ON a computer connected to the UPQ by entering the IP address of the computer to be turned ON in the **Host1** field. The MAC address of the computer to be turned ON will be automatically populated after the setting has been applied.


***Figure 38—Configuration→UPQ ON/OFF Schedule→Wake On LAN***

Test the Wake on LAN signal by sending it to a specific computer. Send this signal by clicking **Test**. The computer must support Wake on LAN and be configured to accept Wake on LAN commands for the test to succeed.

**Warning will be initiated**—Allows connected systems with a monitoring service (such as ClientMate) to be shut down cleanly prior to UPQ shutdown.

Save changes made in this screen by clicking **Apply**.

## 3.5.2—Network

These screens provide tools for modifying the NetAgent wired (Ethernet) network communication settings. Network settings can also be configured using Netility.

---

Manual Helps

For more information about configuring network settings with Netility, see **3.1.3—Using Netility to Modify Network Settings**.

---

### 3.5.2.1—IP Address

Specify the IP allocation method (DHCP, Bootp, or manual) and the IP network settings:

**Obtain an IP address**—Determines how the NetAgent obtains an IP address. The **IP Address**, **Subnet Mask**, and **Gateway** fields are enabled for a Manual assigned IP address.

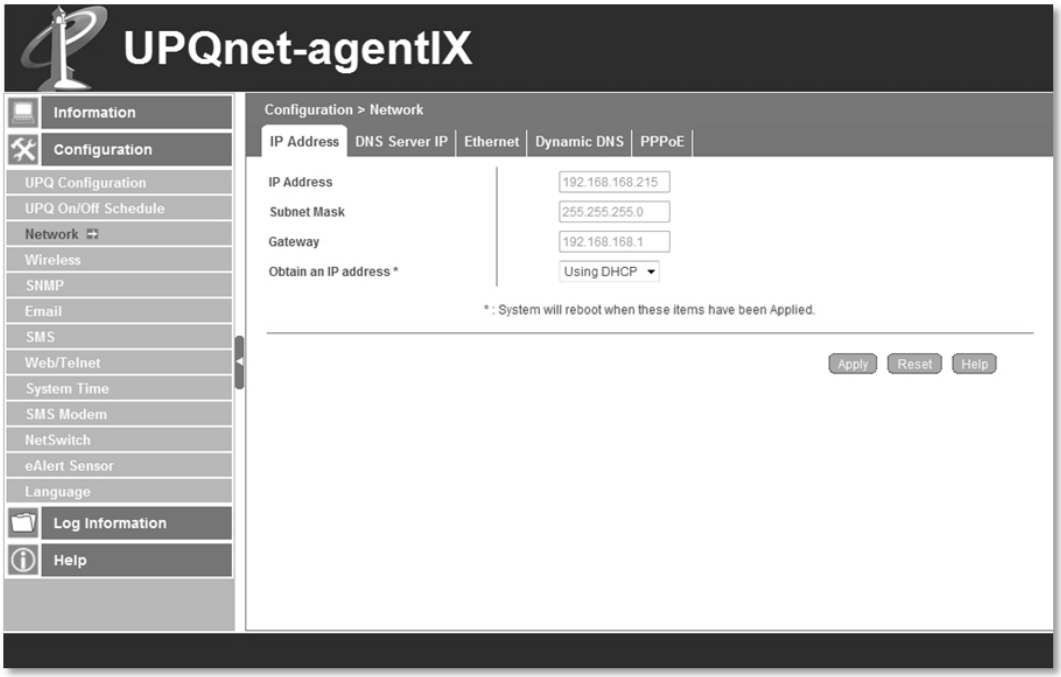



***Figure 39—Configuration→Network→IP Address***

Save all changes made on this screen by clicking **Apply**.

The NetAgent must reboot to change the IP address assignment method. The NetAgent will reboot when **Apply** is pressed.

---

Manual Helps

For definitions of technical terms, see **Appendix A—Glossary**.

---

### 3.5.2.2—DNS Server IP

Specifies the IP address of the primary and secondary DNS servers if IP allocation is being selected manually.

The DNS server IP addresses can only be modified with **Manual** IP allocation.

Save all changes made on this screen by clicking **Apply**.


***Figure 40—Configuration→Network→DNS Server IP***

Manual Helps

For definitions of technical terms, see **Appendix A—Glossary**.

### 3.5.2.3—Ethernet

Select whether to automatically detect the network type or specify a network type.

**Connection Type**—Can be used to specify speed for the Ethernet connection. The NetAgent can also **Auto Sense** the interface for the Ethernet connection.

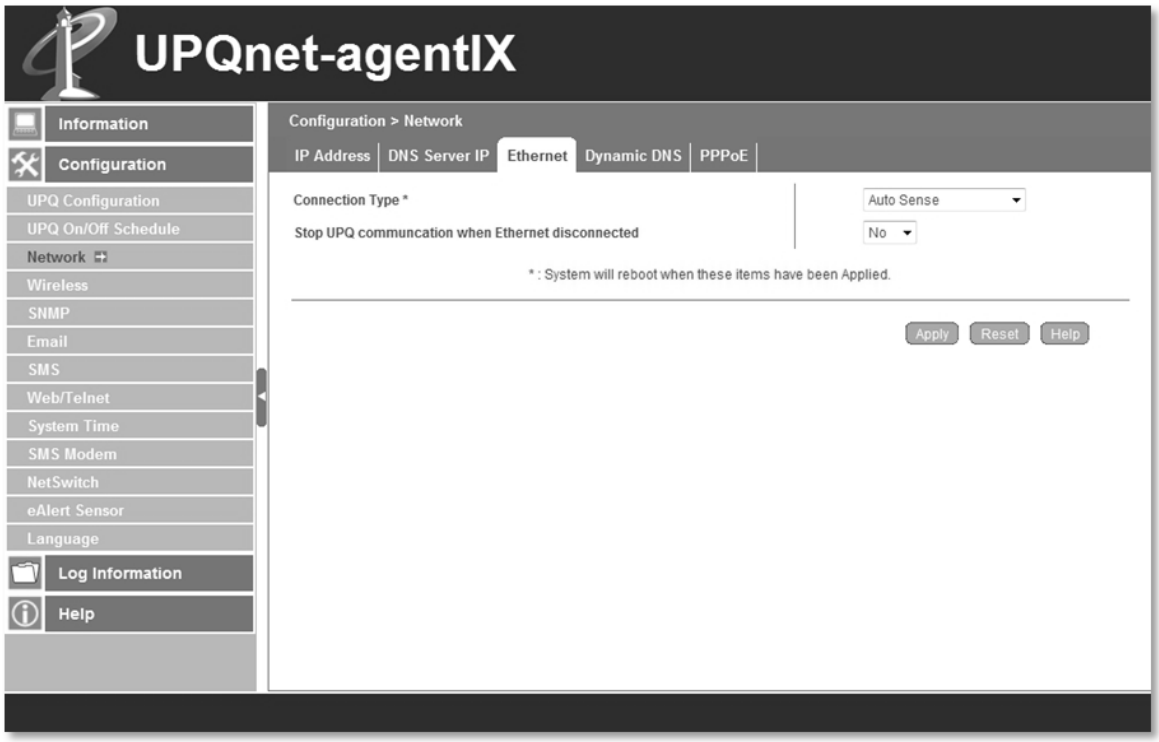



***Figure 41—Configuration→Network→Ethernet***

Save all changes made on this screen by clicking **Apply**.

The NetAgent must reboot to apply a change to this setting. The NetAgent will reboot after **Apply** has been clicked.

### 3.5.2.4—Dynamic DNS

Specify an optional dynamic DNS service to assign the NetAgent a domain name while using DHCP to assign the IP address.

Select a Dynamic DNS **Service Provider**, and enter individual account settings for that provider in the fields.


***Figure 42—Configuration→Network→Dynamic DNS***

Save all changes made on this screen by clicking **Apply**.

### 3.5.2.5—PPPoE

Specify settings for allowing Point-to-Point Protocol over Ethernet (PPPoE) connections between the NetAgent and a DSL modem (to allow remote access to the NetAgent through the DSL modem) or other PPPoE device.


***Figure 43—Configuration→Network→PPPoE***

Make a connection to a PPPoE modem by selecting **Connect Always** for **When Connection should be made**. Enter the **Login Name** and **Login Password** for the PPPoE modem.

Save all changes made on this screen by clicking **Apply**.

---

Manual Helps

For definitions of technical terms, see **Appendix A—Glossary**.

---

## 3.5.3—Wireless

These screens provide tools for modifying the NetAgent wireless (802.11 b/g) network communication settings.

### 3.5.3.1—AP Setting

Specify an 802.11 wireless network and settings for the connection.

Select a specific wireless network by clicking on the radio button beside the SSID of the desired network and clicking **Select**.

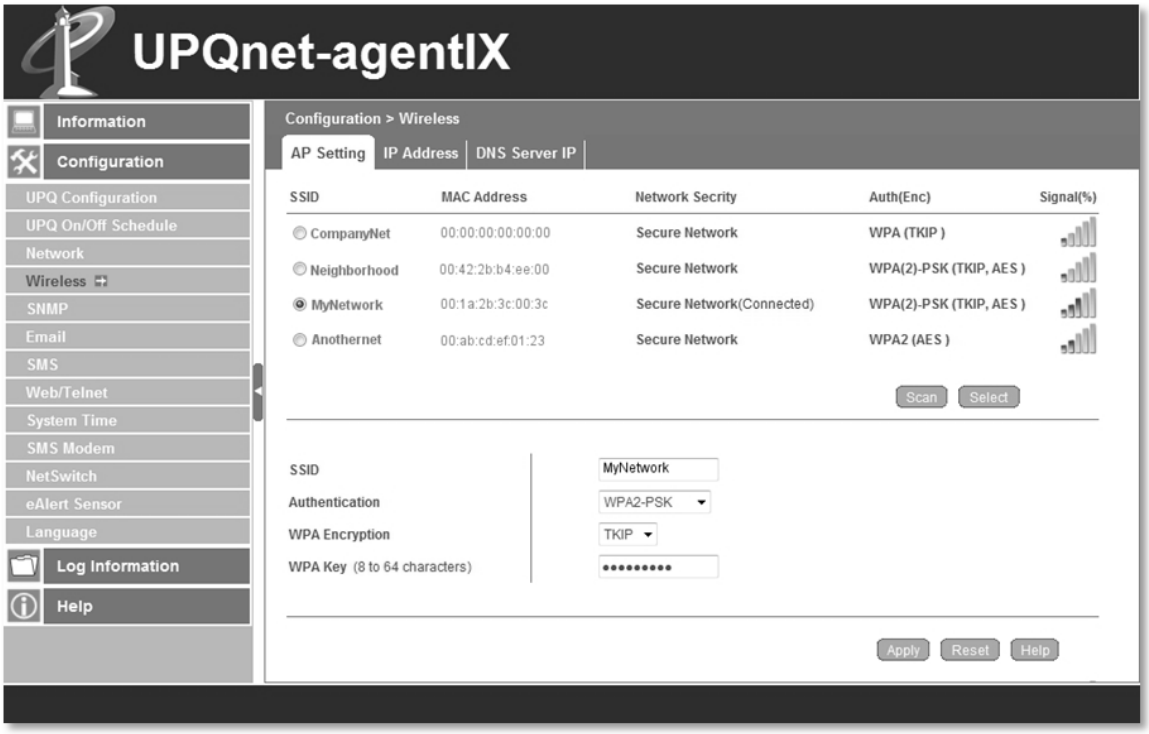



***Figure 44—Configuration→Wireless→AP Setting***

Click **Scan** to update the list of SSIDs if the desired wireless network is not visible.

If the SSID is not being broadcasted by the router or if the NetAgent is unable to detect the network, manually enter the **SSID**, **Authentication** method, and **WPA Encryption** method.

If the desired network uses WPA encryption, the encryption key must be entered in the **WPA Key** field.

Save all changes made on this screen by clicking **Apply**.

Manual Helps

For definitions of technical terms, see **Appendix A—Glossary**.

### 3.5.3.2—IP Address

If IP address allocation has been set manually, the **Obtain an IP Address** method should be set to **Manual**. Afterward, be sure to enter an **IP Address**, **Subnet Mask**, and **Gateway**.


***Figure 45—Configuration→Wireless→IP Address***

Save all changes made on this screen by clicking **Apply**.

If **Obtain an IP Address** method has been changed, the NetAgent will reboot when **Apply** is clicked.

---

Manual Helps

For definitions of technical terms, see **Appendix A—Glossary**.

---

### 3.5.3.3—DNS Server IP

Specify the IP address of the primary and secondary DNS servers if IP allocation has been selected manually.


***Figure 46—Configuration→Wireless→DNS Server IP***

The DNS server fields can be modified if the NetAgent is using manual IP allocation.

Save all changes made on this screen by clicking **Apply**.

---

Manual Helps

For definitions of technical terms, see **Appendix A—Glossary**.

---

## 3.5.4—SNMP

These screens provide tools for modifying the NetAgent SNMP identification and trap notification settings.

### 3.5.4.1—MIB System

Specify identifying SNMP device information for the NetAgent. SNMP monitoring devices such as SNMPView use the MIB entries to easily identify an individual NetAgent.

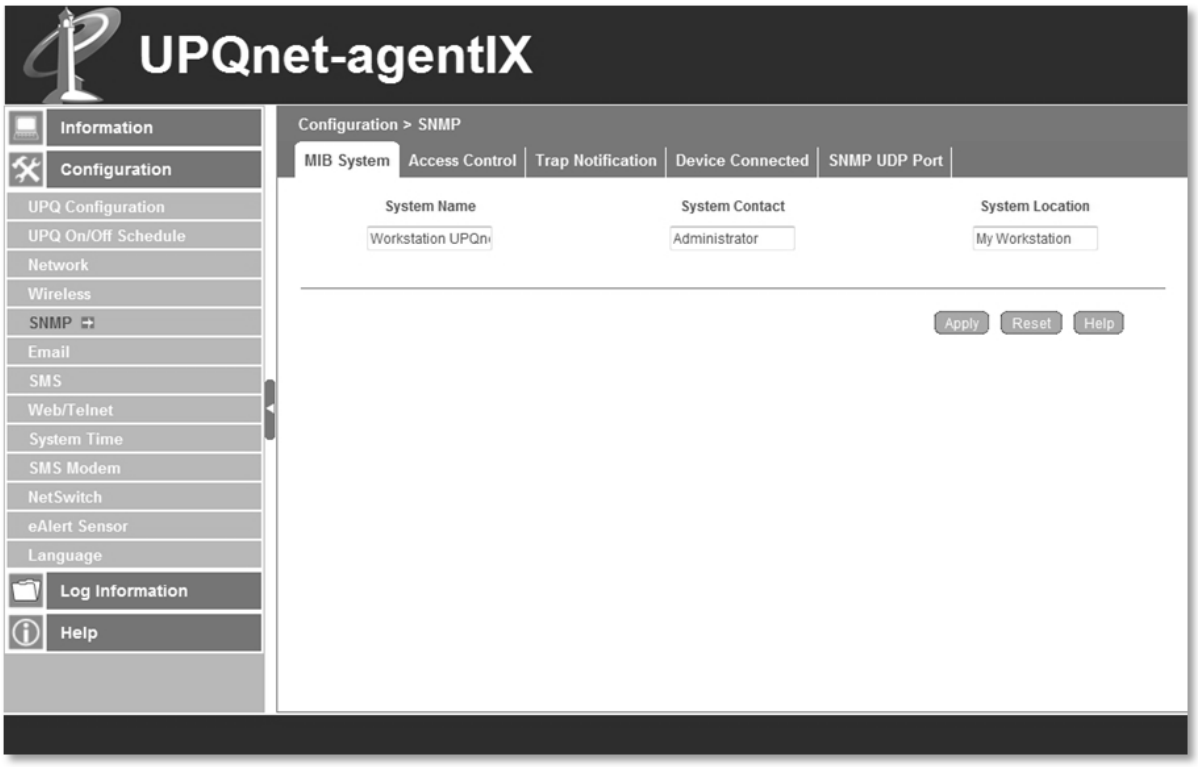



***Figure 47—Configuration→SNMP→MIB System***

The **System Name**, **System Contact**, and **System Location** are used to identify the NetAgent to other SNMP devices.

Save all changes made on this screen by clicking **Apply**.

### 3.5.4.2—Access Control

Specify specific computers with access permissions to manage the NetAgent using an SNMP client.

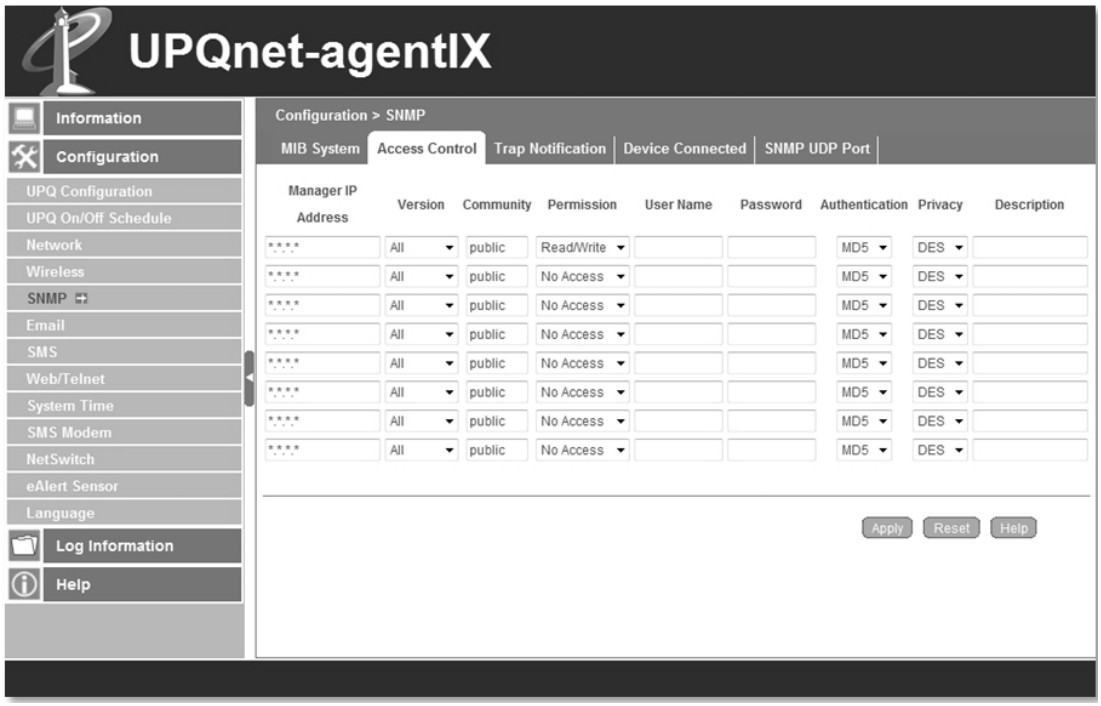



***Figure 48—Configuration→SNMP→Access Control***

If any devices are allowed to communicate with the NetAgent using SNMP, the **Manager IP Address** of the devices should be entered, along with the SNMP version and access rights for the device.

Save all changes made on this screen by clicking **Apply**.

---

Manual Helps

For definitions of technical terms, see **Appendix A—Glossary**.

---

### 3.5.4.3—Trap Notification

Specify the listening SNMP client devices to receive NetAgent trap notifications.

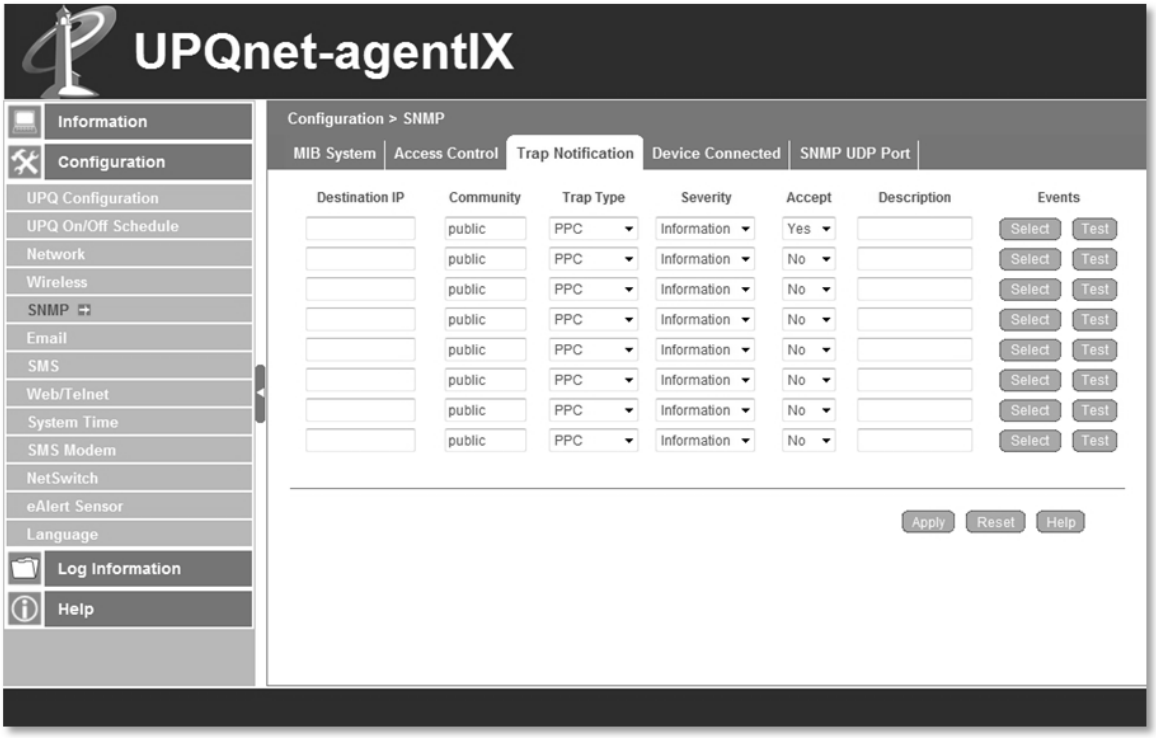



***Figure 49—Configuration→SNMP→Trap Notification***

By clicking **Select**, select which UPQ and e-Alert Sensor events will trigger the specified trap notifications.

### 3.5.4.4—UPQ Events

**Single-phase:** **3-Phase:**

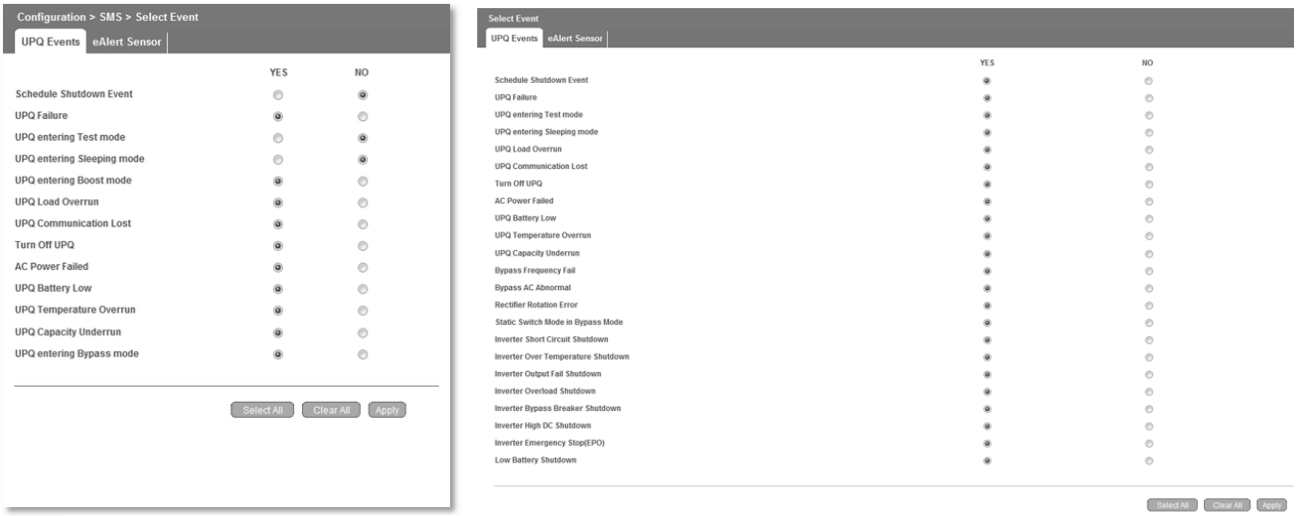



***Figure 50—Configuration→SMS→Select Event→UPQ Events***

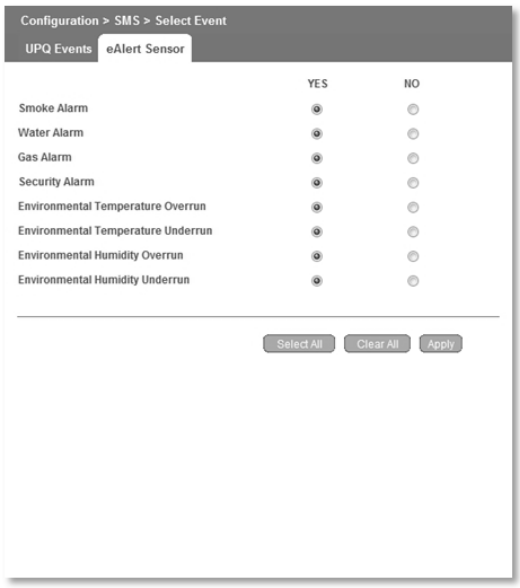



***Figure 51—Configuration SMS Select Event e-Alert Sensor***

Save changes in the pop-up windows by clicking **Apply**. Each pop-up window can be closed to return to the main **SNMP** device configuration screen.

Save all changes made in this screen by clicking **Apply**.

### 3.5.4.5—Device Connected

Specify connection and power use thresholds for SNMP devices connected to the UPQ.


***Figure 52—Configuration→SNMP→Device Connected***

### 3.5.4.6—SNMP UDP Port

Specify the SNMP port for the NetAgent and the port to listen for SNMP Read and Write trap events.

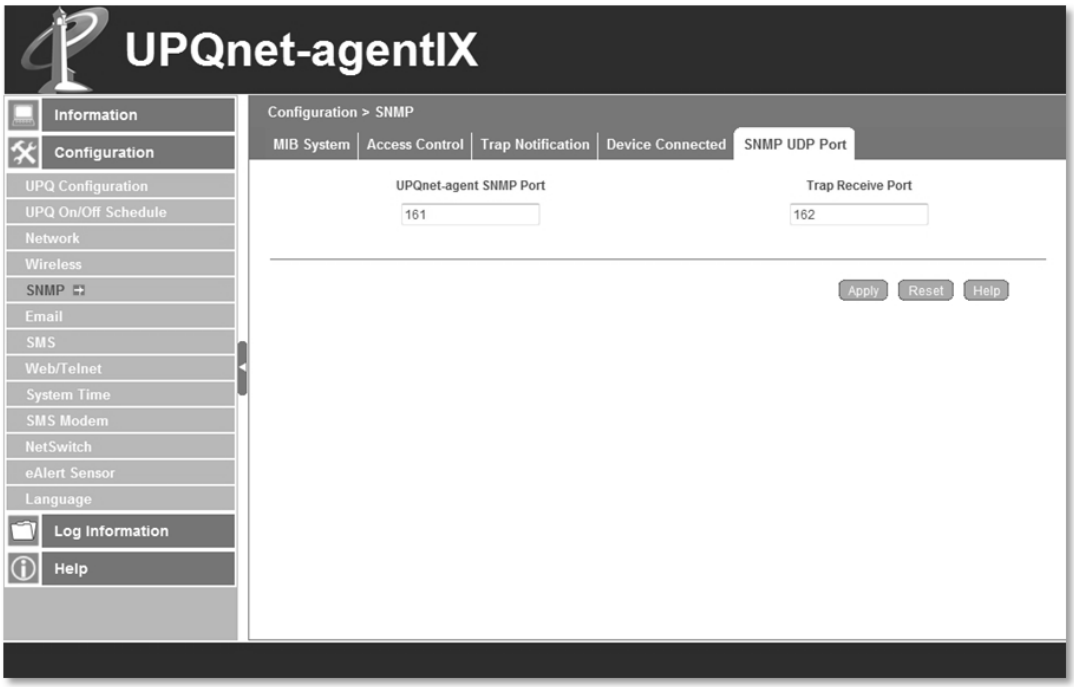



***Figure 53—Configuration→SNMP→SNMP UDP Port***

## 3.5.5—Email

These screens provide tools for configuring and scheduling email notification of NetAgent event information.

### 3.5.5.1—Email Setting

Specify the email account to use for sending email alert notifications.

The NetAgent must be configured to use a remote **Email Server** to send email notifications.

If the email server uses a non-standard port, the **Email Port** must be changed.


***Figure 54—Configuration→Email→Email Setting***

The **Sender's Email Address** that will be used in the email From: field must be specified.

If the remote mail server requires a valid user to send email message, the **Email Server Requires Authentication** option must be set to **YES**.

If the email server requires authentication, the **Account Name** should be entered. The **Password** to authenticate the specific user must also be entered.

Save changes made on this screen by clicking **Apply**.

Test the email server by specifying a test message in the **Sending test mail** field and clicking **Test Mail** (an email recipient must be specified in the **Email for Event Log** screen).

### 3.5.5.2—Email for Event Log

Specify email accounts to receive event notifications and to select which notifications should be included for each email account.

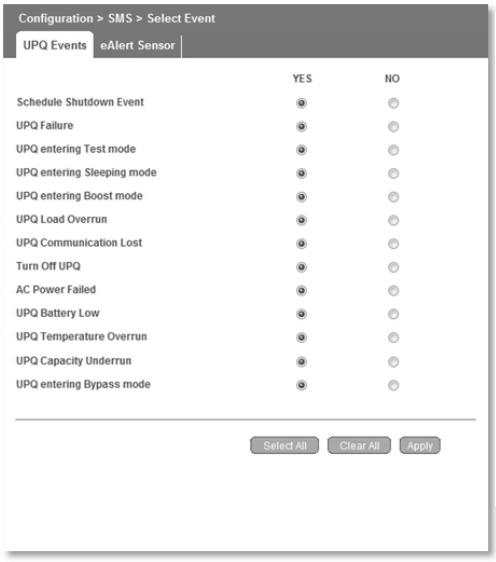
The NetAgent will send event notifications to email addresses listed in the **Account1** through **Account8** fields when the **Send Email When Event Occurs** option is set to **YES**.


***Figure 55—Configuration→Email→Email for Event Log***

Use the Select button to select which **UPQ Events** and **e-Alert Sensor** events will be sent for each individual email address:

### 3.5.5.3—UPQ Events

## Single-Phase




## 3-Phase

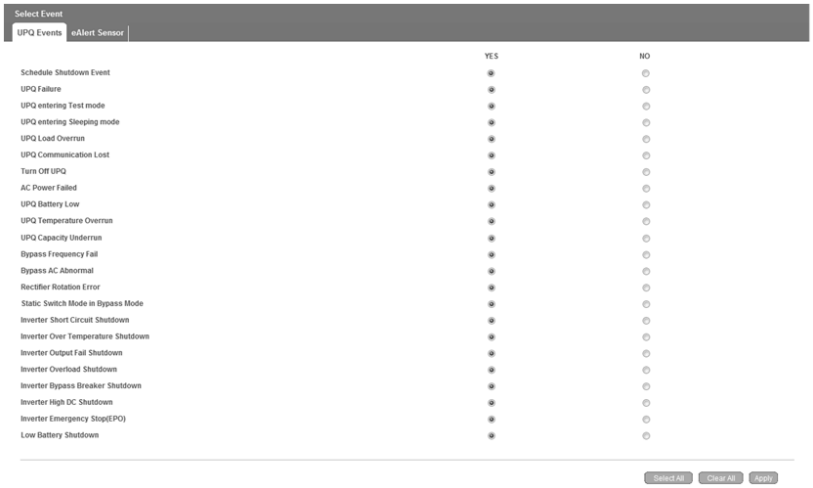



***Figure 56—Configuration→SMS→Select Event→UPQ Events***

### 3.5.5.4—e-Alert Sensor Events

Save all changes in the pop-up windows by clicking **Apply**. After changes are made, close the pop-up window to return to the main **Email** configuration screen.

Save all changes made on this screen by clicking **Apply**.

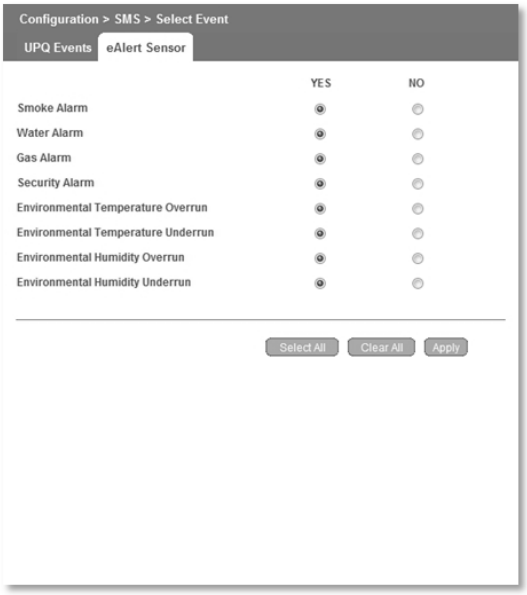



***Figure 57—Configuration→SMS→Select Event→e-Alert Sensor***

### 3.5.5.5—Email for Daily Report

Specify email accounts to receive a daily report containing the event and data log for the NetAgent.

Configure up to four email accounts to receive a daily UPQ activity report by entering the addresses in the **Account1**–**Account4** fields.

Set a daily report by selecting **YES** for **Send Email for Daily Report (hh:mm)** and entering a time when the email message should be sent.

**Send Email when Event/Data Log overflows**: When event or data logs overflow, email notifications will be sent. Old information in the logs will be overwritten by new entries. Copies of the log files can be downloaded from the **Log Information** screens.

Save all changes made on this screen by clicking **Apply**.


***Figure 58—Configuration→Email→Email for Daily Report***

## 3.5.6—SMS

These screens provide tools for configuring scheduled and event-based SMS notification. SMS notification requires an optional GPRS/GSM cellular modem attached directly to the NetAgent or to a monitoring PC running SMS Server.

Manual Helps

For more information on using an optional GPRS modem with the NetAgent, see **8.3—GPRS Modem**.

### 3.5.6.1—SMS Setting

Specify how and when to send SMS alerts.

If a GPRS modem is connected directly to the NetAgent, the **Use Local Modem** option should be selected for **Send SMS When Event Occurs**. The **Use Remote Service** option can be selected to have the NetAgent connect to a PC running SMSServer to send text message notifications.

If the messages will be sent from a remote server, the **SMS Server** IP address, **SMS Port**, and **Account Name** and **Password** (if necessary) to connect to SMSServer must be entered.


***Figure 59—Configuration→SMS→SMS Setting***

Use the **Sending test SMS** field to enter a test SMS message to the phone number(s) configured on the **Mobile for Event Log** screen. Click **Test SMS** to send the test message.

Save all changes made on this screen by clicking **Apply**.

### 3.5.6.2—Mobile for Event Log

Specify which mobile numbers receive alerts and what type of alert each phone number should receive.

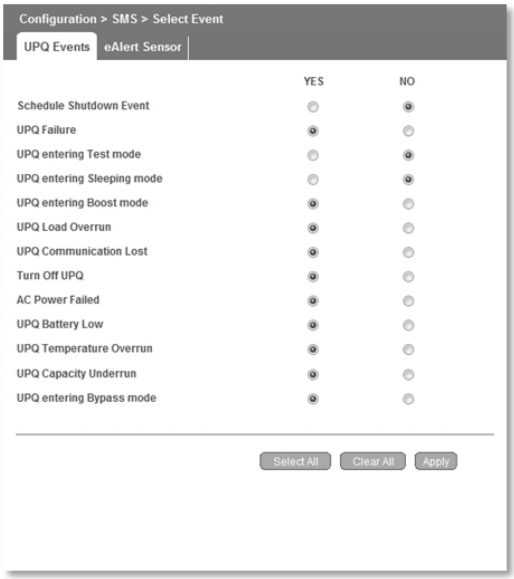
11-digit (1+Area Code + Prefix + Number, e.g. 1958550142) numbers that will receive a text message when an event occurs should be entered in the **Cellular Phone Number1** through **Cellular Phone Number8** fields.


***Figure 60—Configuration→SMS→Mobile for Event Log***

**UPQ Events** and **e-AlertSensor** events that will be sent for each individual cell phone number can be specified by clicking the appropriate **Selec**t button.

### 3.5.6.3—UPQ Events

**Single-Phase** **3-Phase**



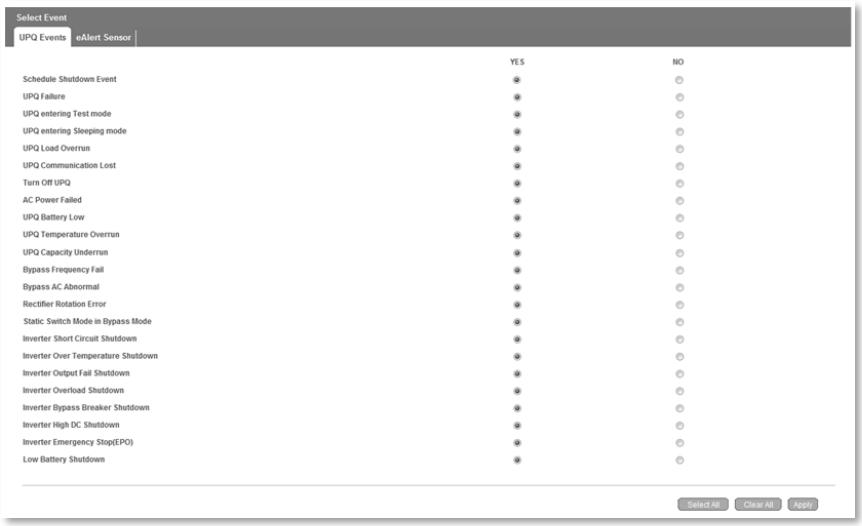




***Figure 61—Configuration→SMS→Select Event→UPQ Events***

### 3.5.6.4—e-Alert Sensor Events

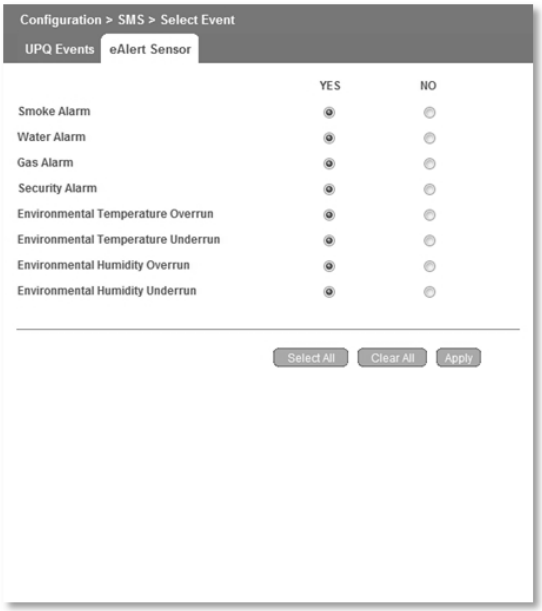



***Figure 62—Configuration→SMS→Select Event→e-Alert Sensor***

Save all changes made in pop-up windows by clicking **Apply**. The pop-up window can be closed to return to the main **SMS** notification screen.

Save all changes made on this screen by clicking **Apply**.

## 3.5.7—Web/Telnet

These screens provide tools for configuring security restrictions for remote connections to the NetAgent management interface.

### 3.5.7.1—User Account

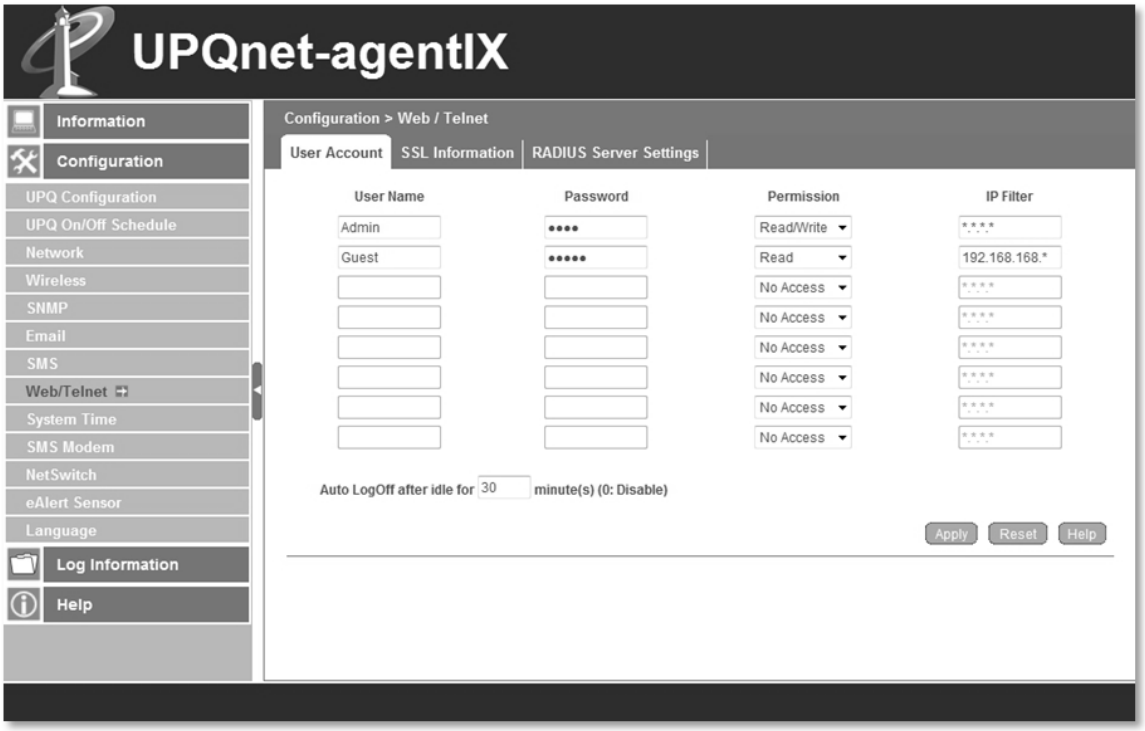



***Figure 63—Configuration→Web/Telnet→User Account***

Specifies individual user accounts and computers with permission to connect to the NetAgent.

The web interface can be set to require authentication for access. To set **Permissions**, enter a **User name** and **Password** and select whether the user will have full read/write permission to modify the NetAgent Settings. If not selecting full **Read/Write** permission, select **Read** to view information but not modify settings.

Enter an **IP Filter** to limit which computers can be used to access the NetAgent using each account. An IP Filter may specify an individual IP address, a block of IP addresses (see the Guest account in the picture above), or from any IP address (*.*.*.*).

At least one account should always be assigned **Read/Write** permission. Otherwise, update settings cannot be changed even when it becomes necessary.

Save all changes made on this screen by clicking **Apply**.

When **Apply** has been clicked, the web server may require the username and password to be entered again for one of the configured accounts.

Manual Helps

For definitions of technical terms, see **Appendix A—Glossary**.

### 3.5.7.2—SSL Information

Upload Secure Socket Layer (SSL) credentials for the NetAgent to use for the secure (https://) network communication.

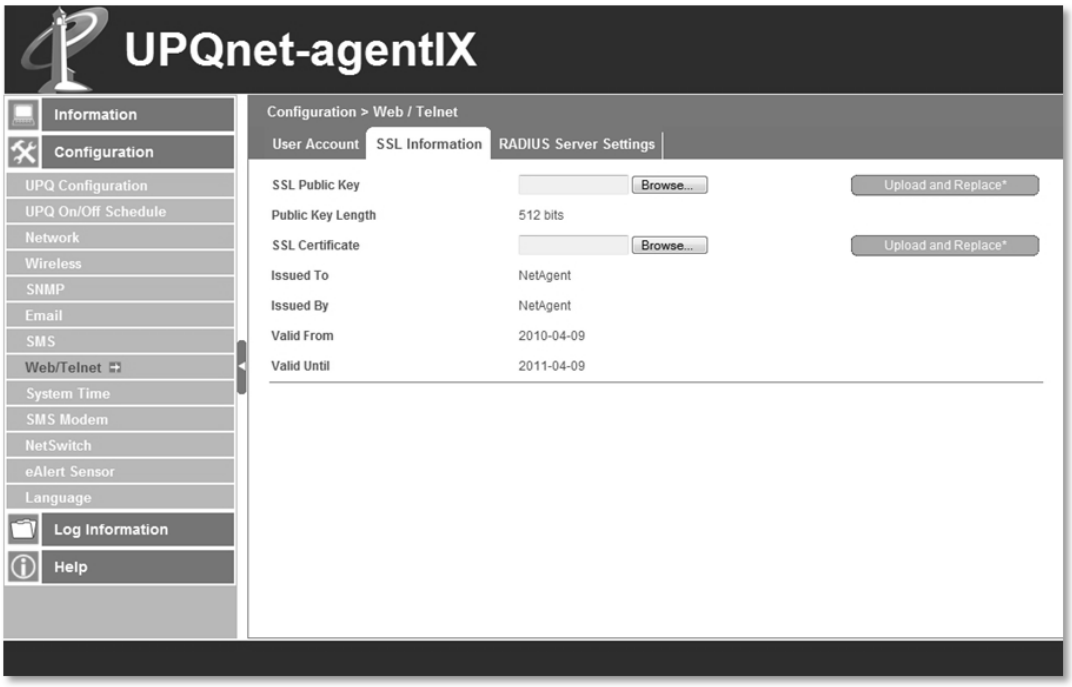



***Figure 64—Configuration→Web/Telnet→SSL Information***

The NetAgent has a built-in, self-assigned **SSL Public Key** and **SSL Certificate** that will be used when secure (https://) connections are made to the web interface. A self-signed certificate creates a security warning in most browsers and may require special actions to access the web interface.

It is possible to purchase and upload a signed certificate from a trusted Certificate Authority (such as GoDaddy, Comodo, or VeriSign) to avoid security warnings.

Manual Helps

See **3.10—Installing a New SSL Certificate** for more information about SSL certificates.

If desired, replace the **SSL Public Key** by clicking **Browse…** to select the key file on the local computer, then clicking **Upload and Replace** to upload the new SSL public key to NetAgent.

If desired, replace the signed **SSL Certificate** by clicking **Browse…** to select the file on the local computer. Click **Upload and Replace** to upload the new SSL certificate to the NetAgent.

Manual Helps

For definitions of technical terms, see **Appendix A—Glossary**.

### 3.5.7.3—RADIUS Server Settings

Configure the NetAgent to use RADIUS secure connections. RADIUS (Remote Authentication Dial-In User Service) is a secure method for centralized network authentication access multiple systems.

If the NetAgent should use a RADIUS server for network authentication, set **Enable RADIUS in Web/Telnet login** to **YES**.

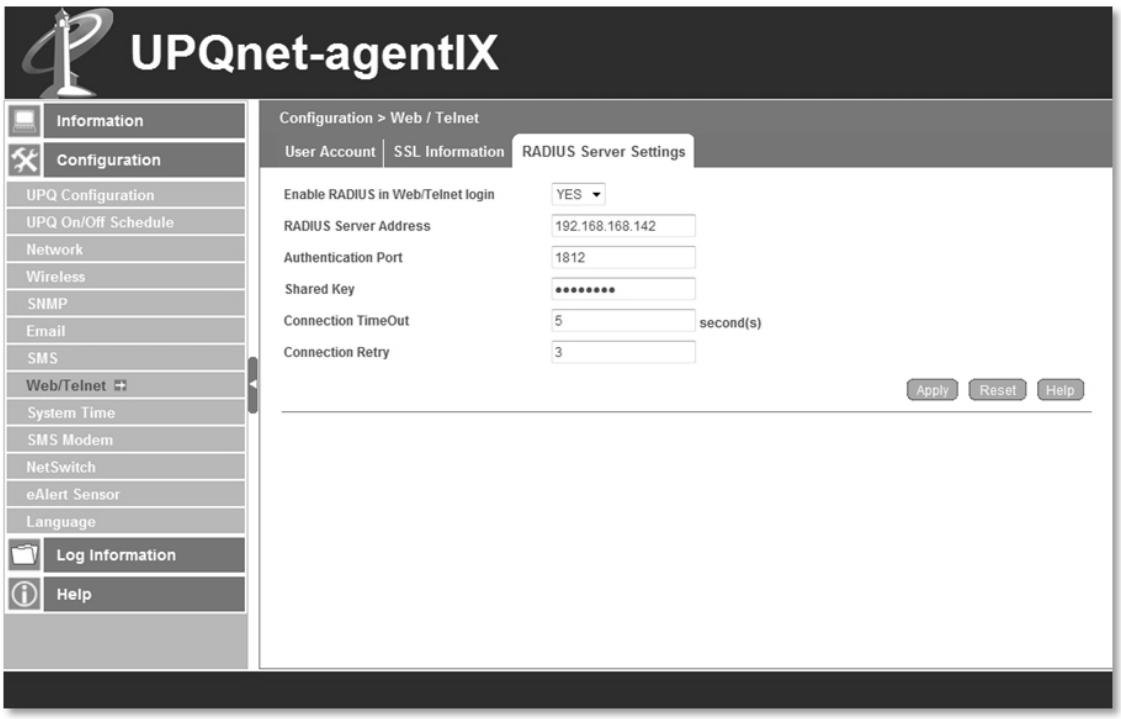



***Figure 65—Configuration→Web/Telnet→RADIUS Server Settings***

Enter the **Shared Key** for connecting to the RADIUS server.

If necessary, change **Connection TimeOut** and **Connection Retry** intervals to longer or shorter times.

Save changes made on this screen by clicking **Appl**y.

## 3.5.8—System Time

These screens provide tools for configuring the NetAgent to use a time server to manage the device system time clock.

### 3.5.8.1—System Time

Configure the NetAgent to use a web time server to maintain the system clock.

The NetAgent can automatically set the system time. To set this feature, select the **Time Between Automatic Updates** and the **Time Server** that will provide the correct time.

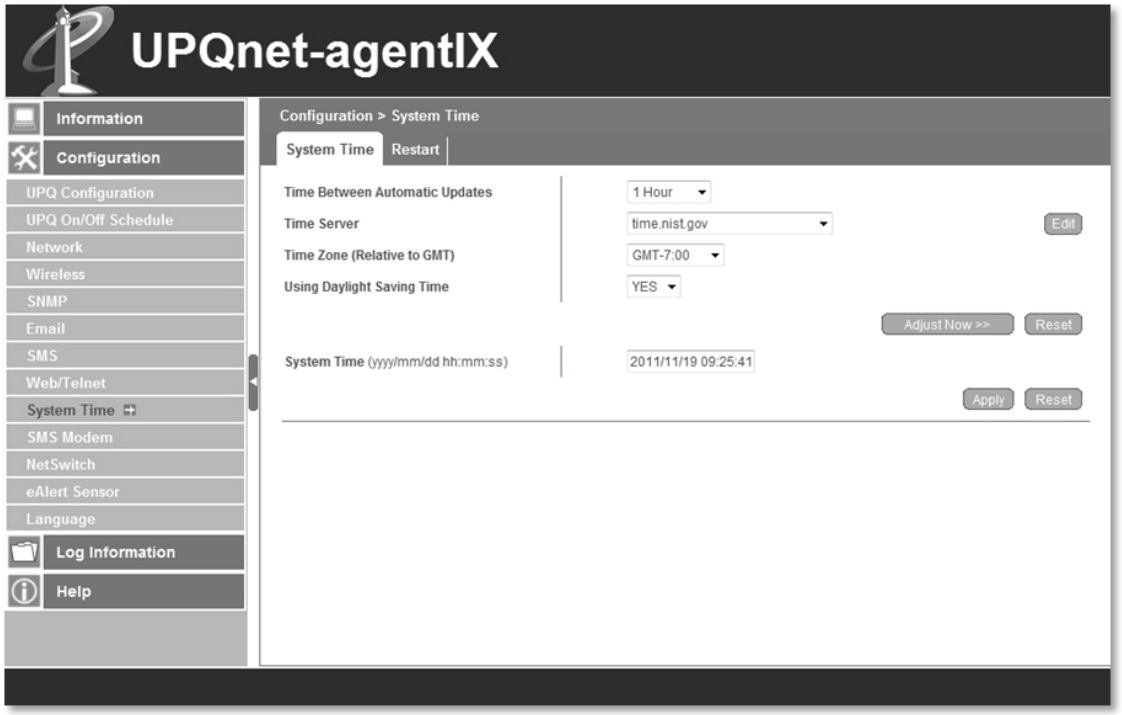



***Figure 66—Configuration→System Time***

Add a custom timeserver to the list of clicking **Edit**, entering the domain name of the new server, and clicking **Add**. Clicking **Back** will return to the main **System Time** screen.

Specify the **Time Zone** and whether to **Use Daylight Time**. This entry is very important.

Press **Adjust Now**>> to set the NetAgent clock using the selected time server.

Save all changes made on this screen by clicking **Apply**.


***Figure 67—Configuration→System Time→Add Server→Time Server***

### 3.5.8.2—Restart

Specify a duration after which the NetAgent will automatically reboot if it has been operating continuously for a specified interval.


***Figure 68—Configuration→System Time→Restart***

If the NetAgent should be restarted after it has been running continually for a specific time, the desired period should be entered in the **Auto Restart System for Every** field. If the period is set to 0, the NetAgent will not automatically restart. Click the top **Apply** button to save changes to the reboot interval.

The NetAgent can be manually forced to reboot by clicking **Apply** for **Manually Reboot System After 30 Seconds**. Manually rebooting will shut down and restart the UPQ 30 seconds after the **Apply** button has been clicked.

## 3.5.9—SMS Modem

These screens provide tools for configuring the connection to an optional GPRS/GSM cellular modem. These settings only apply if the modem is connected directly to the NetAgent.

Manual Helps

See **8.3—GPRS Modem** for more information about using an optional GPRS modem with the NetAgent.

### 3.5.9.1—SMS Modem Settings

Configure the connection between the NetAgent and the GPRS modem.

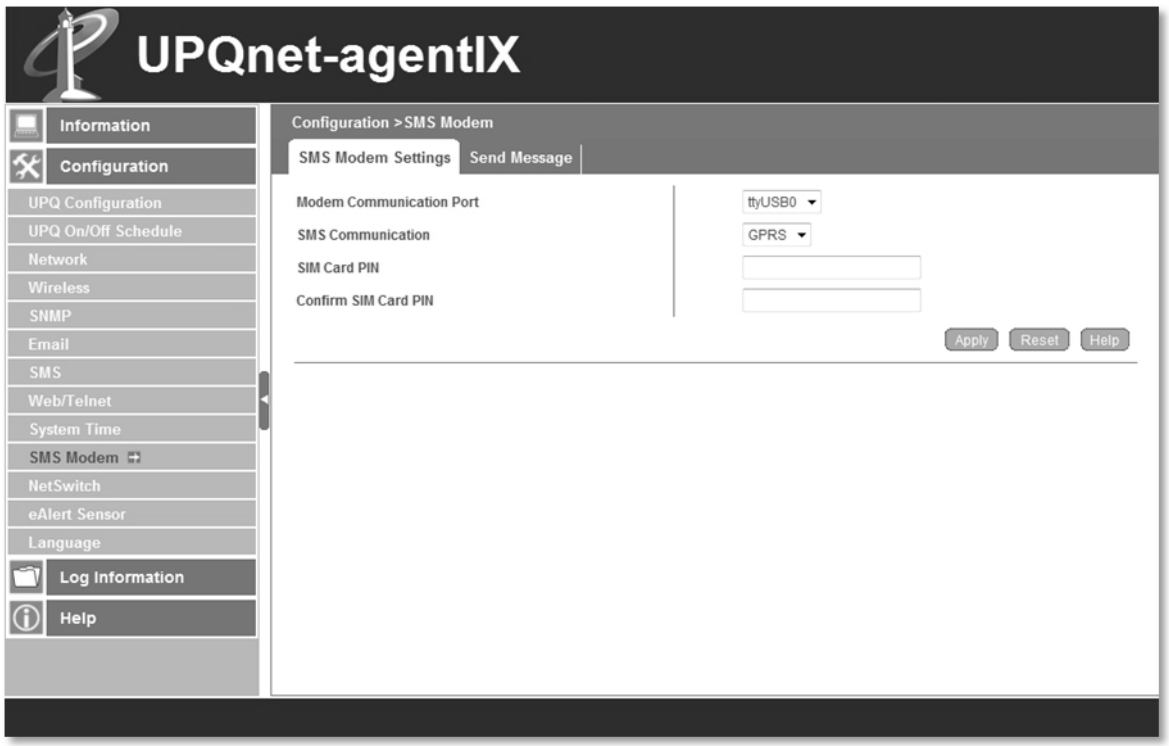



***Figure 69—Configuration→SMS Modem→SMS Modem Settings***

Use **Modem Communication Port** to specify a specific COM port that the NetAgent will use to communicate to GPRS modem.

If the modem supports multiple **SMS Communication** methods, select the preferred method.

Use **SIM Card PIN** and **Confirm SIM Card** if one is configured for the SIM card being used by the modem. If the SIM card PIN is wrong, the modem will be unable to send SMS messages.

Save all changes made on this screen by clicking **Apply**.

### 3.5.9.2—Send Message

Send a test SMS message from the GPRS modem to a specified phone. Test that the SMS modem is working and properly configured after it has been installed.

Send a test message by entering the 11-digit (1 + Area Code + Prefix + Number e.g. 19585550142) **Cellular Phone number**, entering a message in the **SMS content** field, and clicking **Send**. If the full 11-digit number is not used, the message will not be sent successfully.

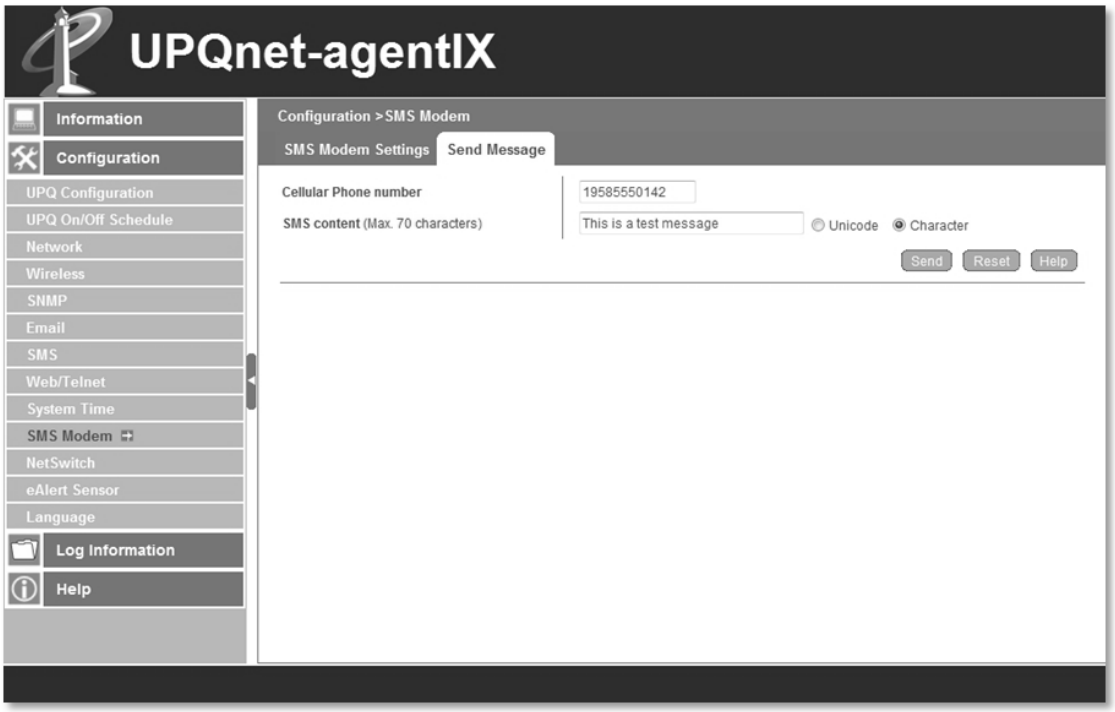



***Figure 70—Configuration→SMS Modem→Send Message***

## 3.5.10—NetSwitch

These screens provide tools for managing NetSwitch (remotely controlled power outlet) devices connected to the NetAgent.

### 3.5.10.1—NetSwitch

Specify NetSwitch action triggers from UPQ events.

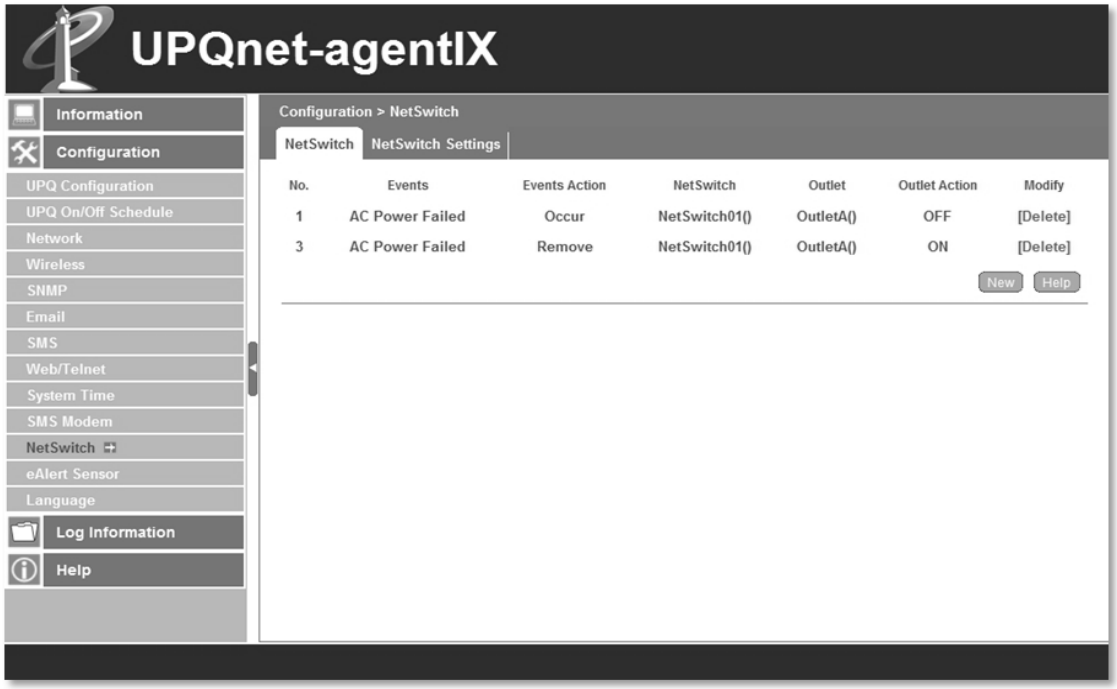



***Figure 71—Configuration→NetSwitch***

Event actions for the NetSwitch can be added by clicking **New** to open a window and selecting the UPQ or e-Alert Sensor event, whether the event begins (**Occur**) or ends (**Remove**), and whether the switch should turn **ON** or **OFF**. Click **Apply** to save the event and create a new one or close the window to return to the main screen.


***Figure 72—Configuration→NetSwitch Action→NetSwitch Action Configuration***

A current action for the NetSwitch can be removed by clicking **Delete**.

### 3.5.10.2—NetSwitch Settings

Configure the connection between the NetAgent and the NetSwitch.

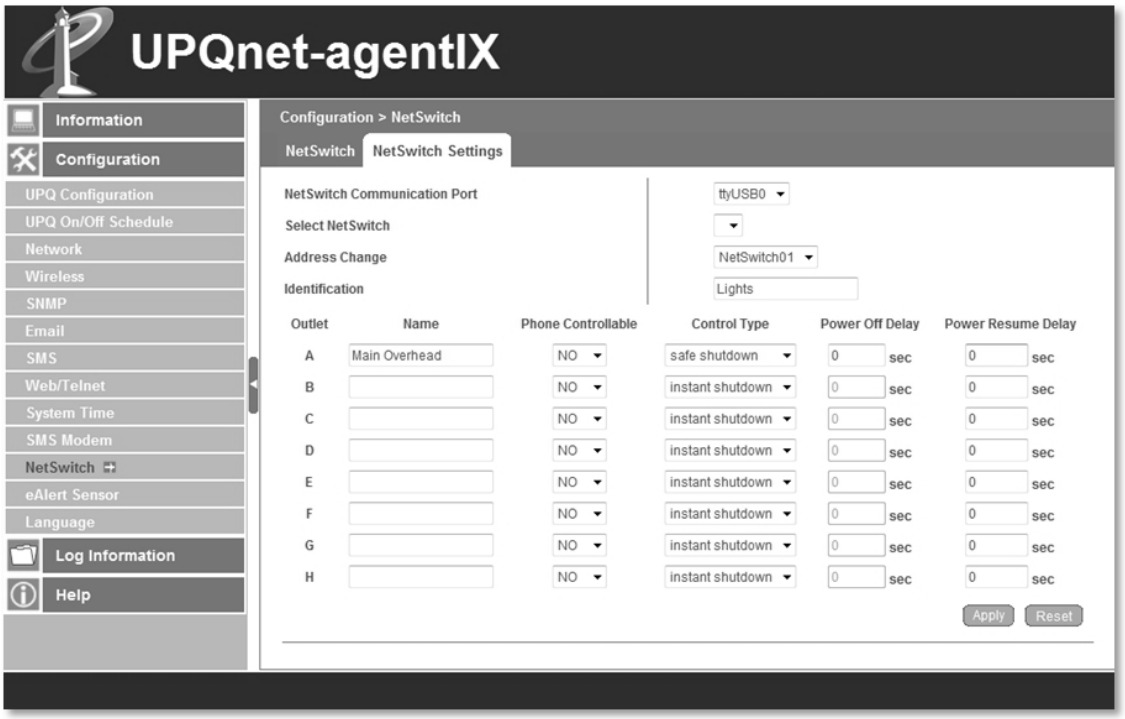



***Figure 73—Configuration→NetSwitch→NetSwitch Settings***

## 3.5.11—e-Alert Sensor

These screens provide tools for configuring the notification settings for the optional e-Alert Sensor if it is connected to the NetAgent. For more information, see **e-Alert Sensor** in the **Optional Add-ons** section of this manual.

### 3.5.11.1—e-Alert Sensor

Specifies alert threshold levels for humidity and temperature readings from the e-Alert Sensor.

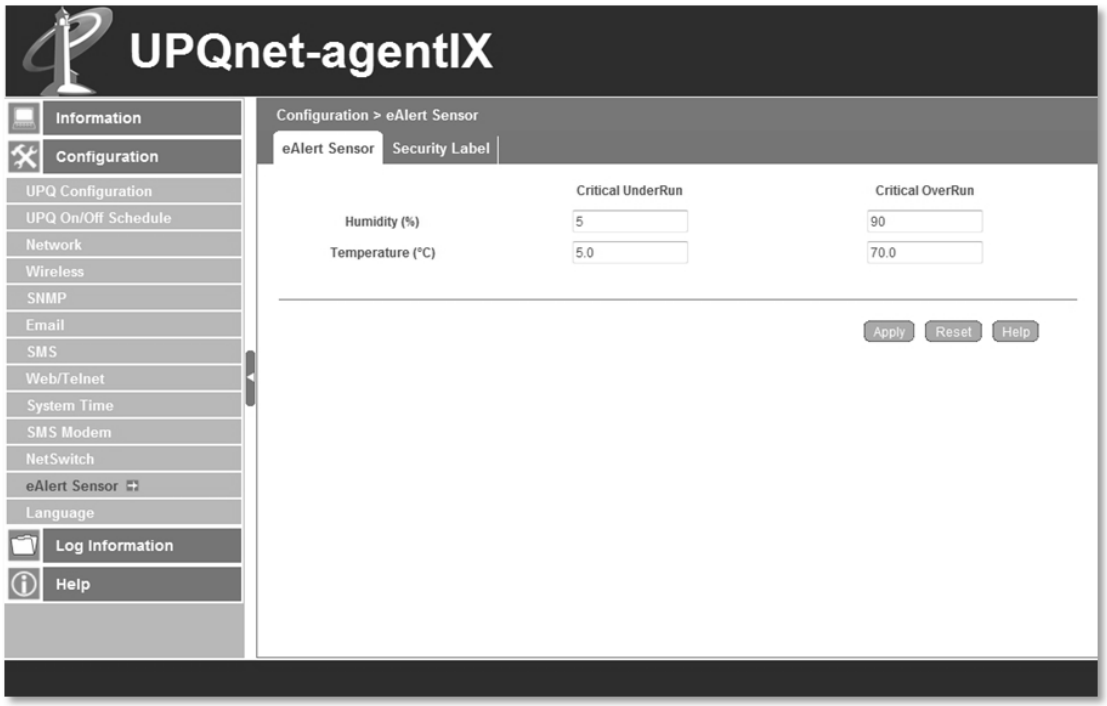



***Figure 74—Configuration→e-Alert Sensor***

The minimum (**Critical UnderRun**) and maximum (**Critical OverRun**) safe operating **Humidity (%)** and **Temperature (°C)** for the UPQ and the systems connected to it should be specified. The NetAgent will send an event notification if the e-Alert Sensor measurements leave the safe range.

Save all changes made on this screen by clicking **Apply**.

### 3.5.11.2—Security Label

Specify custom names for window/door perimeter sensors connected to the e-Alert Sensor.

An alternate name for any of the seven additional perimeter alarm sensors connected to the e-Alert Sensor can be configured using this screen. The alternate names will be used in any log entries or notifications (SMS, email, or SNMP) about an event.


***Figure 75—Configuration→e-Alert Sensor→Security Label***

Save changes made on this screen by clicking **Apply**.

## 3.5.12—Language

These screens provide options for the language used in the NetAgent web interface.

### 3.5.12.1—Interface Language

Specify the language to use in the NetAgent web interface.


***Figure 76—Configuration→Language→Interface Language***

### 3.5.12.2—Email Preferences


***Figure 77—Configuration→Language→Email Preferences***

Specify the language to use in email notifications sent by the NetAgent.

# 3.6—Log Information

The **Log Information** section provides access to view, save, and clear event, data, and test logs for the UPQ and e-Alert Sensor (if installed).

## 3.6.1—Event Log

This screen displays the history of any notification events from the NetAgent and any connected devices.

Download and save a copy of the event on the local computer in a comma-delimited (.csv) file by clicking **Save**. The log can be emptied by clicking **Clear**.

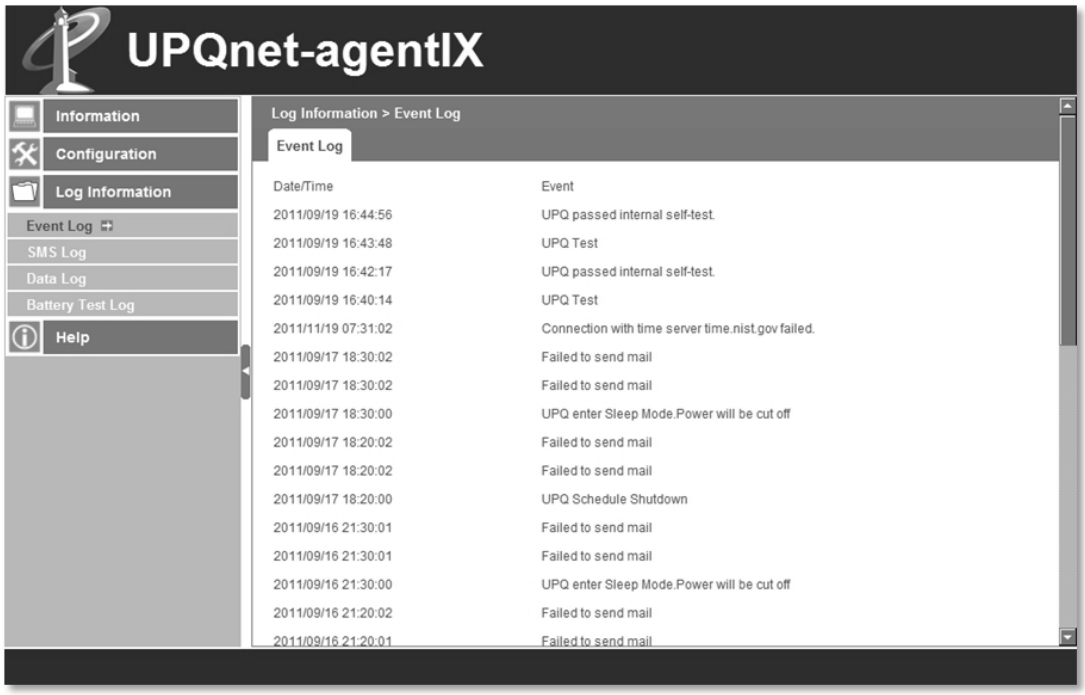



***Figure 78—Log Information→Event Log***

### 3.6.2—SMS Log

This screen displays the history of any SMS notifications sent by the NetAgent.

Clear this log by clicking **Clear**.

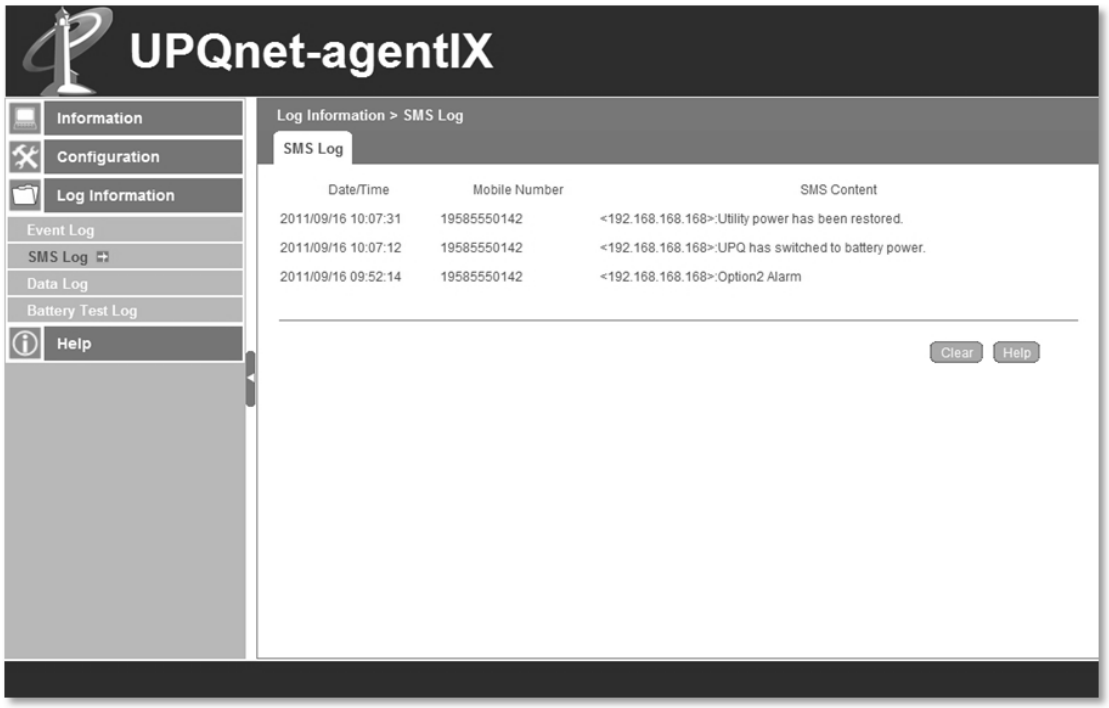
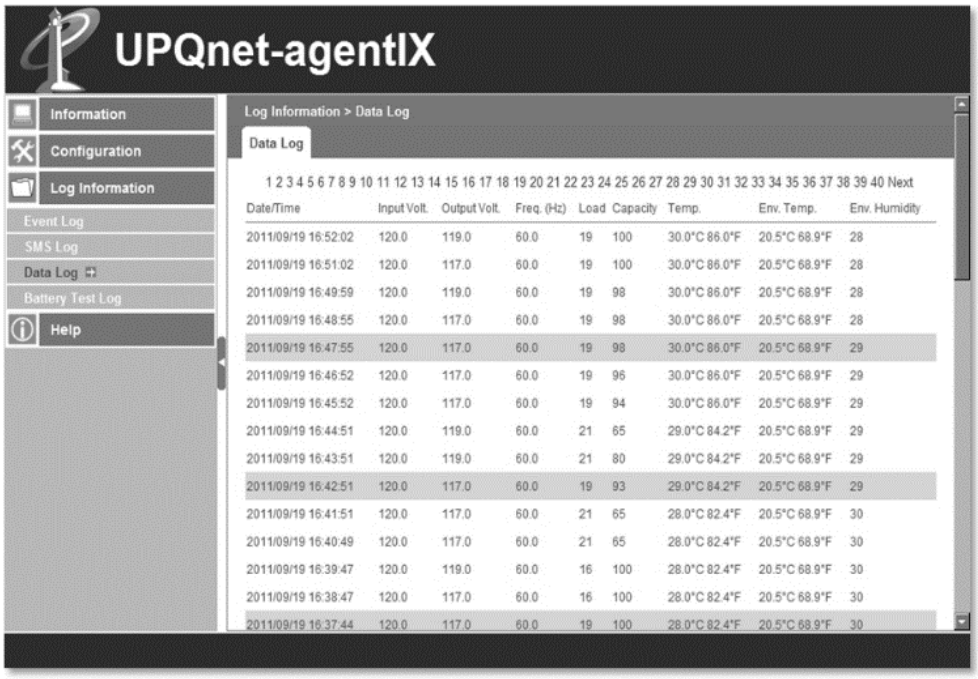



***Figure 79—Log Information→SMS Log***

### 3.6.3—Data Log

This screen displays the periodic history of sensor readings from the UPQ and optional e-Alert Sensor, if installed.

**Single Phase**




**3-Phase**

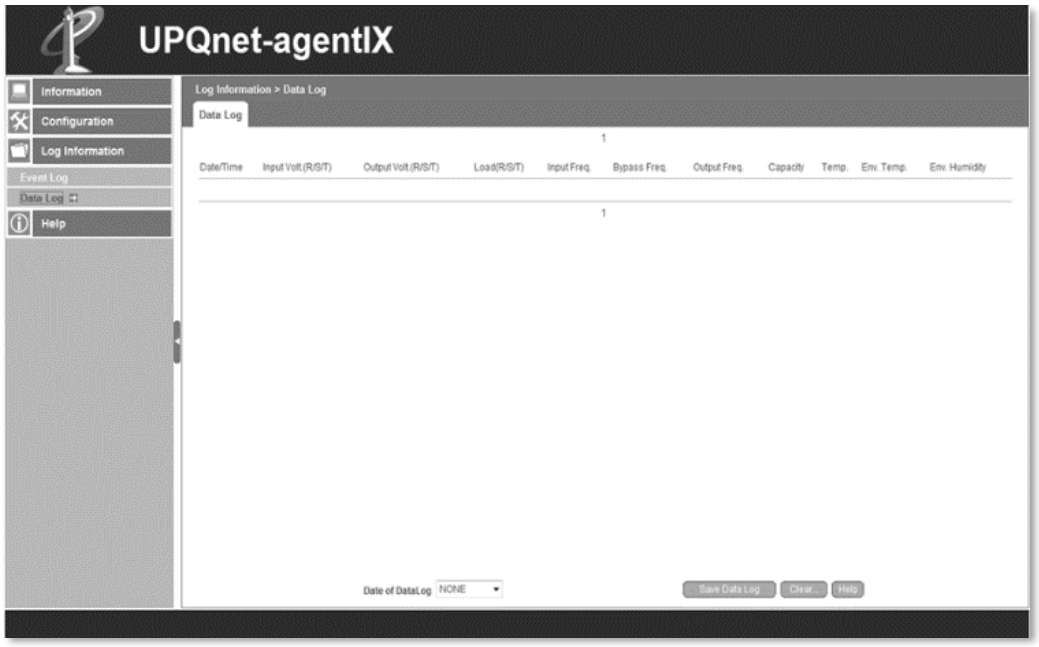



***Figure 80—Log Information→Data Log***

Download and save a copy of the data log on the local computer in a comma-delimited (.csv) file by clicking **Save**. Empty the log by clicking **Clear**.

### 3.6.4—Battery Test Log

This screen shows the two most recent test times and durations.

A log graph displays the system load and battery capacity during each test. It can be viewed by clicking on the individual test.

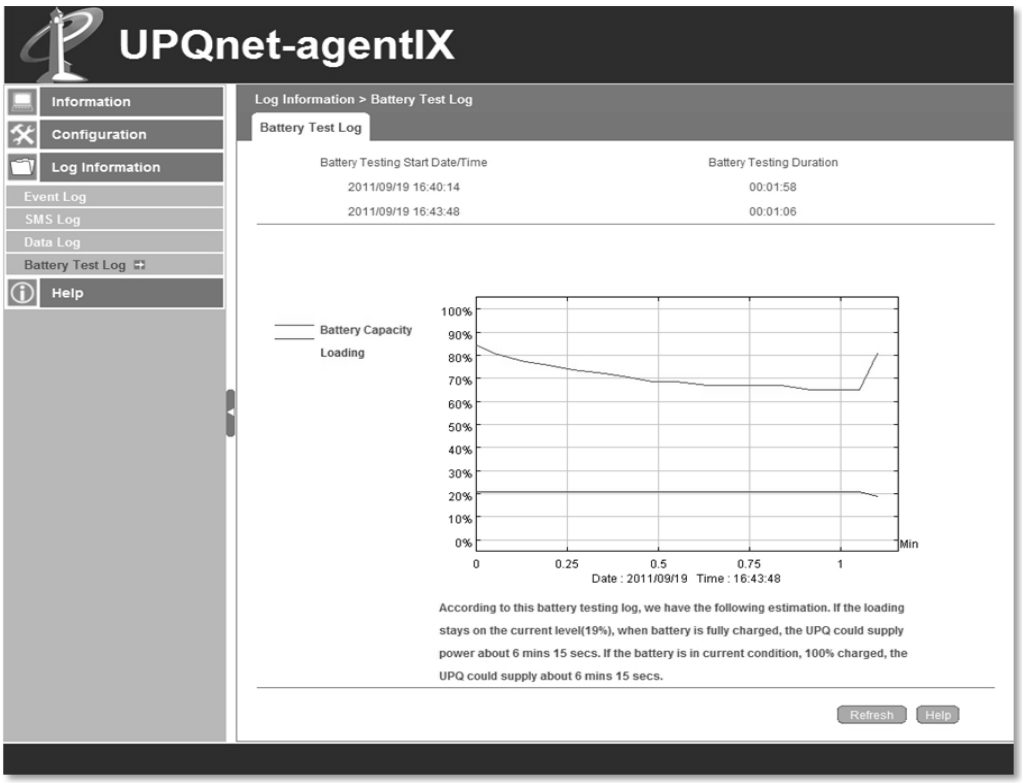



***Figure 81—Log Information→Battery Test Log***

---


Note

When the UPQ switches to battery backup, the % charge of the battery will typically drop off quickly for the first few seconds, then level off and drop slowly. This is typical and should not be a cause for concern.

---

Below the graph, the NetAgent will provide an estimate of how long the system can run on battery with the current load. This is an estimate based off the displayed test only. In order to have maximum accuracy in the estimates, the battery test should run at full typical load and should be run for a long enough period to get at accurate reading (typically more than 2 minutes or at least 60% battery charge).

---

**Caution**

During these tests, do not turn OFF connected equipment that would be ON during an actual power outage. Doing so could produce a false reading.

# 3.7—Help

The **Help** section provides various resources to help manage the NetAgent.

## 3.7.1—Search UPQ-NetAgent9

This screen provides a list of NetAgent devices on the local network. This screen information is similar to the device listing in Netility.

Open the web management screen for any discovered NetAgent by clicking on the device in this list.

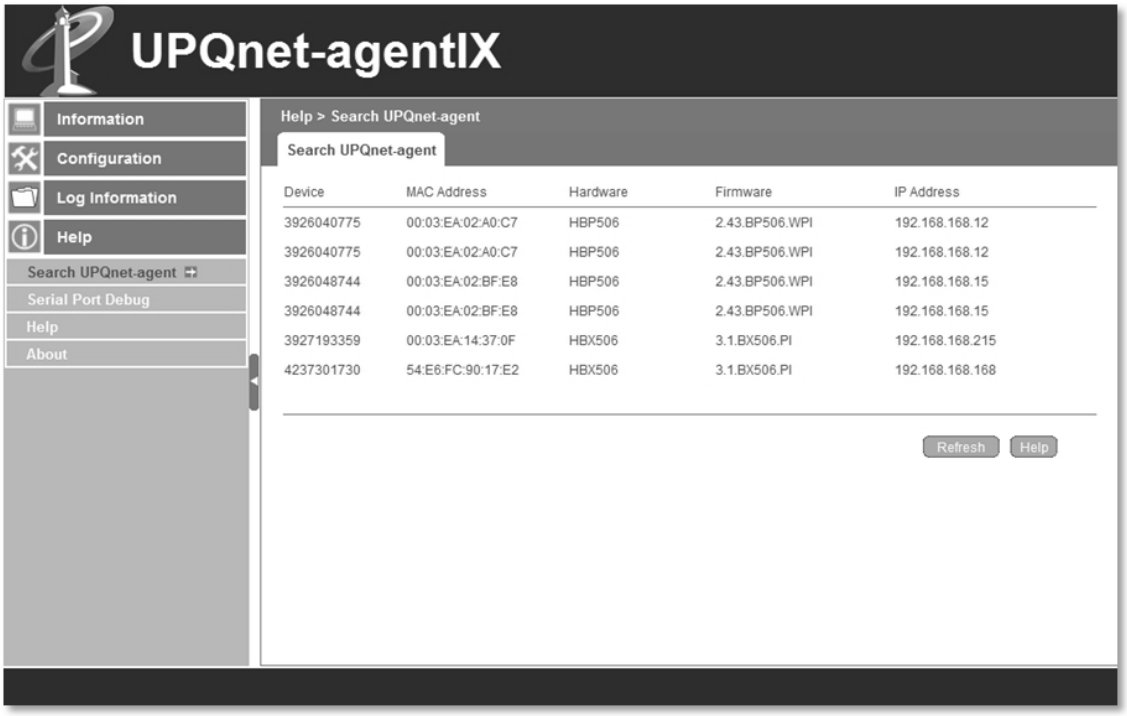



***Figure 82—Help→Search UPQ-NetAgent***

## 3.7.2—Serial Port Debug

These screens provide tools for debugging the serial connection between the NetAgent and the UPQ.

### 3.7.2.1—Port Information

Manually change serial port settings for debugging the connection.


***Figure 83—Help→Serial Port Debug→Port Information***

Manual Helps

For definitions of technical terms, see **Appendix A—Glossary**.

### 3.7.2.2—Debug Information

Debug communication problems between the UPQ and NetAgent using this screen, which displays the communication history between the NetAgent and the UPQ over the RS232 cable.

The **ASCII/Hexadecimal** field selection makes it possible to send specific information from the NetAgent to the UPQ. Select whether the information is in **ASCII** or **Hexadecimal** format before entering the information to send in the **Send Content** box. Click **Send**.

**Sent Information**—Displays the information that has been sent from the NetAgent to the UPQ.

**Received Information**—Displays responses that the UPQ has sent back to the NetAgent.

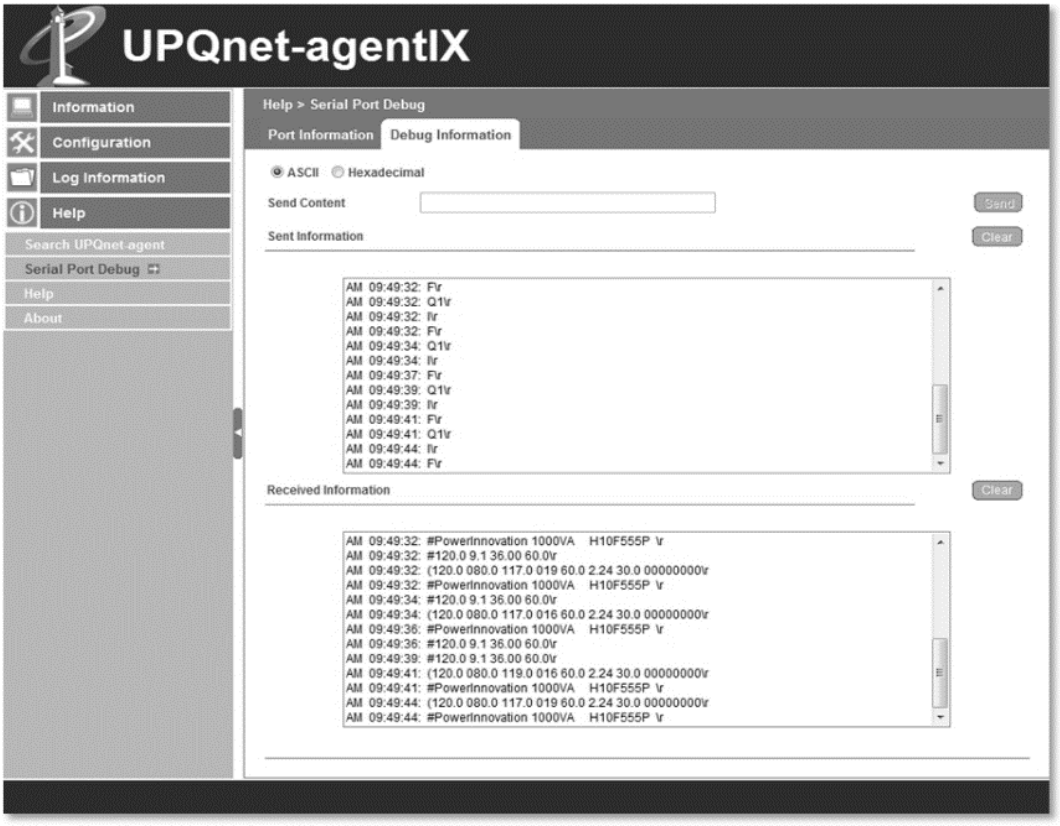



***Figure 84—Help→Serial Port Debug→Debug Information***

### 3.7.3—Help

This screen opens an online screen help guide in a new browser window.

### 3.7.4—About

These screens provide information about the current firmware version of the NetAgent and provide tools for saving the current device settings to a backup file or for upgrading the device firmware.

#### 3.7.4.1—About

View the **Firmware Version**, **Hardware Version**, and **Serial Number** of the NetAgent.


***Figure 85—Help→About***

### 3.7.4.2—Save/Restore Settings

Save the current NetAgent settings to an off-site file or upload a settings file and apply it. It is a good idea to create an off-site backup of system settings before performing a firmware update or making any other significant changes to the NetAgent configuration.


***Figure 86—Help→About→Save/Restore Settings***

### 3.7.4.3—Firmware Update Settings

Configure an FTP server and an interval to have the NetAgent automatically check for and install firmware upgrades.

***OR***

Manually check for and install any firmware upgrades.

---

Manual Helps

For more information about installing firmware upgrades, see **3.1.4—Upgrading NetAgent Firmware**.

---


***Figure 87—Help→About→Firmware/Update Settings***

Use the **FTP Server**, **User**, and **Password** fields to connect to the remote FTP server where the firmware image is located. These fields are populated with the Power Innovations FTP server information by default. Click the top **Apply** button to save all settings.

Click **Update Now**>> to use the FTP access settings to connect to the remote FTP server and check for a firmware update. If an update is found, the NetAgent will download and install the new firmware.

**Auto Update**—Configure the NetAgent to connect to the specified FTP server and check for an update for the firmware automatically. If an update is found, the NetAgent will download and install the new firmware. The interval and time when the NetAgent will check for an update should be specified, or the interval should be set to **NO** to disable automatic updates. Click the middle **Apply** button to save all settings.

The NetAgent can run an FTP server that will allow the firmware to be updated by uploading a new firmware image using an FTP client to connect to the NetAgent. Check the **Enable Firmware Update by FTP Client** option to enable this feature. By default, the FTP server on the NetAgent is disabled. Click the bottom **Apply** button to start or stop the FTP server.

## 3.8—Upgrading NetAgent Firmware

1. Connect to the NetAgent web interface;
2. Click **Help**;
3. Click **About**;
4. Click on the **Firmware Update Settings** tab;
5. If necessary, enter the domain name of the **FTP Server** where the firmware image is stored. By default, the Power Innovations FTP server and login information are already provided;
6. Enter the **Username** and **Password** provided for the specified FTP server;
7. Select an interval and enter a time in the **Auto Update** fields to have the NetAgent automatically check periodically for firmware updates;
8. Click **Update Now**>> to have the NetAgent connect to the specified FTP server and check to see new firmware updates are available:
    a. A pop-up window will open while the NetAgent checks for, downloads, and applies the update if one is available. Do not interrupt the installation process by closing the pop-up window, or it may render the NetAgent unusable;
    b. Click **OK** to close the pop-up window after the installation has completed. The NetAgent will reboot.

## 3.9—Calibrating Battery Capacity Voltage

The battery capacity (%) is determined by the difference between the full charge voltage and the actual voltage of the battery. For the NetAgent to accurately determine the battery capacity, it must have an accurate value for the full charge voltage of the battery.

To calibrate the full charge voltage of the battery:

1. Allow the UPQ to charge the battery for at least 24 hours before beginning a calibration;
2. Connect to the NetAgent web interface;
3. Click **Information**;
4. Click **Current Status**;
5. Click on the **Battery Status** tab;
6. Look at the **Battery Capacity** value. To correctly calibrate the full charge voltage, it is necessary to get a reading below 100% and then gradually adjust to a 100% charge;

    If the capacity is 100% or higher, the full charge voltage will need to be increased to reduce the capacity value.
    If the capacity is below 100%, the full charge voltage will need to be decreased to increase the capacity value.
7. Open a new browser tab or window (do not close the existing **Battery Status** screen);

8. Connect to the NetAgent web interface in the new tab;
9. Click on **Configuration**;
10. Click on **UPQ Configuration**;
11. Adjust the **Battery Full Charge Voltage** (V) up or down using a small increment (a few thousandths);

---

For example…

If the value is 2 and the capacity is reading at 95%, drop the value to 2.264).

---

12. Click **Apply**;
13. Switch back (without closing the current tab) to the tab open to the **Battery Status** screen;
14. Wait for the screen to refresh. It may be necessary to change the value of the **Refresh status every** setting at the bottom of the screen to expedite the calibration process;
15. Compare the new capacity value to the old capacity value;
16. Switch to the **UPQ Configuration** tab;
17. Repeat steps 11–15, using varying increments if necessary, to bring the **Battery Capacity** value to 99%;
18. Repeat steps 11–15, decreasing the **Battery Full Charge Voltage** (V) value by 1/1000 (0.001) increments until the **Battery Capacity** becomes 100%.

# 3.10—Installing a New SSL Certificate

The default SSL certificate on the NetAgent is a self-signed certificate.

Most web browsers will display a warning message any time they encounter an SSL certificate that has not been signed by a trusted Certificate Authority (CA) such as GoDaddy, Verisign, or Comodo, or a certificate that has expired or that does not match the domain name used to access the NetAgent server.

While it is possible to tell the browser to ignore the certificate warning, it may be preferable to purchase a signed certificate. To obtain and install an SSL certificate on the NetAgent:

1. Install *OpenSSL* on the computer that will be used to upload the SSL certificate and key:
    a. Insert the NetAgent management software CD into the CD-ROM drive;
    b. Browse to the *OpenSSL* folder on the CD drive;
    c. Copy all the contents of the *OpenSSL* folder into a new folder on the computer's hard drive;

    Be sure to put the files in a location where they are easy to find (such as in a folder on the desktop);
2. Create a **Public Key** to use on the NetAgent:
    a. Browse to the location on the hard drive where the *OpenSSL* files are saved;
    b. Double-click *openssl.exe* to run the OpenSSL command interface;
    c. Enter the following command to generate the key:

    genrsa –out server.key 1024;
3. Create a Certificate Signing Request (CSR):
    a. Browse to the location on the hard drive where the *OpenSSL* files are saved;
    b. Double-click openssl.exe to run the *OpenSSL* command interface;
    c. Enter the following command to generate the CSR:

    req –new –nodes –config openssl.cfg –keyout server.key –out server.csr;
    d. Answer the questions about the company the certificate will be issued to. This information must match publicly available information about the company or the CA will not issue a certificate;

The common name should be the exact domain name that will be used to access the NetAgent.

For example…

Exact domain name used for access: UPQ-NetAgent9.example.com.

4. Submit the CSR to a CA using their purchasing website. Most CAs only take a few minutes after the purchase is made to create a signed certificate;
5. Save the signed certificate as *server.crt* in the folder where the *OpenSSL* files are saved;
6. Upload the public key (*server.key*) to the NetAgent:
    a. Connect to the NetAgent web interface;
    b. Click on **Configuration**;
    c. Click on **Web/Telnet**;
    d. Click the **SSL Information** tab;
    e. Click **Browse...** for the **SSL Public Key**;
    f. Browse to the folder where the *OpenSSL* files are saved, select the key file (*server.key*) and click **Open**;
    g. Click **Upload and Replace**;
7. Upload the signed certificate (*server.crt*) to the NetAgent:
    a. Connect to the NetAgent web interface;
    b. Click on **Configuration**;
    c. Click on **Web/Telnet**;
    d. Click **the SSL Information** tab;
    e. Click **Browse…** for the SSL Certificate;
    f. Browse to the folder where the *Open SSL* files are saved, select the certificate file (*server.crt*) and click **Open**;
    g. Click **Upload and Replace**.

It is also possible to create and upload a self-signed certificate. A self-signed certificate will still create a warning in the browser window but still allows for a secure connection. To generate and upload a self-signed certificate, follow the instructions above, replacing **Steps 3**, **4**, and **5** with the following:

3. Generate a self-signed certificate:
    a. Browse to the location on the hard drive where the *OpenSSL* files are saved;
    b. Double-click *openssl.exe* to run the OpenSSL command interface;
    c. Enter the following commands to create the certificate:

        req –new –x509 –config openssl.cfg –key server.key –out server.crt –days 365

    d. Answer the questions about the company to which the certificate will be issued. The common name should be the exact domain name that will be used to access the NetAgent.

For example…

# 4—Using SNMPView

SNMPView is a management program designed specifically to easily view and manage multiple NetAgent devices on a single network using SNMP.

Once it is started, SNMPView will remain running and monitoring the devices in the background (to completely exit SNMPView, click **Quit** from the **Device** menu). When SNMPView is running, a battery state icon ( ) will display in the system icons section of the windows taskbar.

SNMPView is available for computers running Windows.

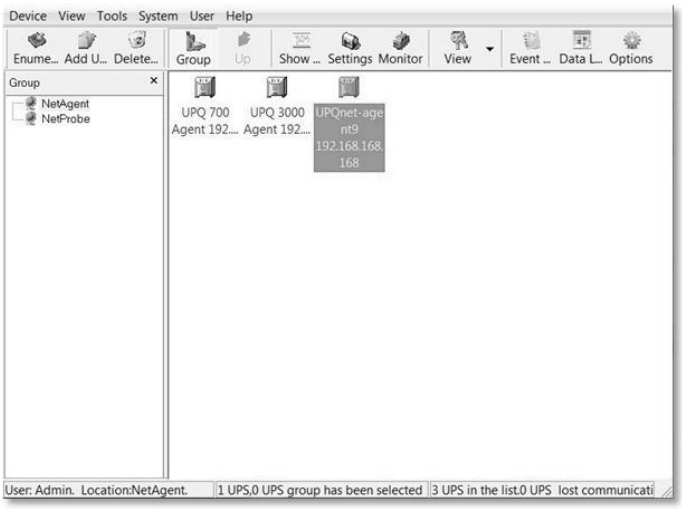



***Figure 88—SNMPView Window***

## 4.1—Installing SNMPView on Windows

1. Insert the management software CD into the CD-ROM drive of the computer where SNMPView will be installed;
2. Browse to the SNMPView folder on the CD drive;
3. Run *setup.exe*;
4. If prompted, click **Yes** to allow setup.exe to make changes to the computer;
5. Follow the installer onscreen instructions to complete the installation process.

## 4.2—Discovering and Viewing NetAgent Devices

1. Launch SNMPView. In Windows, go to **Start** > **(All Programs)** > **NetAgent** > **SNMPView** and click **SNMPView for Windows**;
2. Log in using the appropriate username and password. If SNMPView is running for the first time, the default username is **Admin** with a blank password;
3. Click **Enumerate**. SNMPView will query the network for NetAgent devices and display any it discovers in the view window;
4. If a NetAgent is not discovered automatically, it is possible to manually add a device:
   a. Click **Add UPS**;
   b. Enter the IP address of the UPQ-NetAgent9 in the **IP address (Domain)** field;

c. If necessary, change the **Community** name to the one in which the NetAgent is assigned;

d. Click **OK**;

5. The status of the UPQ connected to the NetAgent is displayed in the View window using different icons and colors:

   a. If the UPQ is online, it is represented by a UPQ icon (  );

   b. If the UPQ is online but has a low battery, it is represented by a crushed battery icon (  );

   c. If the UPQ is offline or disconnected, it is represented by a broken wire icon (  );

   d. If the UPQ is offline or the status is unknown, the text will be red; otherwise, the text will be blue;

6. Click the **View** button to cycle the view between different options for viewing the devices:

   **Large Icons** view provides a tiled display of all the NetAgent devices or groups;

   **Small Icons** view provides a list of all the NetAgent devices or groups with some basic information;

   **Detail** view provides a list of all the NetAgent devices with detailed information about the connected UPQ. It may take a few seconds to update the display with current status information about each UPQ;

   **Map Background** view provides the ability to display and visually arrange the NetAgent devices and groups with the option to provide a background image (such as a map) for additional visual organization. Each group can have its own background image;

7. Click **Event Log** to view, save, print, or clear the combined event history for all the NetAgent devices being monitored by SNMPView;

8. Click **Data Log** to view, save, print, or clear the combined status history for the NetAgent devices or the combined environmental status history for any e-Alert sensors connected to the NetAgent devices.

## 4.3—Creating and Organizing Groups of NetAgent Devices

1. Launch SNMPView. In Windows, go to **Start** > **(All Programs)** > **NetAgent** > **SNMPView** and click **SNMPView for Windows**;

2. Log in using the appropriate username and password;

3. Click **Group** to show or hide the list of groups;

4. Right click in the main window and select **Add Group**;

5. Enter a group name and click **OK**;

6. Drag the icon of the NetAgent to be assigned to the group and drop it on the group folder icon in the **View** window;

7. To view the devices in the group, double-click the group folder icon;

8. Click **Up** to view the parent list of devices and groups.

## 4.4—Managing an Individual NetAgent

1. Launch SNMPView. In Windows, go to **Start** > **(All Programs)** > **NetAgent** > **SNMPView** and click **SNMPView for Windows**;
2. Log in using the appropriate username and password;
3. Double-click the icon for the desired NetAgent device to view details about the individual UPQ.

All the screens show a quick status update at the bottom of the screen. The icons will display a green background for a normal condition, and a red background for an alert condition:

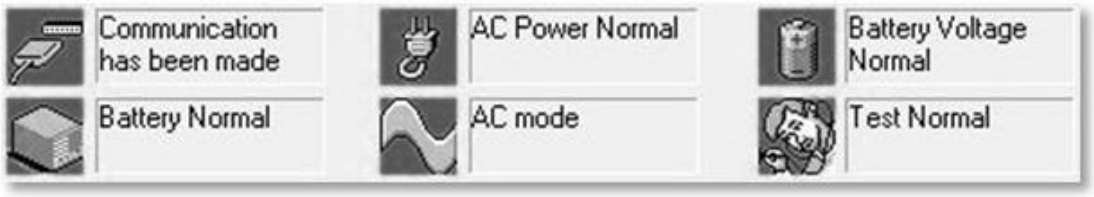



***Figure 89—Quick Status Update Icons***

**Meter** tab—view a graphical representation of the UPQ operating status. The screen displays the **Input Voltage** (v), the **Input Frequency** (Hz), the **Output Voltage** (v), the **Temperature** (if an e-Alert Sensor is connected), the **Capacity** (battery charge %), and the **UPQ Loading** (%):

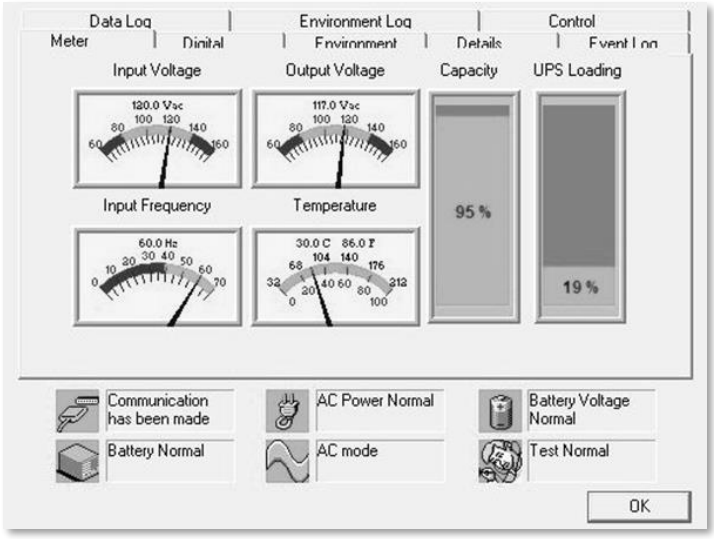



***Figure 90—Meter Tab***

**Digital** tab—view a digital display of the UPQ operating status. The screen displays the **Input Voltage** (v), the **Input Frequency** (Hz), the **Output Voltage** (v), the **Temperature** (if an e-Alert Sensor is connected), the **Capacity** (battery charge %), and the **UPQ Loading** (%):

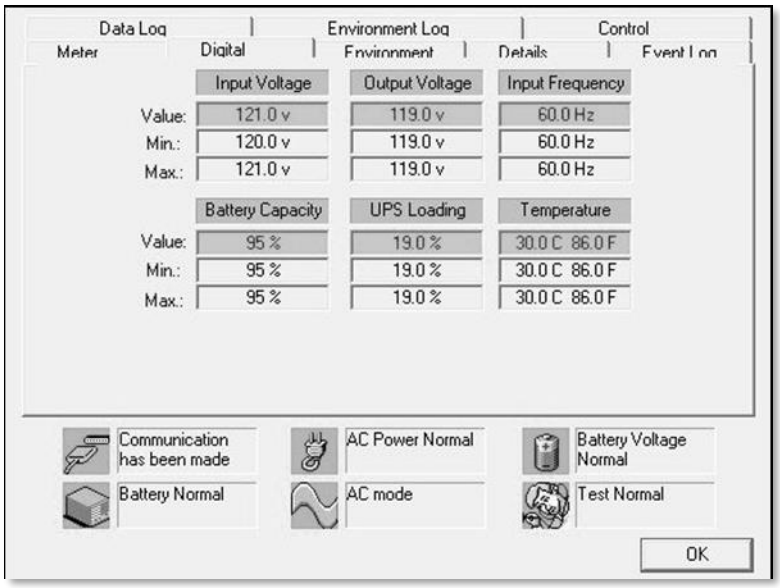



***Figure 91—Digital Tab***

**Environment** tab—view the status of the e-Alert Sensor (if connected). The screen displays a list of environmental sensors connected to the e-Alert Sensor and the status of the sensors:

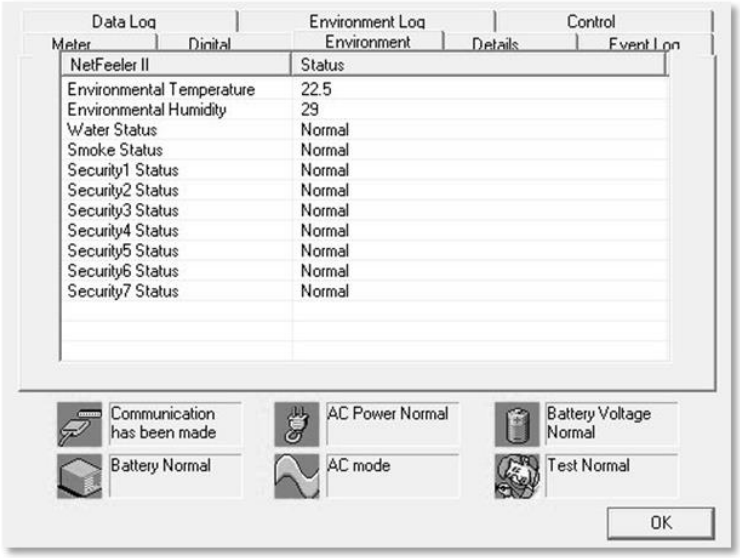



***Figure 92—Environment Log***

**Details** tab—view additional information about the UPQ. The screen displays the name, **IP Address**, **Location**, and **Manager** of the NetAgent, as well as the **Manufacturer**, **Model**, **Version**, and rating information for the UPQ:

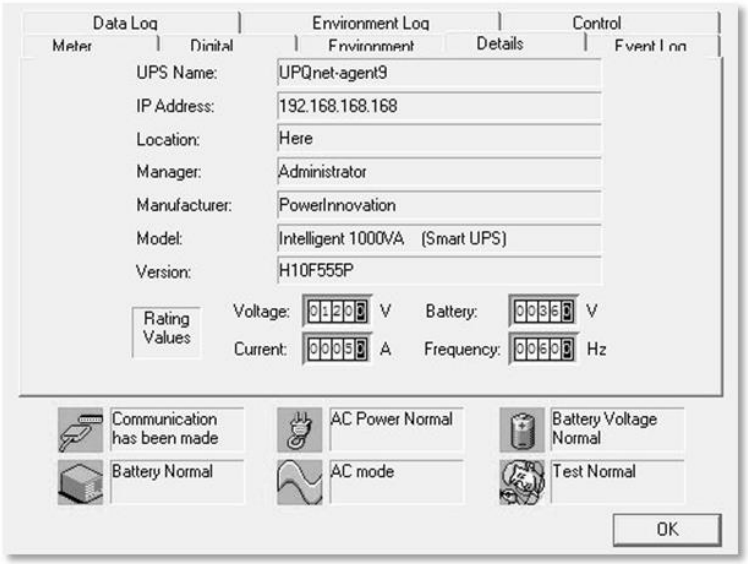



***Figure 93—Details Tab***

**Event Log** button—view the event log for the UPQ:

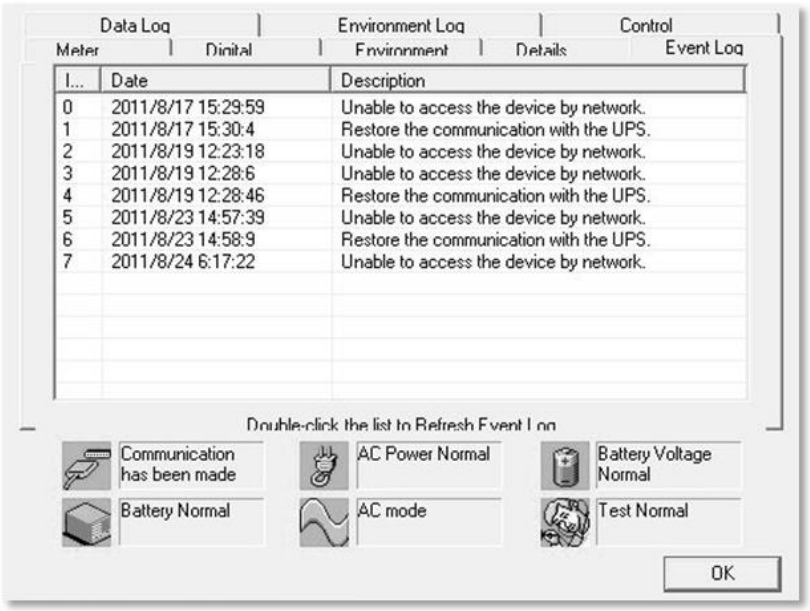



***Figure 94—Event Log Button***

**Data Log** button—view the status log for the UPQ:

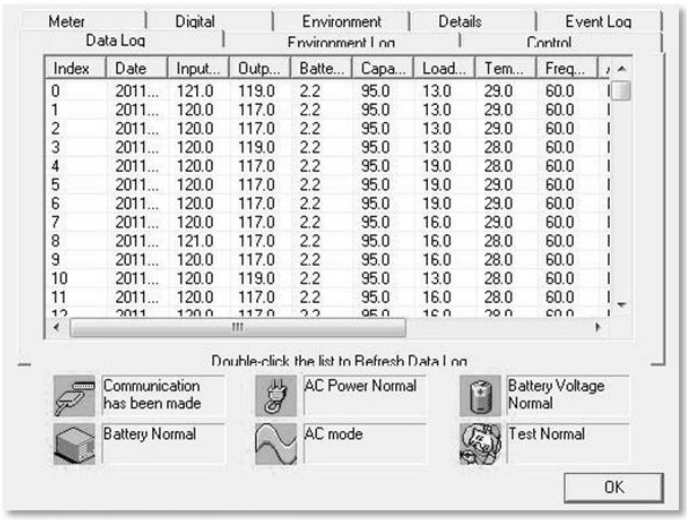



***Figure 95—Data Log Button***

**Environment Log** button—view the status log for the e-Alert Sensor (if connected):

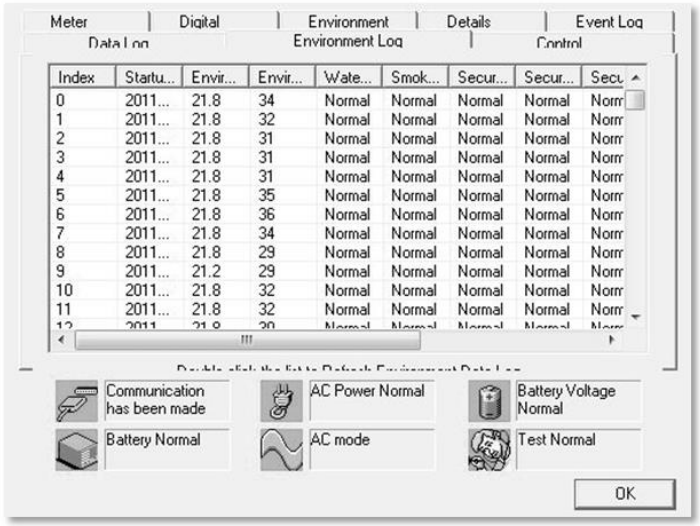



***Figure 96—Environment Log Button***

**Control** button—send commands to the UPQ. It is possible to send management and testing commands to the UPQ. Select the command to send from one of the four command groups (**UPS Control**, **Test Control**, **Turn-Off Parameters**, or **Test Period**) and click the **Execute >>** button to send the command:

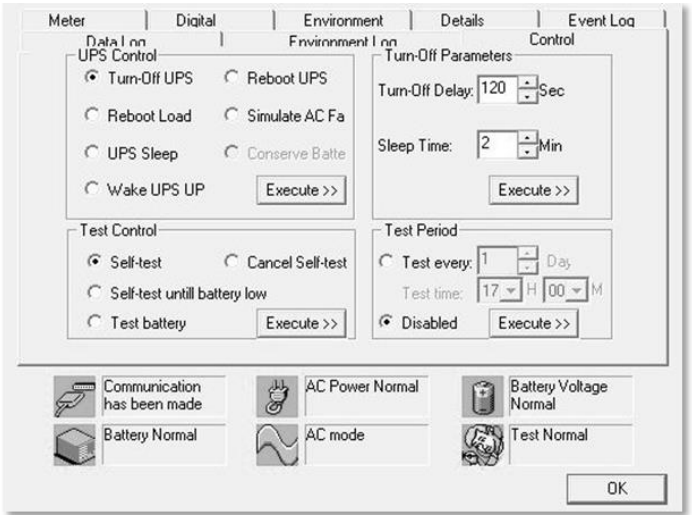



***Figure 97—Control Button***

4. Click **OK** to close the individual UPQ status window.

# 4.5—Managing Users

1. Launch SNMPView. In Windows, go to **Start** > **(All Programs)** > **NetAgent** > **SNMPView** and click **SNMPView for Windows**. SNMPView users only affect who can run SNMPView, and are not the same as SNMP or Web users on the NetAgent;
2. Log in using the **Admin** manager account—by default, there is no password for the **Admin** account;
3. Click **Account Management…** under the **User** menu;
4. To add a user:
    a. Click **Add User**;
    b. Enter the new username in the **Account** field;
    c. Enter a password for the user in the **Password** field;
    d. Click **OK**. The new user will be added as a *Guest* level account. The only difference between a *Guest* and *Manager* account is that the Manager account (**Admin**) cannot be deleted;
5. To delete a user:
    a. Select the user to be deleted—the Admin user cannot be deleted;
    b. Click Delete;
6. To change a user's password:
    a. Select the user that will be getting the new password;
    b. Click **Change Password**;
    c. Enter the new password in the **Password** field;
    d. Click **O**

# 5—Using ClientMate

ClientMate runs as a service on systems connected to the UPQ and can perform clean system shutdowns based on triggers provided by the NetAgent. The ClientMate program is available for computers running Windows, MacOS, Linux, FreeBSD, and VMWare.


***Figure 98—ClientMate Opening Screen***

The NetAgent can be configured (using the web management interface or SNMPView) to send notifications before the UPQ shuts OFF (either for specific shutoff or power-loss events).

ClientMate will attempt to save files, close programs, and shut down the computer before the UPQ shuts off power.

---

Note


ClientMate communicates with the NetAgent and does not know if the computer is connected to the UPQ itself. If the NetAgent sends a shutdown warning, ClientMate will shut down the computer even if it is not connected to the UPQ.

---

ClientMate runs as a service on the PC and will automatically start whenever the computer starts. To start ClientMate manually in Windows, go to **Start**>(**All Programs**)>**NetAgent**>**ClientMate**. When the service is running, the operating system will display a server icon in the **System Icons** menu at the right or bottom corner of the taskbar.

ClientMate includes a user interface that displays the current status and an event log for the UPQ to which the system is connected.

## 5.1—Installing ClientMate on Windows

1. Insert the management software CD into the CD-ROM drive of the computer where ClientMate will be installed;
2. Run *ClientMate.exe*;
3. If prompted, click **Yes** to allow *ClientMate.exe* to make changes to the computer;
4. Follow the installer onscreen instructions to complete the installation process.

## 5.2—Configuring ClientMate to Shut Down a Windows Computer

1. Open the ClientMate User Interface by double-clicking the *ClientMate* system tray icon or by right-clicking the icon and selecting **Open ClientMate**;
2. Click on **Configuration**;
3. Select the radio button for the SNMP method the NetAgent is using (most likely, this will be SNMP V1/V2);
4. Enter the IP address of the NetAgent in the **Host** field or click **Query** to select from a list of devices running on the local network;
5. Check the box(es) for the desired **Warning Messages** to be displayed when the NetAgent sends an event notification to ClientMate;
6. Click the **Power Failure** tab;
7. Select either to have Windows manage the system shutdown using the ACPI interface or to have ClientMate shut down Windows;
8. If ClientMate is handling the shutdown:
    a. Select whether ClientMate should have the computer **Shut down** or **Hibernate**;
    b. Select a time window after which ClientMate should initiate shutdown if the UPQ loses AC power. If AC power is restored before time runs out, ClientMate will abort the shutdown;
    c. Select a time window after which ClientMate should initiate shutdown if the UPQ battery reaches a critical low level;
    d. Select the critical level for the UPQ battery that will trigger a shutdown. Make sure this level is sufficient to allow the computer the shut down before battery failure;
9. Click the **Scheduled Shutdown** tab;
10. Select whether ClientMate should have computer shut down or hibernate during its scheduled shutdown period;
11. Select the time window between the warning and the computer shutdown;
12. Select the time window between the Windows computer shutdown and scheduled UPQ shutdown;

13. Click **OK**.

## 5.3—Installing ClientMate on Linux


Note

ClientMate for Linux is only available as an RPM.

1. Insert the management software CD into the CD-ROM drive of the computer where ClientMate will be installed;
2. If necessary, mount the CD-ROM drive;
3. Navigate to the *ClientMate for Linux* folder on the CD-ROM;
4. Extract the *ClientMate RPM installer* from the *ClientMate zip* file;
5. Install ClientMate using the Linux RPM installation tool.

Manual Helps

For definitions of technical terms, see **Appendix A—Glossary**.

## 5.4—Configuring ClientMate to Shut Down a Linux Computer

1. Launch ClientMate by selecting **ClientMate** from the **Network Applications** menu. If this is the first time it has been launched, ClientMate will launch in the Mandarin language;
2. Change the program language if necessary:
   a. Click the **Configuration** button;
   b. Select **English** (or the preferred language) from the **Language** menu at the bottom of the configuration window;
   c. Click the left button at the bottom of the configuration window to save the changes;
   d. Exit ClientMate:
      i. Close the ClientMate's user interface window;
      ii. Locate and right-click the **ClientMate service** icon (  );

iii. Select the bottom menu option to exit ClientMate;

e. Restart ClientMate (see **Step 1** above)—ClientMate will launch in the selected language;

3. Click **Configuration**;
4. Enter the NetAgent IP address in the **Address** box;
5. Click the **Power** tab;
6. Configure ClientMate to handle the shutdown:
   a. Select whether ClientMate should have the computer shut down or hibernate;
   b. Select a time window after which Client Mate should initiate shutdown if the UPQ loses AC power. If AC power is restored before time runs out, ClientMate will abort shutdown;
   c. Select a time window after which ClientMate should initiate shutdown if the UPQ battery reaches critical low levels;
   d. Select the UPQ battery critical level that will trigger shutdown. Make sure this level is high enough that the computer will shut down before the battery fails;
7. Click the Schedule Shutdown tab;
8. Select whether ClientMate should have the computer shut down or hibernate during a scheduled shutdown;
9. Select the time window between the warning and computer shutdown;
10. Select the time window between Windows computer shutdown and UPQ scheduled shutdown;
11. Click OK.

## 5.5—Installing ClientMate on MacOS

1. Insert the management software CD into the CD-ROM drive of the computer where ClientMate will be installed;
2. Navigate to the *ClientMate for MAC* folder on the CD-ROM;
3. Double-click *ClientMate.pkg* to run the install utility;
4. Follow the onscreen instructions to complete the installation.

---

Manual Helps

For definitions of technical terms, see **Appendix A—Glossary**.

---

## 5.6—Configuring ClientMate to Shut Down a Mac

1. Open the ClientMate User Interface by double-clicking the *ClientMate system tray* icon or right-clicking the icon and selecting **Open ClientMate**;
2. Click on **Configuration**;
3. Enter the NetAgent IP address in the **Host** field or click **Query** to select from a list of devices running on the local network;
4. Check the box or boxes for the **Warning Messages** that will be displayed when the NetAgent sends an event notification to ClientMate;
5. Click the **Power Failure** tab;
6. Configure ClientMate to handle the shutdown:
    a. Select whether the computer will shut down or hibernate;
    b. Select a time window after which ClientMate will initiate a shutdown if the UPQ loses incoming AC power. If AC power is restored before time runs out, ClientMate will abort shutdown;
    c. Select a time window after which ClientMate will shut down if the UPQ battery reaches critical low levels;
    d. Select the UPQ battery critical level that will trigger UPQ shutdown. Make sure that this level is sufficiently high to allow the computer to shut down before the battery fails;
7. Click the **Schedule Shutdown** tab;
8. Select whether ClientMate should have the computer shut down or hibernate during a scheduled shutdown:
    a. Select the time window between the warning and computer shutdown;
    b. Select the window between Mac shutdown and the scheduled shutdown of the UPQ;
    c. Click **OK**.

# 5.7—Monitoring the UPQ Status with ClientMate

Open ClientMate by double-clicking the *ClientMate system tray* icon or right-clicking the icon and selecting **Open ClientMate**.

If ClientMate has not been configured with a connection to a NetAgent or if it cannot communicate with the configured NetAgent, ClientMate will display a no network connection icon.

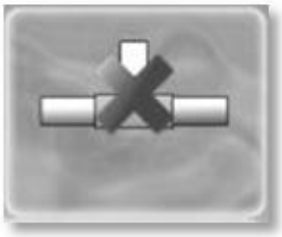


***Figure 99—No Network Connection***

If ClientMate has a good connection to the configured NetAgent, ClientMate will display a **Network Connected** icon with the IP address of the connected NetAgent.

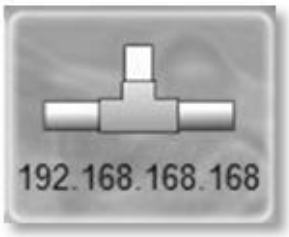



***Figure 100—Network Connected***

If the UPQ is getting AC input power, ClientMate will display an **AC Normal** icon.


***Figure 101—AC Normal***

If the AC input to the UPQ has failed, ClientMate will display an **AC Fail** icon.


***Figure 102—AC Fail***


***Figure 103—Battery Normal***

ClientMate will show the battery charge status.

If an event has triggered a system shutdown, ClientMate will display a shutdown timer.


***Figure 102—Shutdown Timer***

# 6—Using SMS Server

SMS Server is a PC-based service capable of sending SMS alerts from multiple NetAgent devices using a single GPRS/GSM modem connected to the PC.

SMS Server runs as a service on the PC and will display a phone icon (  ) in the system icons menu at the right or bottom corner of the taskbar. SMS Server will automatically start whenever the computer starts.

---

Manual Helps

For definitions of technical terms, see **Appendix A—Glossary**.

---

## 6.1—Installing SMS Server on Windows

1. Insert the management software CD into the computer CD-ROM drive on which SMS Server will be installed;
2. Browse to the *SMS Server* folder on the CD drive;
3. Run *setup.exe*;
4. If prompted, click **Yes** to allow *setup.exe* to make changes to the computer;
5. Follow the installer onscreen instructions to complete the installation process.

## 6.2—Configuring SMS Server on a PC

1. Connect the GPRS modem to the PC, following the instructions in **7.3—GPRS Modem**;
2. Right-click on the **SMS Server** system icon and select **Modem Information** from the menu;
3. Confirm that SMS Server is detecting the modem and that the SIM card is properly installed in the modem;
4. Click **OK**;
5. Right-click on the **SMS Server** system icon and select **System Settings**;
6. Select the COM port connected to the GPRS modem (see **Devices and Printers** to see which COM port to select);
7. Enter the SIM card PIN in the **SIM PIN** field;
8. Enter the SIM card PIN in the **Confirm SIM PIN** field;
9. Click **OK**;
10. Send a test message to a cellular phone:
    a. Right-click on the **SMS Server** system icon and select **Send Message**;

b. Enter the 11-digit (1+area code + prefix + number, such as 19585550142) phone number of the cellular phone to receive the message;

---


Note

The 1- prefix must be included or the message will not be successfully sent.

---

c. Enter a short message to be sent as the body of the test message;

d. Click **Send**;

e. Confirm that the message was successfully received;

f. Click **OK** to close the test message window.

## 6.3—Configuring the NetAgent to Connect to SMS Server

1. Connect to the NetAgent web interface by entering the IP address of the device in a web browser address bar or by selecting the correct NetAgent in Netility and clicking **Launch Web User Interface**;
2. Click on **Configuration**;
3. Click on **SMS**;
4. Select **Use Remote Service** from the **Send SMS When Event Occurs** menu;
5. Enter the IP address of the computer running SMS Server in the **SMS Server** field;
6. If SMS Server was configured for user authentication, enter the **Account Name** and **Password** into the fields.
7. Configure the NetAgent to send SMS messages:
   a. Click on the **Mobile For Event Log** tab;
   b. Enter the 11-digit (1 + area code + prefix + number, e.g. *19585550142*) phone number of the cellular phone that should receive notifications in the **Cellular Phone number1** box. The 1- prefix *must* be included or the message will not be sent;
   c. Click the **Select** button to the right of the **Cellular Phone number1** box;
   d. Select **Yes** or **No** for each of the UPQ events for which this number should receive notifications;
   e. If an e-Alert Sensor is installed, click the **e-Alert Sensor** tab and select **Yes** or **No** for each of the e-Alert Sensor events for which this number should receive notifications;
   f. Click **Apply**;
   g. Close the **Select Event** window to return to the regular UPQNetAgent9 configuration window;
   h. Repeat steps **D** through **I** for any additional cellular phones for the **Cellular Phone number2** through **Cellular Phone number 8** fields;
   i. Click **Apply**;
8. Check to confirm that the notification number(s) are properly configured:
   a. Click on the **SMS Setting** tab;
   b. Enter a test message in the **Sending test SMS** field;
   c. Click the **Test SMS** button. A test SMS message will be sent to all the cellular phones configured in the list.

# 7—Using the LCD Display

The external NetAgent module includes an LCD display that cycles through a series of status notifications about the state of the NetAgent and the connected UPQ. The LCD will indicate the following information in sequence:

**Input Volts**, **Input Hz**, **Loading**, **Output Volts**, **Battery Volts**, **Battery Charge %**, **Temperature C** (requires e-Alert sensor), **Temperature F** (requires e-Alert sensor), **Humidity** (requires e-Alert sensor), **IP Address** (one octet at a time), **Net Mask IP** (one octet at a time), **Gateway IP** (one octet at a time):

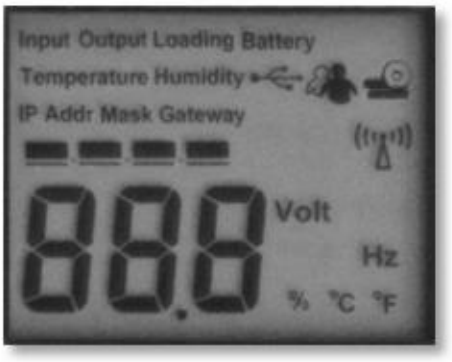



***Figure 103—NetAgent LCD Display***

- IP addresses are displayed one octet at a time, with the indicator bar ( ) above the position of the octet that is currently being displayed.
- The **e-Alert Sensor** icon ( ) will display when a reading (Temperature, Humidity) is being provided by the e-Alert Sensor.
- The **wireless network** icon ( ) will display when the UPQ-NetAgent9 is connected to a wireless network through a USB wireless adapter. The wireless network icon will flash while the UPQ-NetAgent9 is attempting to establish a connection to a wireless network.
- The **USB** icon ( ) will display if any device is connected to either of the USB ports on the front of the NetAgent.
- The **USB Drive** icon ( ) will display if a USB drive is connected to one of the USB ports on the front of the NetAgent.

## 7.1—Using the LED Status Lights

The three LEDs on the end of the NetAgent indicate the status of the module. When power is connected, and the NetAgent is functioning, the green LED will be lit. The yellow and red LEDs will be on, off, or flashing depending on what the NetAgent is doing:

| Yellow | Red | Green | Status |
|---|---|---|---|
| Solid Off | Solid Off | Solid ON | Power ON |
| Flashing | Solid ON | Solid ON | System Initializing |
| Solid ON | Solid Off | Solid ON | Normal Operation |
| Solid ON | Flashing | Solid ON | No Connection to UPQ system |
| Flashing | Flashing | Solid ON | Writing Data to Flash Memory |

***Table 3—LED Status Indicators***

*This page intentionally left blank.*

# 8—Installing Supported Add-ons

The NetAgent has built-in support for the e-Alert Sensor environmental monitor, a USB 802.11 b/g wireless network adapter, or a GPRS/GSM cellular modem.

## 8.1—e-Alert Sensor

The e-Alert Sensor environmental monitor adds temperature, humidity, and flood sensors to the NetAgent, as well as an optional wireless smoke/gas alarm and up to eight wireless door/window perimeter sensors.

SNMP Trap, Email, or SMS notifications can be sent if the temperature or humidity goes outside a specified safe range, or if the flood, smoke/gas, or perimeter sensors are triggered. The status of sensors can be monitored or reset through the NetAgent user interfaces.

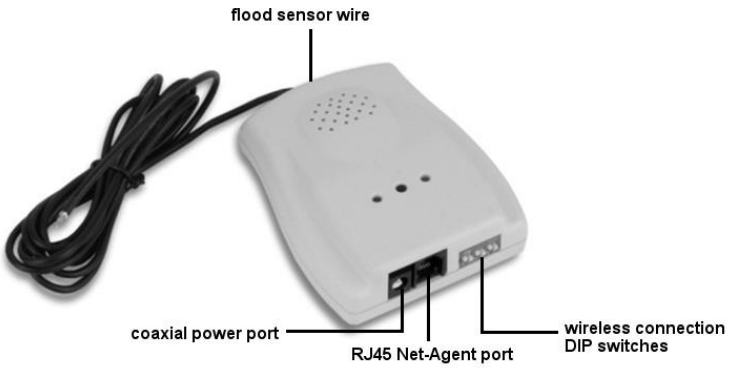



***Figure 104—e-Alert Sensor Overview***

### 8.1.1—Connecting the e-Alert Sensor to the NetAgent

1. Unpack the e-Alert Sensor;
2. Connect one end of the included RJ45 cable to the jack on the e-Alert Sensor. When connected to the NetAgent, the e-Alert Sensor will get power from the NetAgent and does not need a separate power cord attached;
3. Connect the other end of the included RJ45 cable to the jack in the center port of the NetAgent (the white cable in the picture below);
4. Position the end of the flood sensor wire in a location in which the sensor will provide warning of flooding *before* the UPQ or any of the equipment connected to the UPQ would be affected by the water;

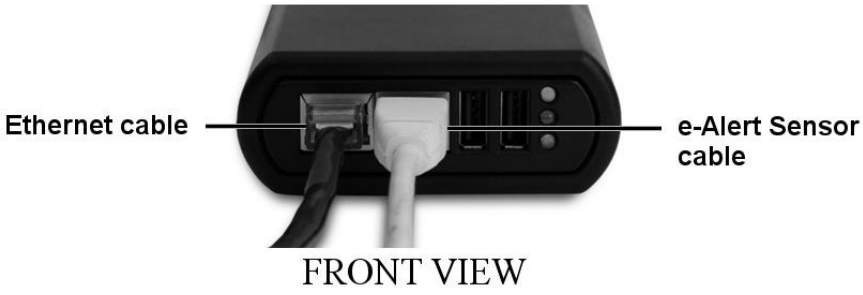



***Figure 105—A NetAgent with Attached Cables***

### 8.1.2—Connecting Environmental Warning Thresholds

Connect to the NetAgent web interface by entering the IP address of the device in a web browser address bar or by selecting the correct NetAgent in Netility and clicking **Launch Web User Interface**;

1. Click **Configuration**;
2. Click **e-Alert Sensor**;
3. Enter a minimum safe humidity level and temperature in the **Critical UnderRun** fields;
4. Enter a maximum safe humidity level and temperature in the **Critical OverRun** fields;
5. Click **Apply**.

### 8.1.3—Configuring Notifications

The SNMP Trap, Email, and SMS notification systems each have options for which notifications an individual recipient will receive.

When configuring a notification recipient for any of these methods, click the **Select** button, then click the **e-Alert Sensor** tab to view and select which environmental notifications the specified recipient will get.

### 8.1.4—Connecting Optional Wireless Sensors

1. Set DIP switch 1 on the e-Alert Sensor to the up ON position to enable wireless sensors;
2. Set DIP switches 2–6 to any pattern. These switches set the wireless ID of the e-Alert Sensor;
3. If multiple e-Alert Sensors have the same wireless ID, the wireless sensors will be detected by all e-Alert Sensors within range that share the wireless ID. Giving each e-Alert Sensor a different wireless ID allows for different wireless sensors to be connected to only specific e-Alert Sensors;
4. Set DIP switches 1–6 on the wireless sensor(s) to match the pattern on the e-Alert Sensor. It may be necessary to open the battery cover panel of the sensor in order to set the DIP switches;
5. If the wireless sensor is a window/door sensor, set the unique sensor ID with the separate set of 4 DIP switches using the following table. 1 is up (ON) and 0 is down (OFF):

| 1234 | Security Sensor ID |
|---|---|
| 1000 | Security Sensor 1 |
| 1001 | Security Sensor 2 |
| 1010 | Security Sensor 3 |
| 1011 | Security Sensor 4 |
| 1100 | Security Sensor 5 |
| 1101 | Security Sensor 6 |
| 1110 | Security Sensor 7 |

***Table 4—Security Sensor IDs***

# 8.2—USB 802.11 Wireless Adaptor

A USB 802.11 wireless adapter can be plugged into one of the USB ports on the front of the NetAgent to provide internet connectivity to a local wireless network. The NetAgent includes built-in support for 802.11 B/G wireless networks using **Open**, **Shared Key**, **WPA-PSK**, and **WPA2-PSK** authentication on a TKIP or AES encrypted network.

---

Note


Initial configuration of a wireless adaptor required a wired (Ethernet) network connection. The wired network connection is not required once the NetAgent has been configured to connect to the wireless network.

---

Once the NetAgent is configured to use the wireless network, a wired (Ethernet) connection is no longer required to connect to the web interface. The wireless IP address of the NetAgent will be different than the wired IP address.

## 8.2.1—Connecting a USB Wireless Adaptor to the NetAgent

1. Connect the USB plug on the wireless adapter into one of the USB ports on the front of the NetAgent;
2. Connect to the NetAgent web interface by entering the *wired* network IP of the device into the address bar of a web browser connected to the network or by selecting the correct NetAgent in Netility and clicking **Launch Web User Interface**;
3. Click **Configuration**;
4. Click **Wireless**;
5. Click the radio button beside the SSID of the desired network;
6. Click **Select**;
7. If the desired SSID does not show in the list, click **Rescan** or manually enter the SSID into the **SSID** field;
8. Select the **Authentication** type for the desired wireless network;
9. Select the **WPA Encryption** type for the desired wireless network;
10. Enter the **WPA Key** (if required) for the desired wireless network;
11. Click **Apply**.

# 8.3—GPRS Modem

A USB GPRS/GSM cellular modem can send SMS event notifications from the NetAgent to one or more cell phones.

The modem can be connected to the USB port on the front of the NetAgent or via a PC running SMS Server. An SMS Server allows multiple NetAgents to share a single GPRS modem.

To use a GPRS/GSM cellular modem, acquire an activated SIM card from a GSM cellular service provider. The SIM card must be linked to an account with a text-messaging plan (no voice or data plan is necessary).

Make sure to know the PIN assigned to the SIM card.


***Figure 106—GPRS Modem with Connected Serial-to-USB Adapter Cord***

## 8.3.1—Connecting Directly to the NetAgent

1. Unpack the GPRS modem;
2. Attach the serial connector from the serial-to-USB cable to the serial connector on the modem;
3. Push the button on the top of the modem to eject the SIM card from the slot (see picture below);


***Figure 107—Ejecting the SIM Card Caddy***

4. Insert the SIM card into the slot with the metal connectors facing up (see picture below);


***Figure 108—Inserting the SIM Card***

5. Slide the SIM card back into the slot in the modem, making sure it seats completely (see pictures below);

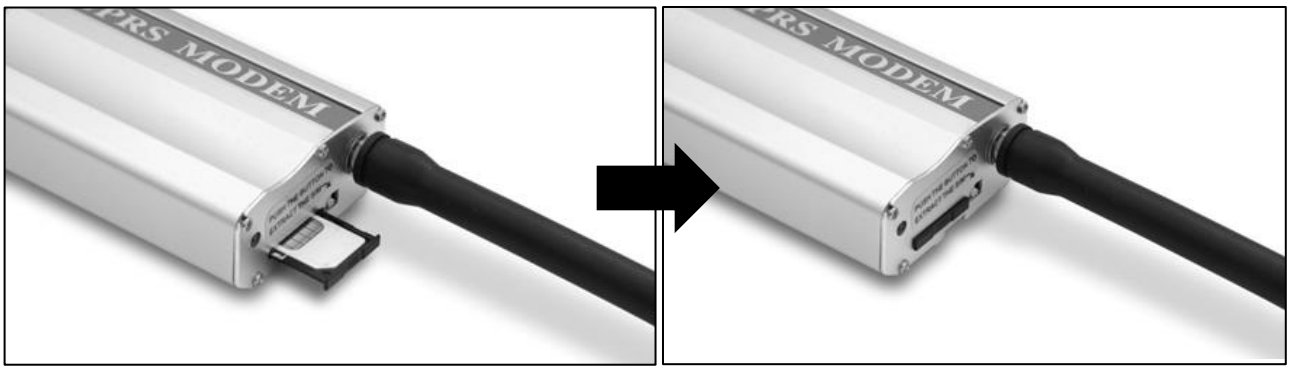



***Figure 109—Sliding the SIM Card into the Slot***

6. Attach the DC power plug into the power jack on the modem;
7. Plug the AC converter into a power outlet on the UPQ;

**Caution**

*The modem power supply must be plugged into the UPQ* in order to send SMS messages in the case of a power failure.

8. Plug the USB connector from the serial-to-USB cable into one of the USB ports on the NetAgent;
9. Use the web interface to configure the NetAgent to use the GPRS modem:
    a. Connect to the NetAgent web interface by entering the IP address of the device in a web browser address bar or by selecting the correct NetAgent in Netility and clicking **Launch Web User Interface**;
    b. Click **Configuration**;
    c. Click **SMS Modem**;
    d. Select **ttyUSB0** for the **Modem Communication Port**;
    e. Select **GPRS** for the **SMS Communication**;
    f. Enter the correct PIN for the **SIM Card PIN**;
    g. Enter the PIN again for the **Confirm SIM Card PIN**;
10. Use the web interface to confirm the modem is configured correctly:
    a. Click **Information**;
    b. Click **SMS Modem Status**. The modem manufacturer, model, and firmware version should be displayed under the **Modem Information** tab;
    c. Click the **GSM Modem Current Status** tab;
    d. Confirm that the modem is connected to the correct service provider;

e. Confirm that the modem has an adequate signal;
f. Confirm that the **SIM card PIN is correct or not** status indicates **SIM card PIN correct or no PIN configured**. If the SIM card PIN is incorrect, the modem will be unable to send SMS messages;

11. Send a test message to a cellular phone to confirm the modem will successfully send messages:
    a. Click **Configuration**;
    b. Click **SMS Modem**;
    c. Click the **Send Message** tab;
    d. Enter the 11-digit (1 + area code + prefix + number, e.g. *19585550142*) phone number of the cellular phone that should receive the message. The 1- prefix *must* be included or the message will not be successfully sent;
    e. Enter a short message to be sent as the content of the text message;
    f. Select the **Character** radio button;
    g. Click **Send**. The text message should arrive at the destination cellular phone in a few seconds;
12. Use the web interface to configure the NetAgent to send event notifications over SMS:
    a. Click **SMS** under the **Configuration** menu;
    b. Select **Use Local Modem** as the **Send SMS When Event Occurs** setting. This setting will lock out the other settings on the tab;
    c. Click on the **Mobile For Event Log** tab;
    d. Enter the 11-digit (1 + area code + prefix + number, e.g. *19585550142*) phone number of the cellular phone that should receive notifications in the **Cellular Phone number1** box. The 1- prefix *must* be included or the message will not be successfully sent;
    e. Click the **Select** button to the right of the **Cellular Phone number1** box;
    f. Select **Yes** or **No** for each of the UPQ events that this number should receive notifications for.
    g. If an e-Alert Sensor is installed, click the **e-Alert Sensor** tab and select **Yes** or **No** for each of the e-Alert Sensor events that this number should receive notifications for;
    h. Click **Apply**;
    i. Close the **Select Event** window to return to the regular NetAgent configuration window.
    j. Repeat steps **D** through **I** for any additional cellular phones for the **Cellular Phone number2** through **Cellular Phone number 8** fields;
    k. Click **Apply**;
13. Check to confirm that the notification number(s) are properly configured:
    a. Click on the **SMS Setting** tab;
    b. Enter a test message in the **Sending test SMS** field;
    c. Click the **Test SMS** button. A test SMS message will be sent to all the cellular phones configured in the list.

### 8.3.2—Connecting the GPRS Modem to a PC

Connect the GPRS Modem to a PC to send SMS notifications from one or More NetAgent devices by following these steps:

1. Unpack the GPRS modem;
2. Attach the serial connector from the serial-to-USB cable to the serial connector on the modem;
3. Push the button to eject the SIM card caddy from the modem;
4. Insert the SIM card into the caddy with the metal connectors facing up (away from the caddy);
5. Slide the SIM card caddy back into the slot in the modem, making sure it seats completely;
6. Attach the DC power plug into the power jack on the modem;
7. Plug the AC converter into a power outlet on the UPQ;
8. Plug the USB connector into the USB port on the PC;
9. Install and configure SMS Server on the PC, following the instructions in **5—Using SMS Server**.

*This page intentionally left blank.*

# 9—Legal Information


Note

For warranty information, please refer to the accompanying Q-LS manual, e.g. MNL120.

*This page intentionally left blank.*

# Appendix A—Technical Glossary

**802.11b/g:** A network frequency that complies with LAN wireless specifications created by the IEEE (Institute of Electrical and Electronics Engineers). The numbers refer to the frequency spectrums used by the network, while the letters refer to frequency extensions that enable larger, faster transmissions between two stations.

**AP (Access Point) Settings**: The settings for the network modem or connection site, including SSID, Encryption, IP address (if static), Subnet Mask, DHCP service, and RADIUS. These settings control the access into the network.

**Bootp (Bootstrap Protocol):** Using this protocol, a configuration server will assign an IP address to each device located in the network. This assignment is made automatically rather than manually.

**DHCP (Dynamic Host Configuration Protocol):** A networking protocol that reduces the need for manual configuration by automatically updating information such as IP addresses to comply with larger network policies.

**DNS Server (Domain Name System:** A system that reads and updates numerical IP addresses to find domain addresses. Commonly known as the Internet phone book, this system updates the numerical addresses without changing the corresponding domain names.

**Dynamic DNS:** A DNS Server that automatically adds or updates client sites as part of a network. This is especially helpful for cases in which the client site cannot be assigned a static IP address.

**Gateway:** A router or server used to connect between networks.

**GPRS (General Packet Radio Service):** A mobile internet service based on mobile networks such as GSM.

**GSM (Global System for Mobile Communications):** A standard assigned by ETSI (European Telecommunications Standards Institute) to distinguish protocols for mobile system networks. This system is intended for second-generation mobile phone internet use.

**HTTP (Hypertext Transfer Protocol):** The protocol used to program the World Wide Web. Many URLs include the term as a prefix.

**HTTPS (Hypertext Transfer Protocol Secure):** A protocol used to securely trade online information.

**IP Address:** A set of identifying number assigned to each computer on a network. The IP address divides the numbers with periods.

**IP Allocation:** The method by which an address is assigned to a server: Static and Dynamic IP address assignment are two examples.

**IP Filter:** A feature that filters out information with certain data, such as destination address, source address, or type.

**LAN (Local Area Network):** Computers connected to a network accessible only within a specific space or area.

**MAC Address (Media Access Control Address):** An address identifying device hardware that connects to a network. The method for finding this address varies, depending on the type of hardware and the software installed.

**PIN (Personal Identification Number):** A unique, user-programmed set of numbers used to access personal information.

**PPPoE (Point-to-Point Protocol over Ethernet):** A specification used for connecting a single network of Ethernet users to the internet through one common connection.

**RADIUS (Remote Authentication Dial-In User Service) Server:** A server that checks a username and password before allowing access through a specific provider.

**Read/write permissions:** Control who has varying levels of access to shared file information. Read information only allows the file to be viewed, while write permission allows viewers with access to make changes.

**RPM (originally Red Hat Package Manager):** A program for installing, uninstalling, and managing software packages in Linux.

**SIM (Subscriber Identity Module) card:** A removable card that contains a circuit used to track information in mobile phones.

**SMS (Short Message Service):** A service used to send mobile text messages.

**SNMP Network (Simple Network Management Protocol):** A protocol used for configuring devices designed to use networks (servers, printers, routers).

**SSID (Service Set Identifier):** A 32-character code assigned to a wireless network. The SSID allows all wireless equipment that shares the SSID to communicate.

**SSH (Secure Shell):** An encrypted protocol that can be used to exchange information between two networked computers.

**SSL (Secure Socket Layer):** A secure internet protocol that uses key encryption to safely exchange information between parties.

**Subnet:** A set of numbers that divides an IP network into one of many portions based on certain sequences of numbers used in the IP address. Each subnet forms a kind of neighborhood in the network. The network would be more like a city made up of all IP addresses.

**Subnet Mask:** A filter that includes or excludes certain computers and servers from a connection, based on the subnet numbers included in the IP address.

**Telnet:** A user on one network computer may log in to another computer in the network using a remote connection by using this local area network protocol.

**Trap Notifications:** A SNMP feature that sends a notification from a device on a network to connected computers if the device exceeds preset parameters.

**UDP (User Datagram Protocol) Port:** A data transmission port that allows computers to receive or accept messages passed along a network. Many ports exist for a single IP address.

**USB (Universal Serial Bus):** A computer-electronics interface typically used in USB mass storage systems as well as many other applications.

**Wake on LAN:** Allows a LAN network message from one computer in the network (or installed program on that computer) to activate another computer or program connected to the same network.

**WAN (Wide Area Network):** A network that covers a larger network area than that of a LAN (such as a network shared over a large geographic region).

# Contacting Power Innovations

## Customer Support

Questions concerning the operation, repair, or maintenance of this equipment should be directed to the Customer Support Department of PI. When making such an inquiry, please provide the model number, serial number, and detailed description of the issue. To service or repair any product, the customer must obtain Customer Support Ticket number from Customer Support.

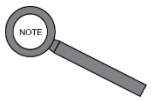
## Contacting Power Innovations

If there is any question or comment about this product, please feel free to contact us.

**Power Innovations International, Inc.**

Tel: (801) 785-4123
Fax: (801) 785-6999
Email: support@power-innovations.com

Note




This Uninterruptible Power Quality system includes the *Q-LS*, as well as any attached battery cabinets. Therefore, by extension, the ETL Listed Conformance notice on the *Q-LS* cabinet also indicates that the battery cabinets in the system conform to UL STD 1778 and are certified to CSA std. C22.2 No. 107.3. Battery cabinets as well as *Q-LS* cabinets have been tested and approved by ETL (Intertek).