
# SmartZone™ Gateway EPA064

# User Manual

**Release 1.0**
**Issue 2**

# Table of Contents

# Introduction

## Overview

The EPA064 is a compact device used to monitor and control up to four PDUs and six multifunction inputs (temperature, humidity, voltage, and digital inputs).

The unit comprises both a Simple Network Management Protocol (SNMP) interface and a secure web-based interface for monitoring and management.

Some of the main features of the EPA064 unit are:

- Secure web management and configuration interface.
- SNMP enabled.
- Six monitoring channels.
- Monitoring of up to four PDUs.
- Optional LCD Status module.

## Safety and Installation Statement

### Grounding

This is a Class I product using double insulation to provide electrical safety of the product form the main power source.


For correct operation and compliance with Class A and Class B electromagnetic emission compliance and improved safety the 4mm earth stud (labeled “Earth” on rear face of unit) must be connected to an electrical earth ground.

If the network covers an area served by more than one power distribution system, be sure their electrical safety grounds are securely interconnected.

Network cabling may occasionally be subject to hazardous transient voltages (such as lightning or disturbances in the electrical utilities power grid). Handle exposed metal components of the installation with caution.

### Servicing

There are no user-serviceable parts inside these products. Any maintenance or repair must be performed by approved service-trained personnel.

This product does not have a power switch; it is powered on when the adapter's power cord is plugged in.

## -48v DC Supply

A readily accessible disconnect device must be incorporated in the supply external to the equipment. This must have contact separation of at least 1.5mm in the open (disconnect) position.

Over-current protection is required with a maximum rating of 5 Amps.

# Waste Electrical and Electronic Equipment (WEEE) Statements

## Disposal of Waste Equipment by Users in Private Household in the European Union

This product must not be disposed of with your other household waste. It is your responsibility to dispose of your WEEE equipment by handing it over to a designated collection point for the recycling of waste electrical and electronic equipment.

For more information about where you can drop off your waste equipment for recycling, please contact your local city or council office, your household waste disposal service or the organization where you purchased the product.

CE EC Declaration of Conformity
In accordance with EN ISO 17050-1:2005

In accordance with the following Directives:

- 2006/95/ECThe Low Voltage Directive
- 2004/108/ECThe Electromagnetic Compatibility Directive
- 2002/95/EC The Restriction of the Use of certain Hazardous Substances in Electrical and Electronic Equipment (RoHS)
- 1907/2006/ECThe Registration, Evaluation, Authorization & Restriction of Chemicals. (REACH)

The equipment: SmartZone EPA064
Model Numbers:
Is in conformity with the applicable requirements of the following documents

| Ref No. | Title |
|---|---|
| BS EN 55022:2010 | Information technology equipment. Radio disturbance characteristics. Limits and methods of measurement. Class A. |
| BS EN 55024:2010 | Information technology equipment. Immunity characteristics. Limits and methods of measurement. |
| BS EN 60950-1:2006+A12: 2011 | Information technology equipment. Safety. General requirements |

# SmartZone Gateway Applications

## Remote Temperature and Humidity Sensing

The SmartZone Gateway monitors temperature and humidity and raises alarms or takes action if a user-configured threshold is crossed.

## Power Monitoring

This equipment allows around-the-clock monitoring of the electrical power environment of the rack.

# Gateway EPA064 Package

## Contents

The standard EPA064 package contains an EPA064 unit with a Localized mains lead.

## Front of Gateway EPA064

The following image shows the front panel of the EPA064 unit.


## LEDs

Six LEDs can be found on the front of the EPA064 Unit. Their purpose is described below.

### Network

- **Speed (amber)**: Illuminates when a 100mbps connection is used.
- **Network Link (green)**:  Embedded in the RJ45 Ethernet connection. Illuminates when the Ethernet link is established. Flashes with network activity.

### Status

- **CPU:** Indicates system activity.
- **Alarm**: Analog Alarm (for example, Temperature, Humidity, or Voltage). Digital Alarm (for example, Open / Close contact switch).

### Power

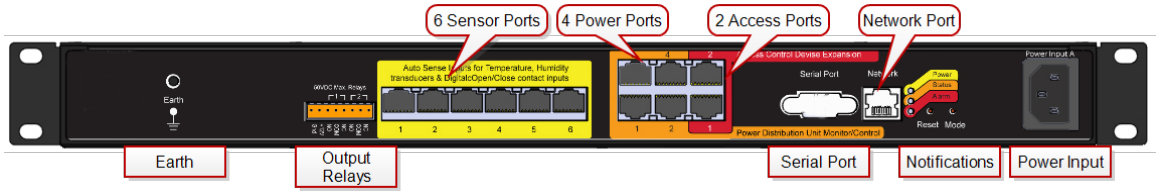
- **On**: Illuminates when the unit is powered.
- **Feed**: Illuminates when Power Supply A is functioning.

## Buttons

The EPA064 MCU also includes two buttons:

- **Reset**: Allows the user to reboot the unit.
- **Mode**: The mode select switch is used to reset the unit to factory defaults.

## Back of the Gateway EPA064

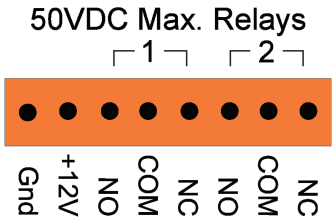



- **Earth**: Grounding stud.
- **Output Relays**: Connect up to two Output Devices (such as Front and Back Electronic Swing Handles, and more).
- **Sensor Ports 1 through 6:** Connect up to six sensors (such as Temperature, Humidity, Water, Door Contacts, and More)
- **PDU-1 through 4:** Connect up to four power devices (such as Gateway-Enabled Rack PDUs, Inline Meters, and Clamp Meters).

- **Access Ports:** Connect up to two access and control devices (such as Keypads or HID Card Readers).
- **Network Port:** An RJ-45 port to connect Gateway to LAN/Network.
- **Notifications**: Reset/Mode/Power/Status/Alarm notifications duplicated from the Front Panel.
- **Power Input**: Mains or -48v DC voltage.

## Output Relays

The following diagram shows the output relays of the EPA064 unit.

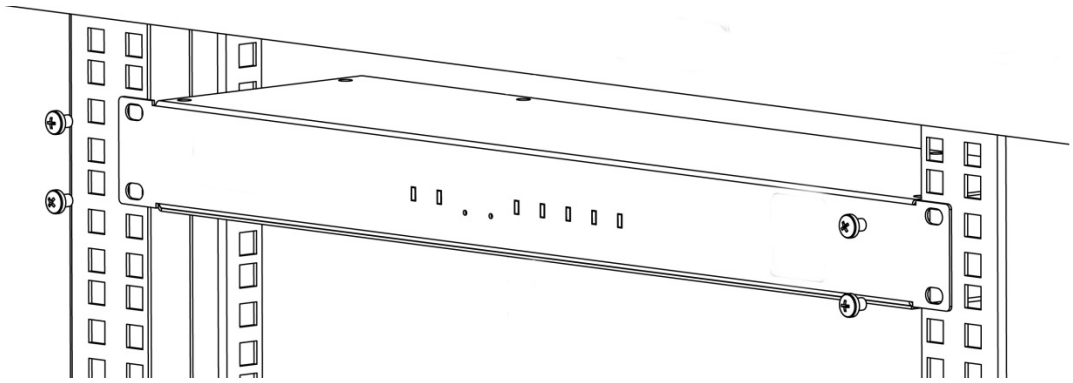


# Installation Requirements

- SmartZone Gateway unit
- Main power cable (supplied)
- 10/100baseT network connection
- Network-connected computer system to setup the Gateway
- 1 x network crossover cable
- Screwdrivers

## Attaching the Brackets

Hold the EPA064 and attach the bracket to the rack using two 12-24 screws.



# Rack Mounting

This section covers the rack-mounting of the SmartZone Gateway unit.

## Additional Equipment Required

Along with the installation requirements listed above, you need a number-1 and a number-2 Phillips screwdriver to rack-mount the SmartZone Gateway unit.

## Before You Begin

When determining where to install the Gateway, verify that these guidelines are met:

- Airflow around the Gateway unit is unrestricted.
- Front-panel LEDs can be easily read.
- Access to ports is sufficient for unrestricted cabling.
- AC/DC power cord can reach the Gateway unit.
- The 10/100 network cabling does not exceed 100 meters from the Gateway unit to the Network switch.
- Temperature around the Gateway unit does not exceed 40° C.
- Relative humidity around the Gateway unit does not exceed 90 %.

## Installation Warnings

- Only trained and qualified personnel should be allowed to install, replace, or service this equipment.
- To prevent the Gateway unit from overheating, do not operate in an area that exceeds the maximum recommended ambient temperature of 40° C.
- Installation of the Gateway unit must comply with local and national electrical codes.
- To prevent personal injury when mounting or servicing the Gateway unit, ensure that the rack or cabinet is adequately secured so that the system remains stable.
- Circuit Overloading - Consult the equipment nameplate ratings when connecting the equipment to the supply circuit to avoid overloading of circuits, which can adversely affect current protection and supply wiring.
- Maintain reliable grounding of rack-mounted equipment. Particular attention should be given to supply connections other than direct connections to the branch circuit (for example, the use of PDUs)..

# Initial Setup

## Default Settings

The SmartZone Gateway unit in factory default condition has the following network configuration. Advanced users may wish to make use of these settings to access the Gateway unit's Web Management Interface immediately and proceed with configuration.

Users who do not know how to do this should proceed through this section for information on how to configure the Gateway unit.

| | |
|---|---|
| IP Address | 192.168.0.253 |
| Subnet Mask | 255.255.255.0 |
| Default Gateway | 192.168.0.1 |
| Web Management Address | http://192.168.0.253/ |
| Default username | admin |
| Default password | admin |

**Note**: Password entries are case-sensitive.

## Connecting to the Web Management Interface

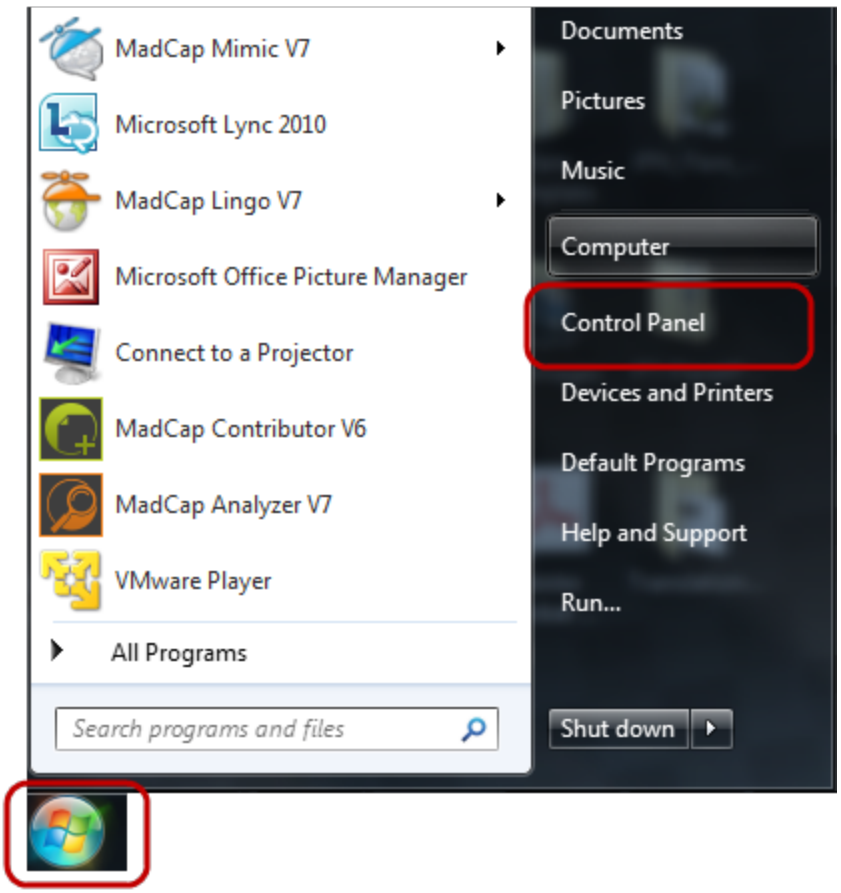
The SmartZone Gateway monitoring solution can be configured entirely using the built-in Web Management Interface.

You may need to change the IP address of the PC to connect to the Web Management Interface for the first time. The following section details how to change the IP address and connect to the Web Management Interface.

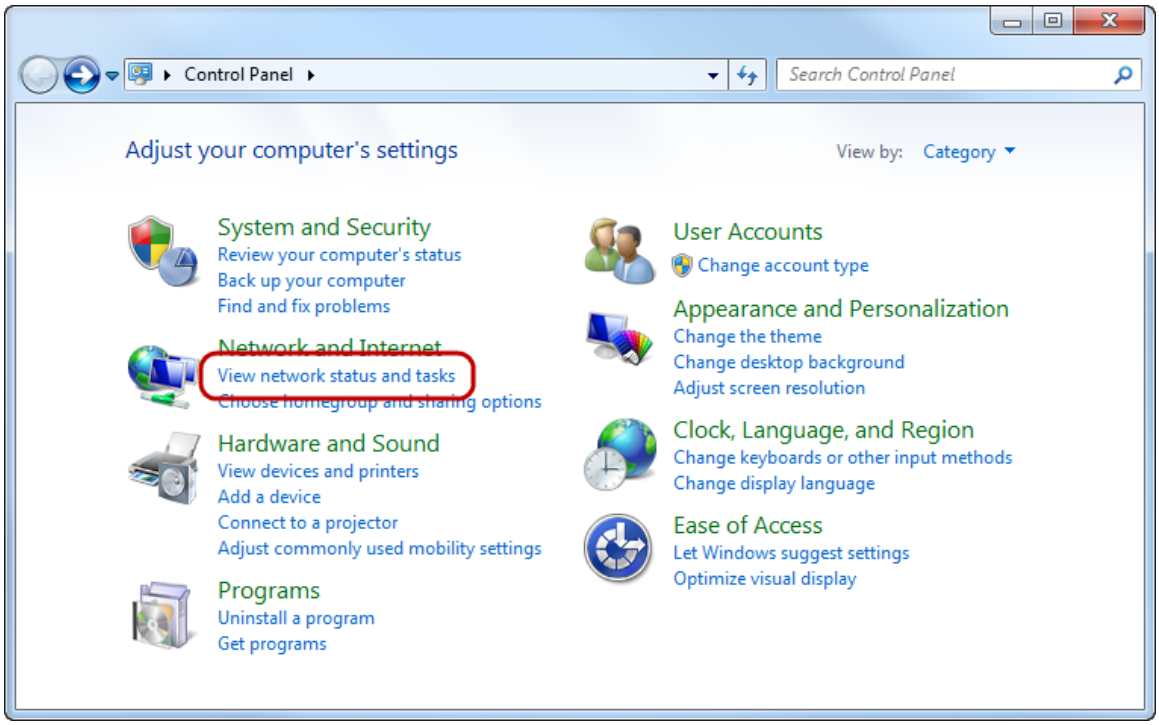
## Changing your PC's IP Address

**Note**: Instructions refer specifically to Windows 7. Please refer to your operating system documentation if you are not using Windows 7.

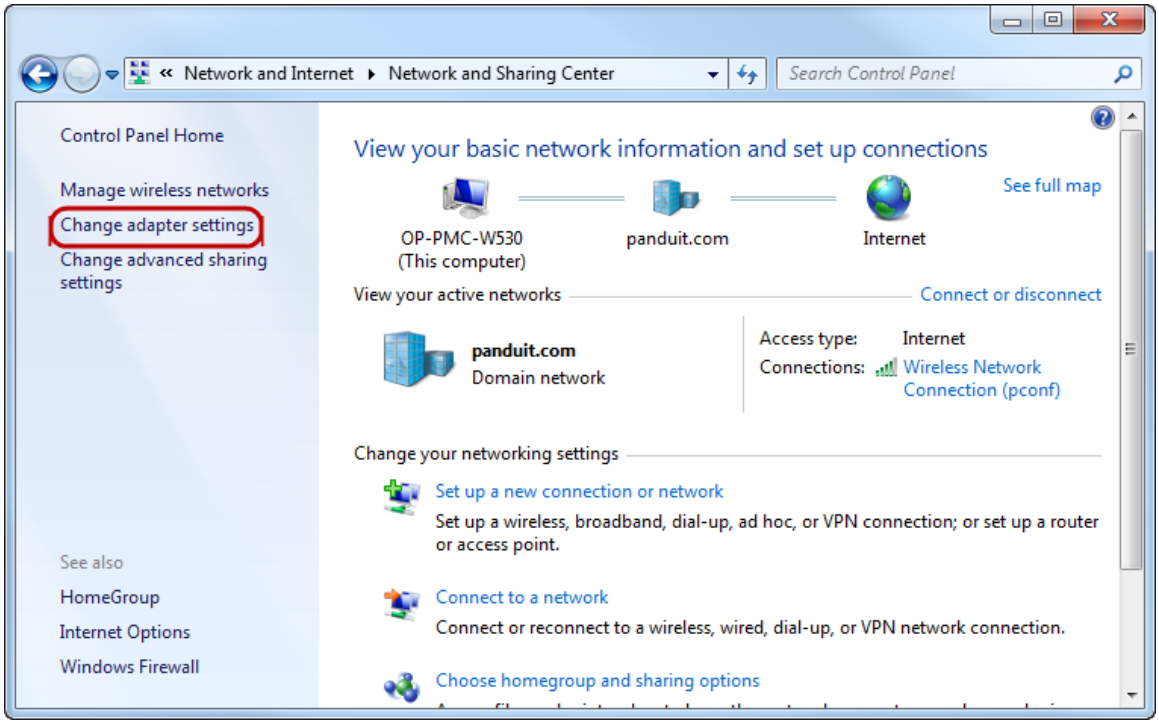
1. Click the Windows button and select **Control Panel**.



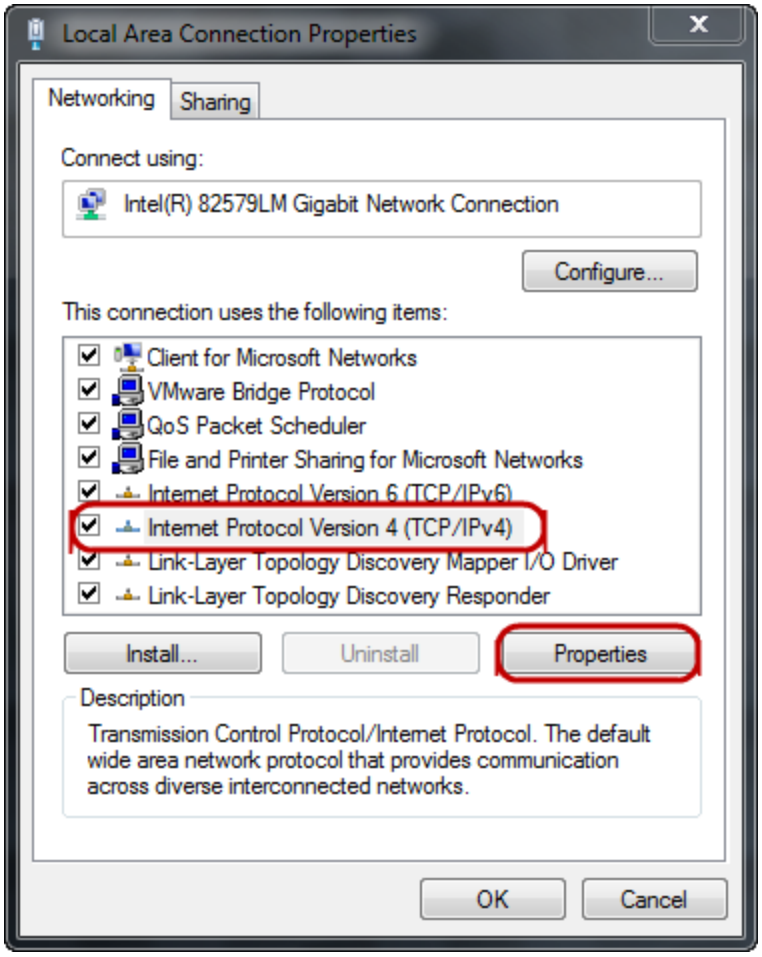

2. In the Control Panel window, select **View network status and tasks** under the Network and Internet heading.



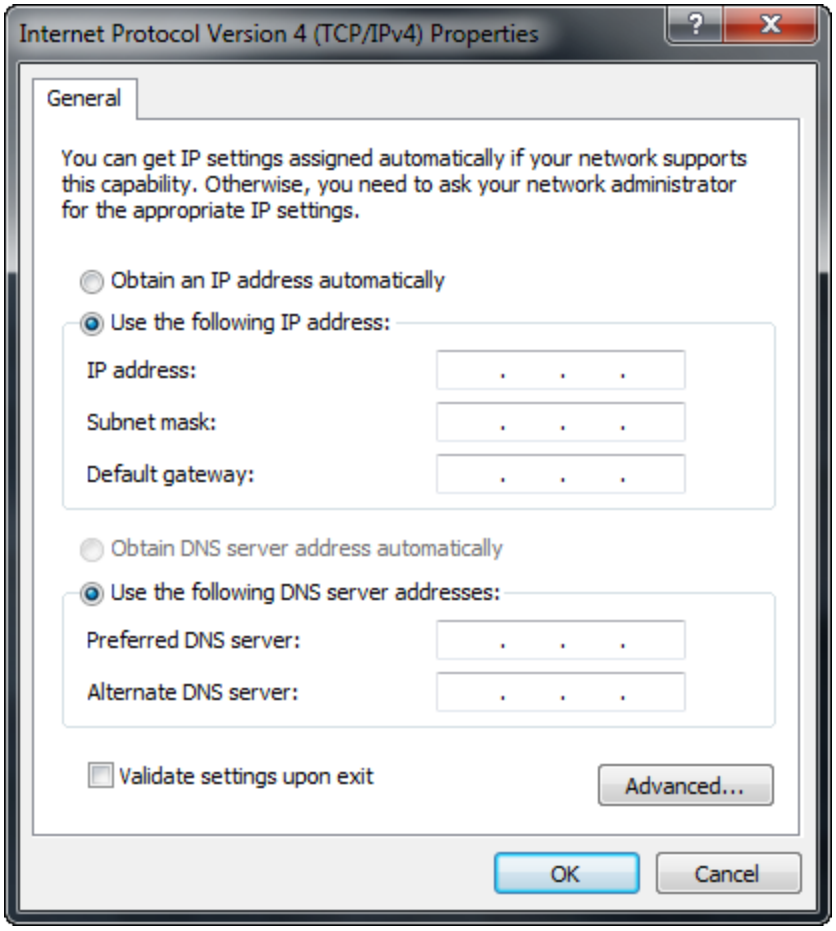

3. Select **Change adapter settings** from the menu on the left.



4. Select **Local Area Connection**.
5. Select **Internet Protocol (TCP/IP) Version 4** (you may need to scroll down). Then click the **Properties** button.



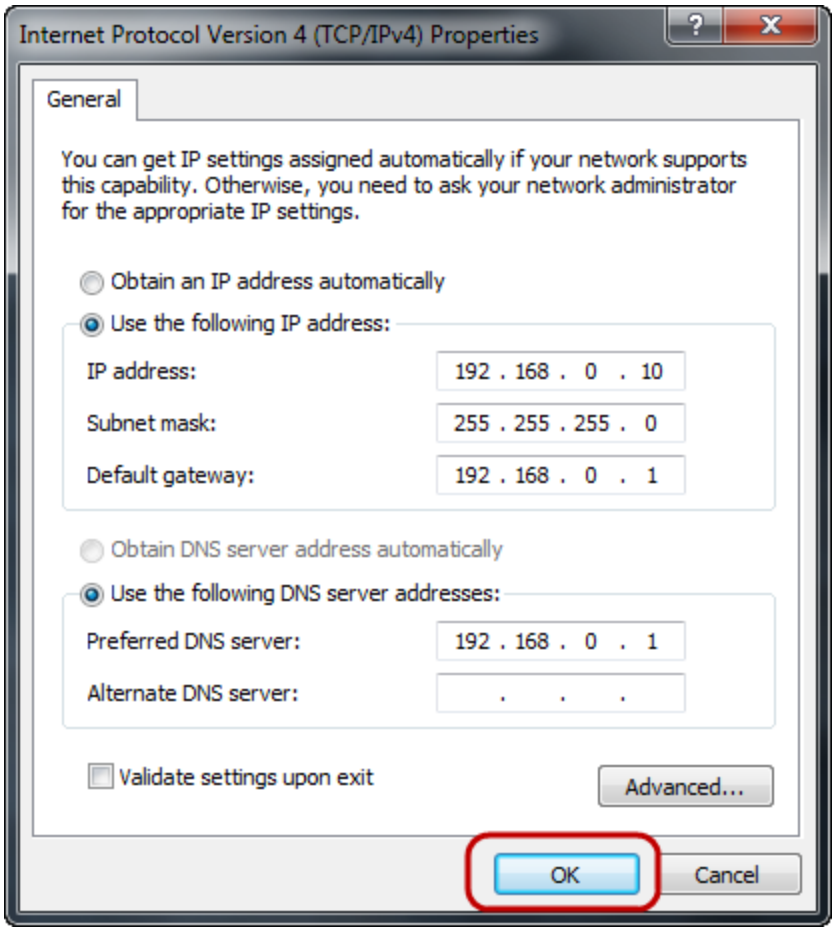

6. Select the **Use the following IP address** radio button.The **Use the following DNS server addresses** radio button then selects automatically.




Enter the following details into the appropriate boxes.

- **IP address:** 192.168.0.10
- **Subnet mask:** 255.255.255.0
- **Default Gateway:** 192.168.0.1
- **Preferred DNS server:** 192.168.0.1

7. Click **OK** to accept the entries.




8. On the Local Area Connection Properties, click **OK** to return to the desktop.

# Connecting to the SmartZone Gateway Web Management Interface

1. Connect the SmartZone Gateway unit's network connection directly to a PC's Ethernet network card using a patch cable.

**Note**: A crossover cable must be used when directly connecting the Gateway unit to a PC's network card.

2. Power the Gateway unit.
3. Open a web browser.
4. Enter the following in the address field: `http://192.168.0.253`.
5. The Web Management Interface loads.


6. Click login and enter the username and password. The unit defaults are:

- **Login**: `admin`
- **Password**: `admin`

**Note**: Password entries are case sensitive.

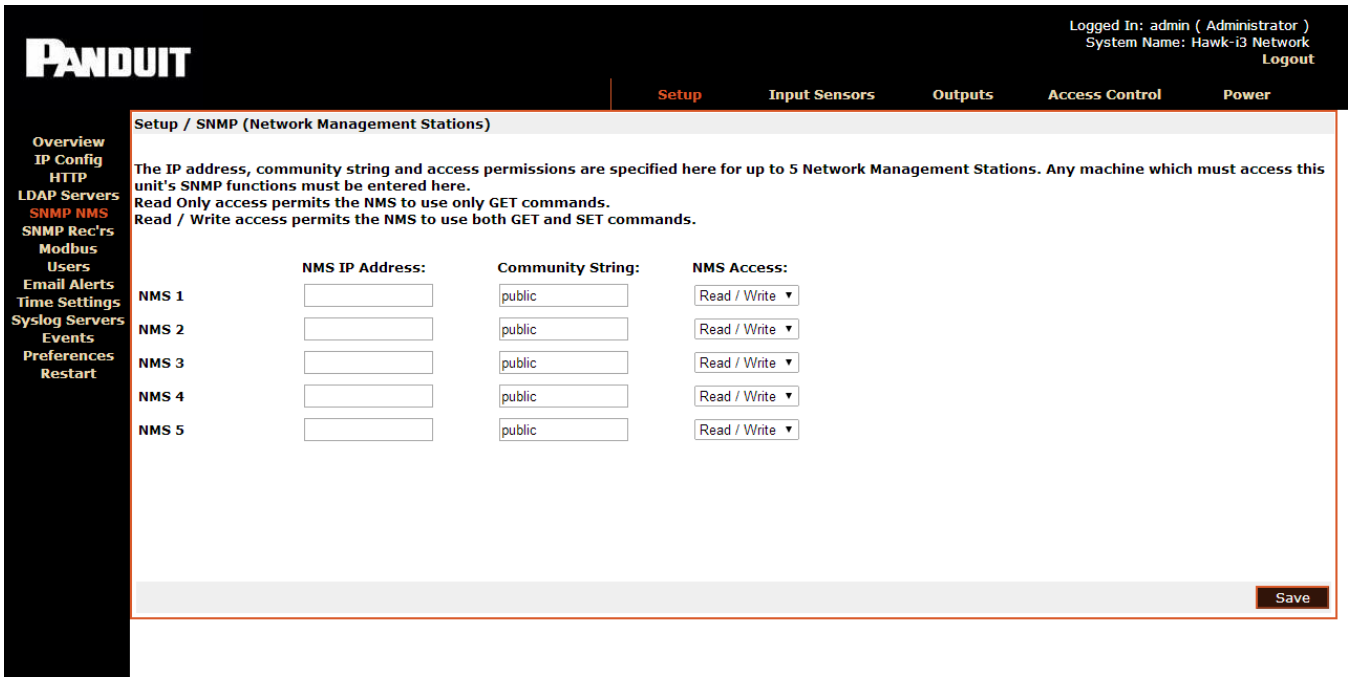
# Initial Network Setup

This section provides details on preparing the unit for network access and allowing Simple Network Management Protocol (SNMP) network management.

Connection to the Web Management Interface is required.

## Entering NMS Details

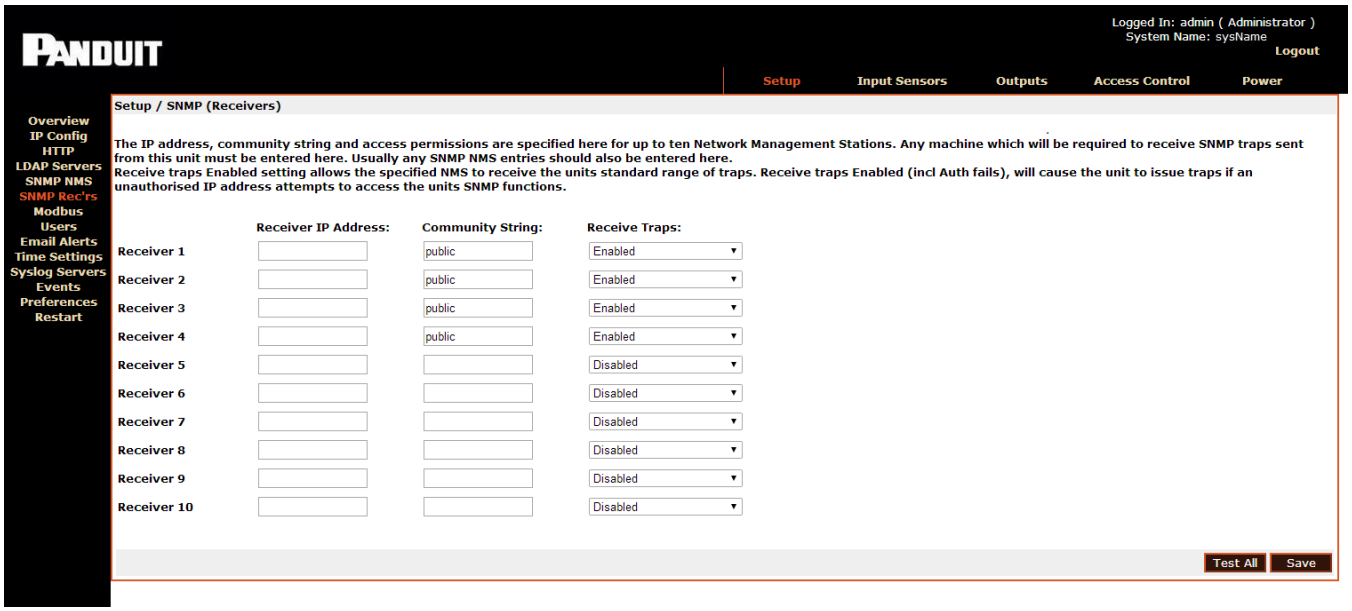
1. Click the **Setup** tab on the top menu bar, and then select the **SNMP NMS** link on the left menu bar.




2. Enter the IP address, chosen community string, and required Network Management Station (NMS) access permissions of the NMSs to be used.
3. Click **Save** to confirm the changes.
4. To disable an NMS, select the **Disabled** option from the **NMS Access** drop-down list.

## Entering Trap Receiver Details

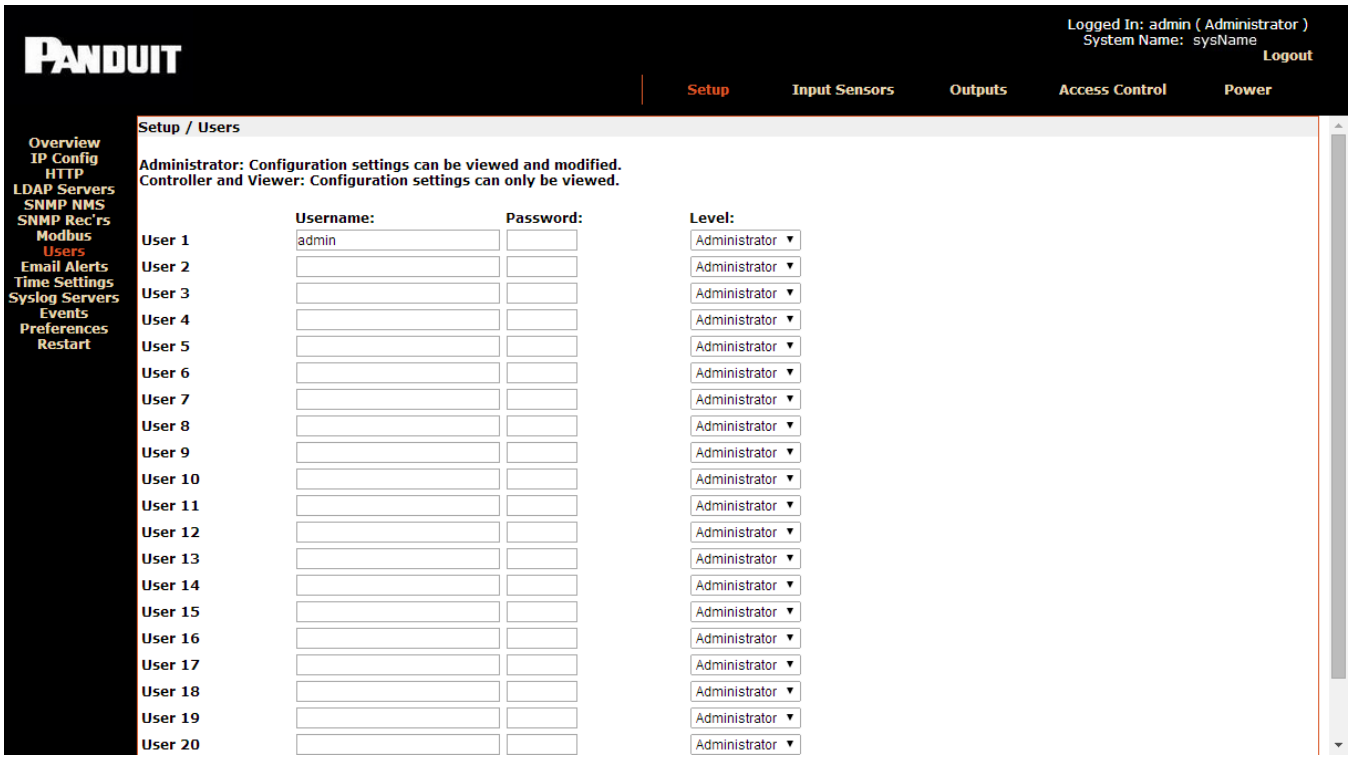
1. Click the **Setup** tab on the top menu bar.
2. Select the **SNMP Rec’rs** link on the left menu bar.




3. Enter the IP address.
4. Enter the chosen community string
5. Choose whether to enable traps, disable traps, or enable traps including authorization failures (meaning the unit will issue traps if an unauthorized IP address attempts to access the unit's SNMP functions) for each receiver.
6. Click **Save** to confirm the changes.

# Adding Users

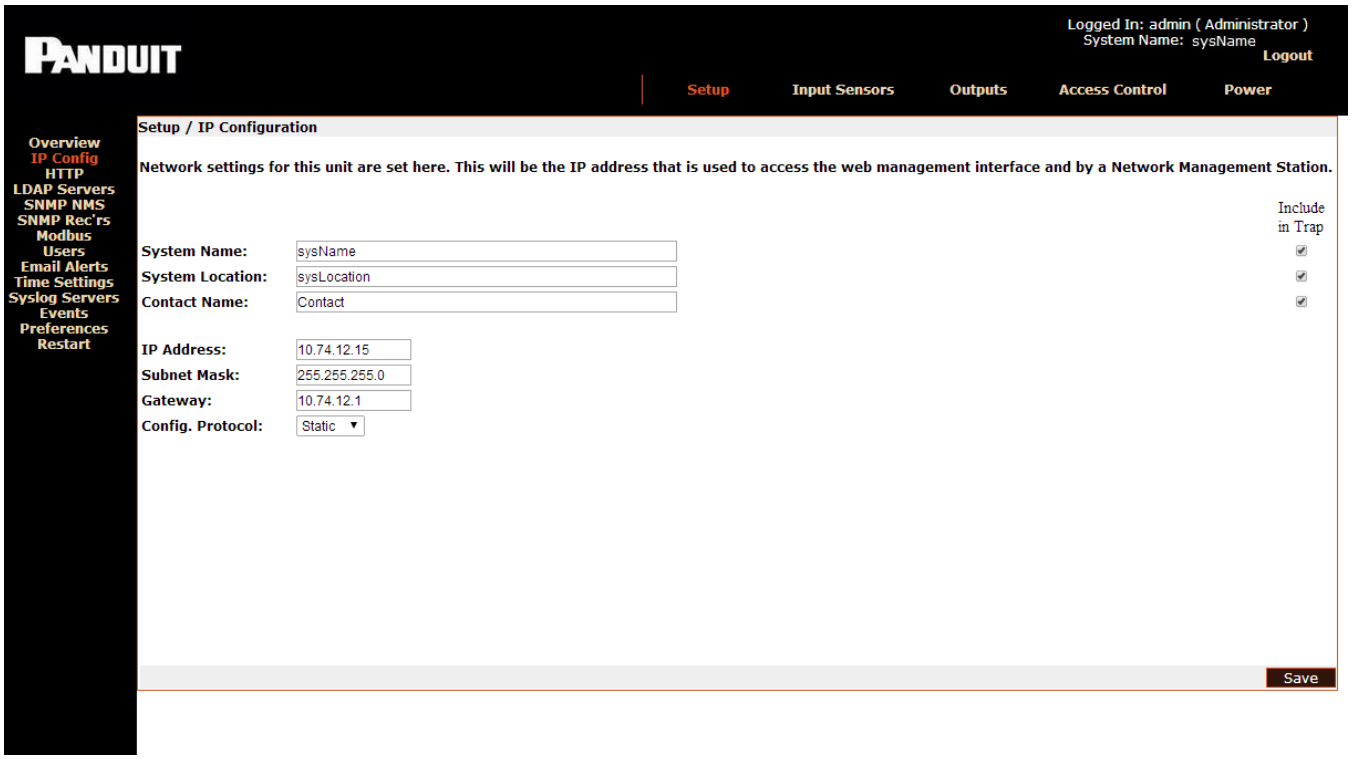
1. Click the **Setup** tab on the top menu bar.
2. Select the **Users** link on the left menu bar.




3. You can set usernames, passwords, and access levels here. Unique usernames can be set for individuals who require web management access to the Gateway unit.
4. Click **Save** to confirm the changes.

# Changing the Unit IP Address

1. Click the **Setup** tab on the top menu bar.
2. Select the **IP Config** link on the left menu bar.




3. Enter the **IP Address**, **Subnet Mask**, and the **Gateway** address that the SmartZone Gateway unit will use (required). Contact your network administrator if you do not know the values that you must enter here.
4. Select the **Config. Protocol** (Static, DHCP, or BootP).
5. Enter the SNMP **System Name, System Location** , and **Contact Name** if required. These fields will be added to all SNMP traps generated by the unit.
6. Click **Save** to confirm the changes.
7. Click **Restart** ,and then select **Restart Now** to reboot the unit and implement the changes.

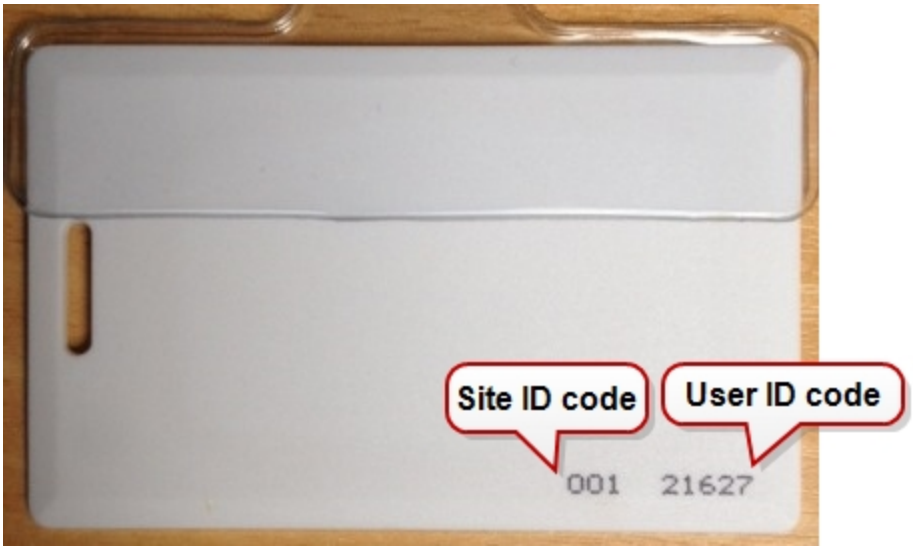
**Note**: Once the IP configuration has changed, the Gateway unit will no longer be accessible via the default IP address, because the new address will be operational.

The Gateway unit should now be connected to the main network and any further required configuration will be done via the unit's new IP address.

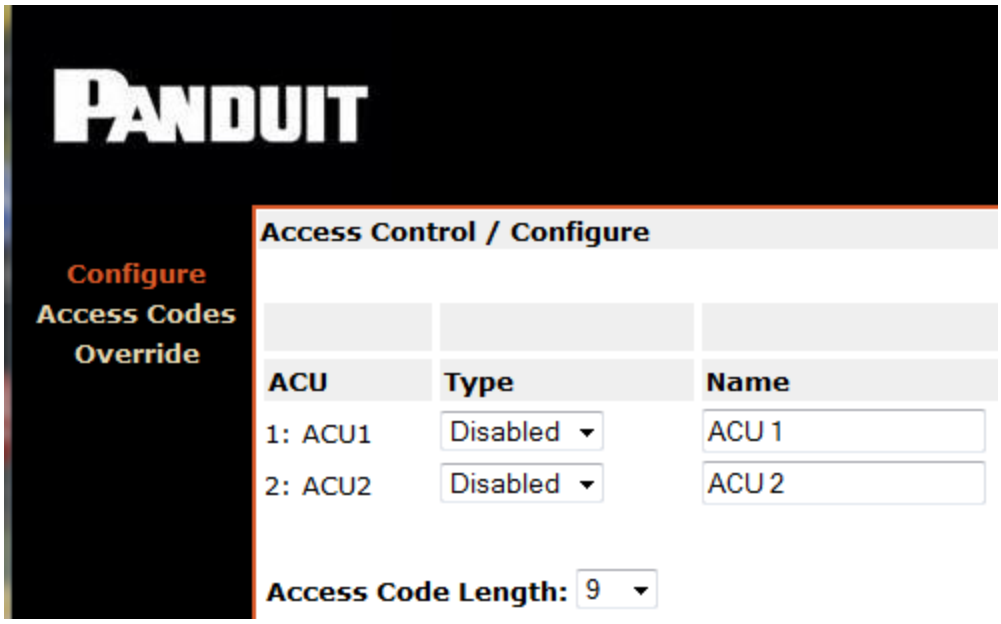
# HID Reader

The SmartZone EPA Series Gateways include Smart Card readers that support HID 26 bit cards and HID Corporate 1000 cards.

# HID 26 Bit Cards




For 26 Bit cards the Gateway interface must be programmed for nine digits.



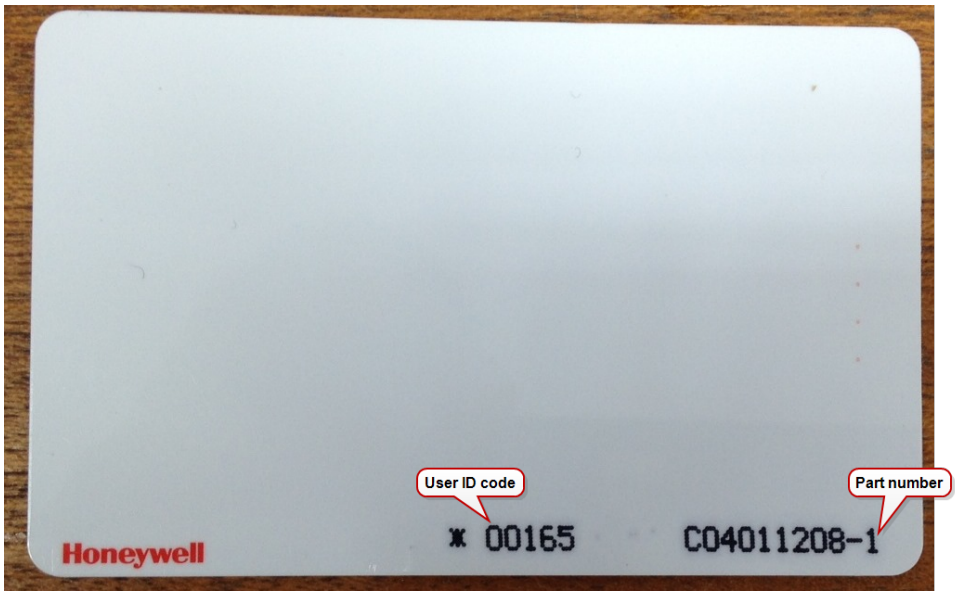

These nine digits consist of the following:

- 3-digit site code
- 1 hyphen
- 5-digit User ID code

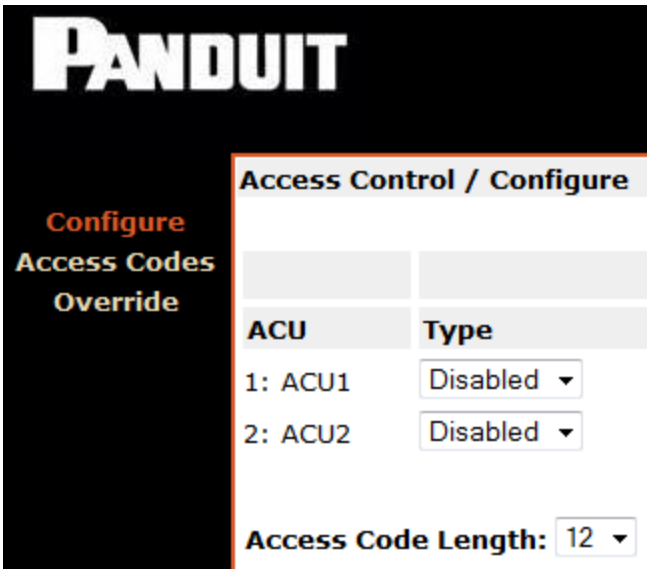
Example: 001-21627

**Note**: The hyphen character must be input (it is included in the length).

## HID Corporate 1000 Cards




Corporate Site IDs are not normally printed on HID Corporate 1000 cards. This is confidential to each organization. You will need to ask the security office of the organization or supply company for the Site ID code, which is a four-digit number.
For 34 Bit Corporate 1000 cards, the Gateway interface must be programmed for 12 digits.



These 12 digits consist of the following:

- 4-digit site code
- 1 hyphen
- 7-digit User ID code

Example: 001-21627

**Note**: The hyphen character must be input (it is included in the length).

If the user ID code does not have seven digits, then the ID number must be padded out with leading zeros. Thus an ID code of “00165” becomes: “0000165”.

Example for a card with a 2033 Site ID: 2033-0000165

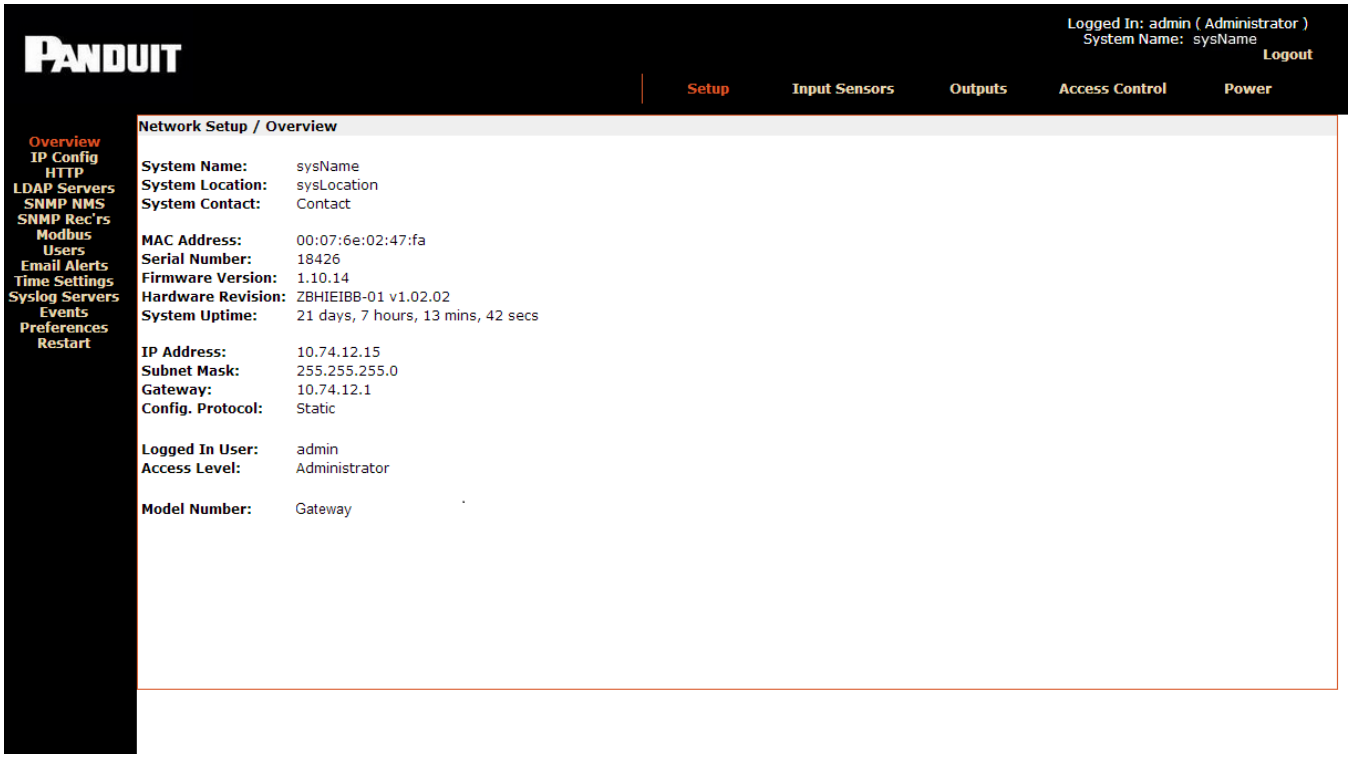
# Web Management Interface

The SmartZone Gateway unit has a built-in Web Management Interface that can be accessed securely. The interface permits complete configuration and monitoring of the Gateway unit.

Windows where changes can be made have a **Save** button in the lower right-hand area. Click **Save** to activate and save any changes made.

## Network Setup - Overview

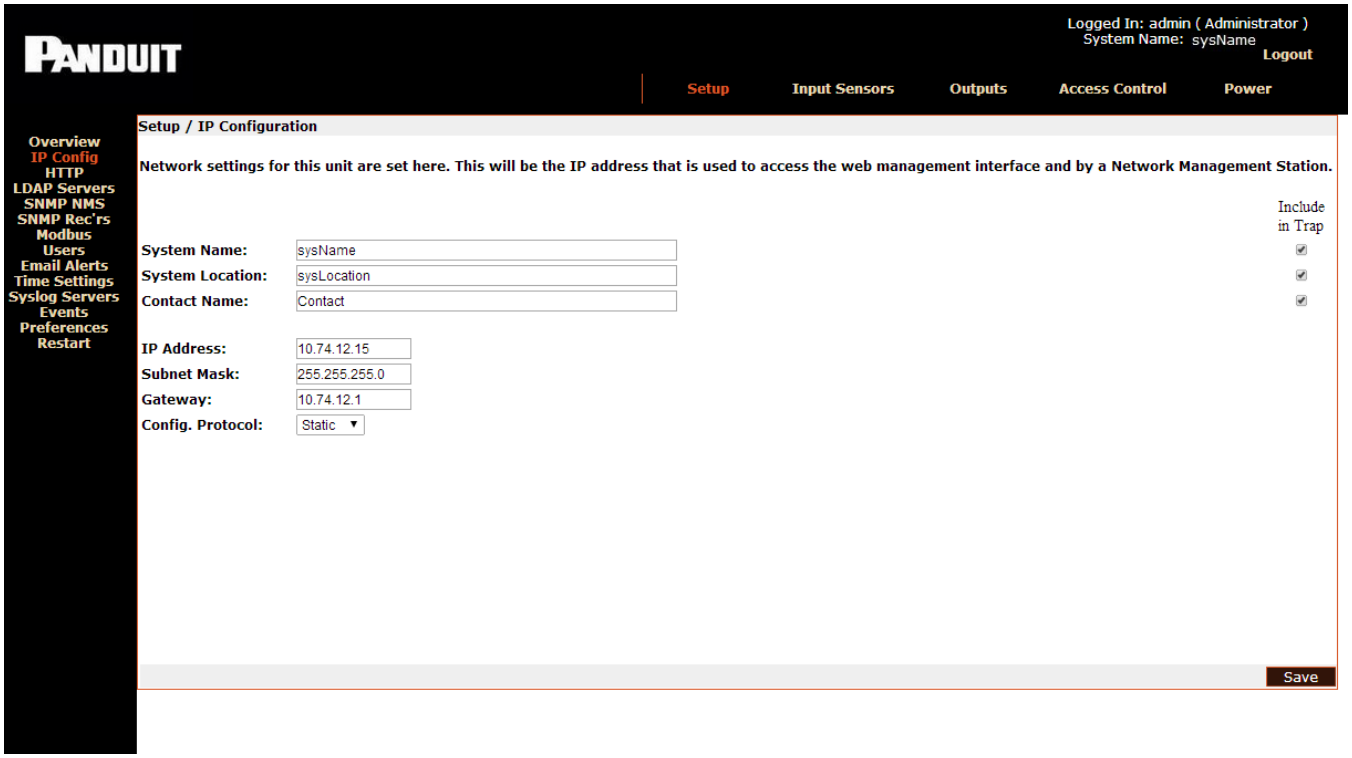
The Overview page is the first page displayed and provides the user with an overview of the Gateway unit's current status.




System name, MAC address, serial number, firmware version, and other system details can be found here.

# Setup - IP Configuration

The IP Config page allows you to set the SmartZone Gateway unit's own management IP address.




## System Name

You can specify the system name here. This is normally the Fully Qualified Domain Name (FQDN) of the device, but this is not enforced.

You can retrieve the value specified here by querying the sysName node via SNMP. This allows SNMP management platforms to obtain unique names for units where specified. This value has no effect on network communications, and the unit will function correctly with or without a value.

## System Location

You can specify the system location here.

You can retrieve the value specified here by querying the ‘sysLocation’ node via SNMP. This allows SNMP management platforms to obtain location names for units where spe-

cified. This value has no effect on network communications, and the unit will function correctly with or without a value.

## Contact Name

You can retrieve the unit support contact name by querying the ‘sysContact’ node via SNMP. This value has no effect on network communications and the unit will function correctly with or without a value.

## IP Address

You can enter a standard IP address here. The address is entered in decimal format (for example: 192.168.0.44 or 22.10.45.33).The address entered here will be the address by which the Gateway unit is accessed and managed.

## Subnet Mask

The subnet mask is used to determine what part of the IP address is the network portion and what part is the host portion.
It is often 255.255.0.0 or 255.255.255.0. The correct setting is essential for correct operation.

The subnet mask is entered in decimal format (for example: 255.255.255.0 or 255.255.224.0).

## Gateway

The Gateway setting specifies the IP address of the machine/router that the Gateway unit uses to communicate with different networks.

The Gateway address is entered in decimal format (for example: 192.168.0.1 or 11.2.24.103).

Most networks will have a Gateway. Correct setting is important for correct network communications.

## Config. Protocol

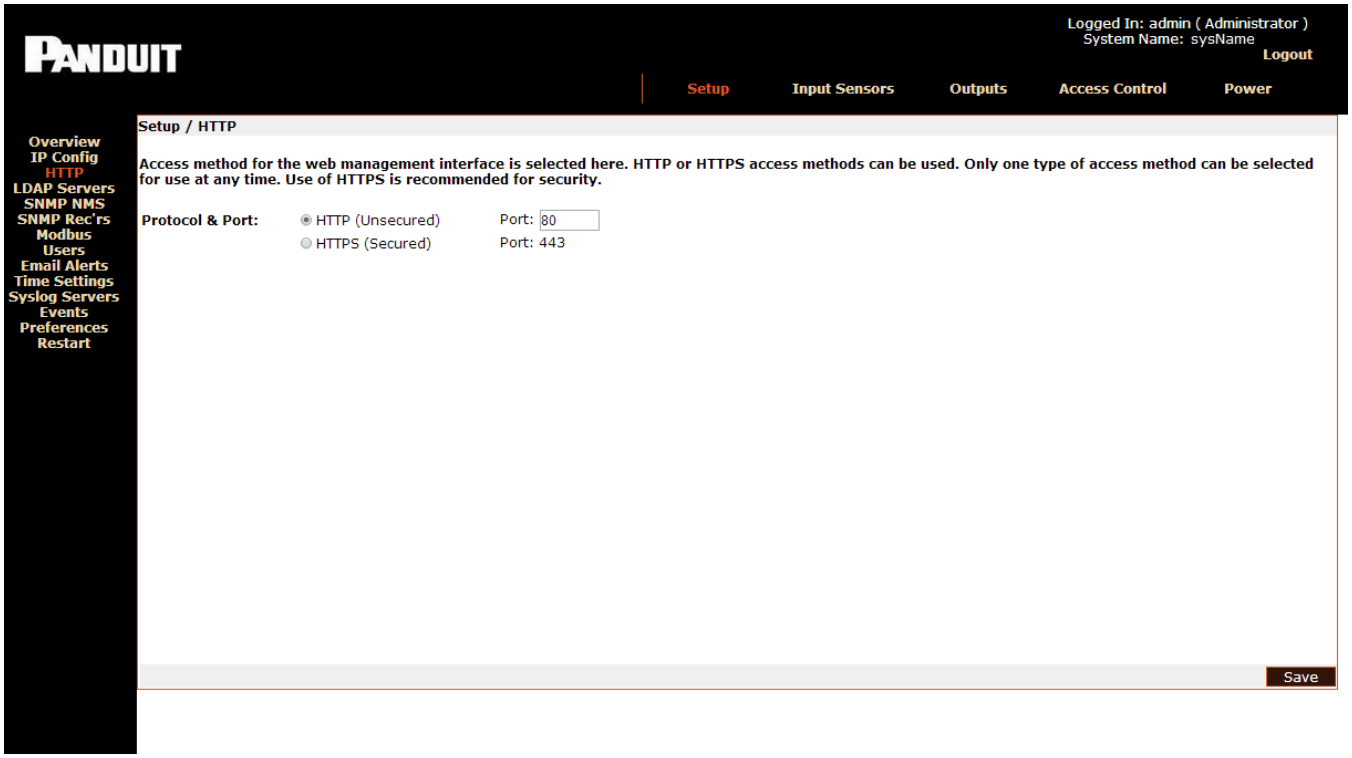
Select the configuration protocol. Choices include:

- Static
- DHCP
- BootP

**Note**: Once you enter the IP Configuration options and click **Save**, the changes take effect. If incorrect entries are made, this may result in loss of communication. If this happens, reset the Gateway unit's network configuration. Details of how to do this can be found in the Troubleshooting section.

# Setup - HTTP

Select the access method for the Web Management Interface here. Both HTTP and HTTPS access modes are available by default. Selecting the HTTPS radio button will allow only HTTPS configuration.



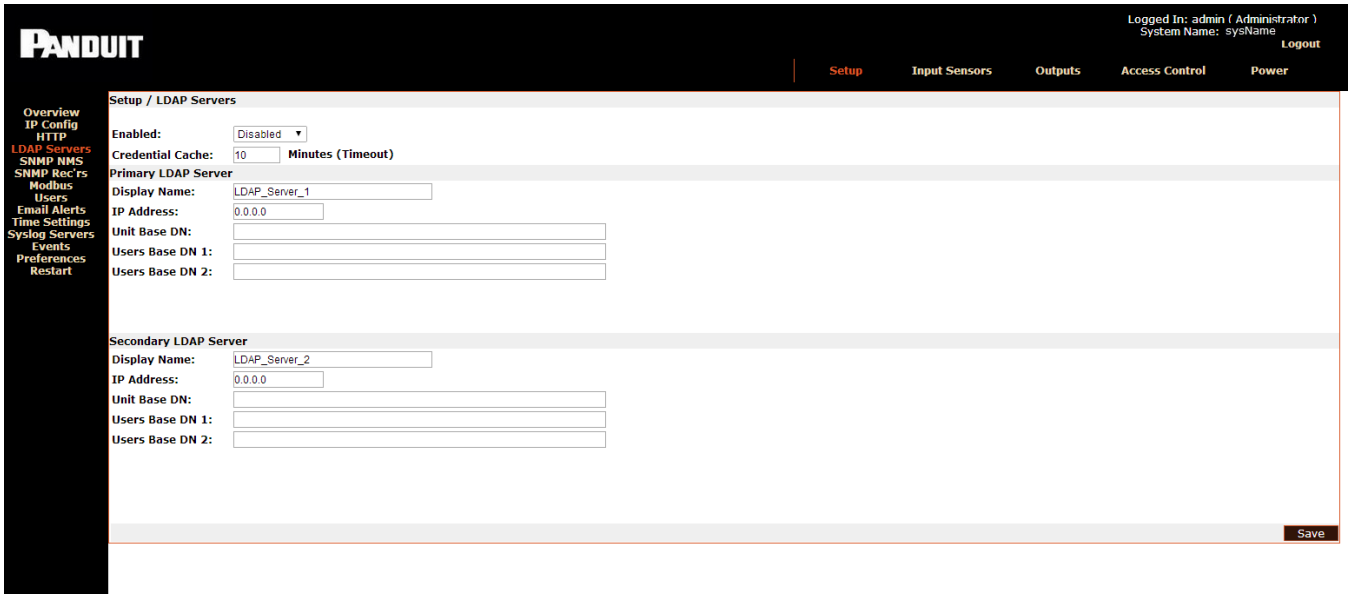

Use of HTTPS is recommended for security, because the connections will be encrypted.

Additionally, you can specify the TCP port for connection to the Web Management Interface here. If you have specific requirements for default ports, these can be left at their default settings (for example, port 80 for HTTP and port 443 for HTTPS).

**Note**: Changing the selection to HTTP or HTTPS requires a reboot for the selection to take effect.

# Setup – LDAP Servers

Lightweight Directory Access Protocol (LDAP) configuration options are specified here.




Configuration options for a Primary and Secondary server are provided with identical configuration choices.

## Enabled/Disabled

If you select Disabled, no LDAP servers will be queried to verify user login credentials' access and privileges. Only internal users will be able to log in.

## Credential Cache

This configuration option specifies how long (in minutes) users successfully authenticated via LDAP will be allowed to access the unit without re-authenticating against LDAP.

## Primary/Secondary LDAP Server

- If you specify only the Primary LDAP Server, only the primary server will be queried to verify user login credentials' access and privileges.
- If you specify only the Secondary LDAP Server, only the secondary server will be queried to verify user login credentials' access and privileges.

- If you specify both the Primary and Secondary LDAP Servers, both servers will be queried (with priority given to the Primary) to verify user login credentials' access and privileges.

## Display Name

You can create a display name for the specified LDAP server here. The Display Name is for reference and logging purposes and has no direct effect on LDAP functionality.

## IP Address

Specify the IP address of the LDAP server here.

## Unit Base DN

You must provide the Distinguished Name (DN) of the directory object containing the SmartZone Gateway LDAP authentication structure here. This field is required for LDAP function.
See LDAP for configuration details.

## Users Base DN 1

Provide the Distinguished Name (DN) of the directory object containing directory users for authentication here. This field is required for LDAP function.

See LDAP for configuration details.

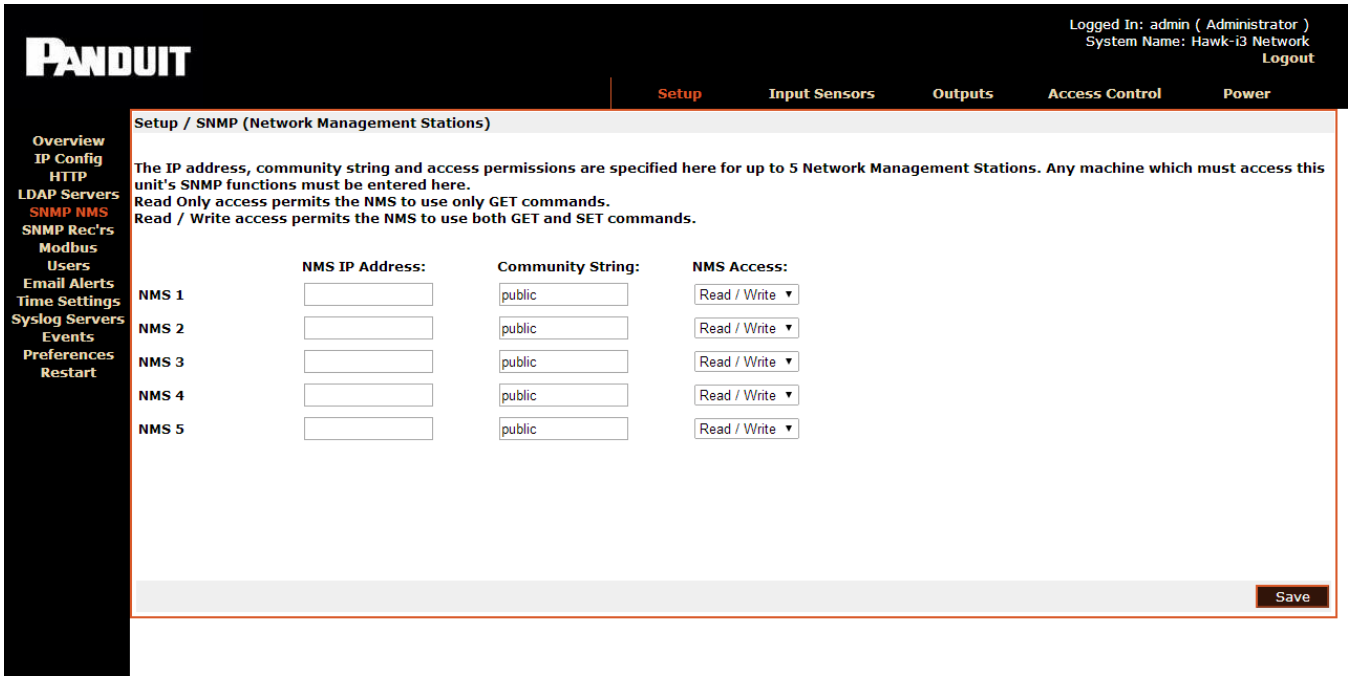
## Users Base DN 2

You can specify the Distinguished Name (DN) of the directory object containing directory users for authentication here. This field is optional for LDAP function when Users Base DN 1 has been specified.

# Setup - SNMP NMS

Specify the IP address, community string, and access permissions for up to five Network Management Stations here.

Any machine that needs to access the unit's SNMP functions must be entered here.




## NMS IP Address

Enter the IP address of the NMS machine here.

## Community String

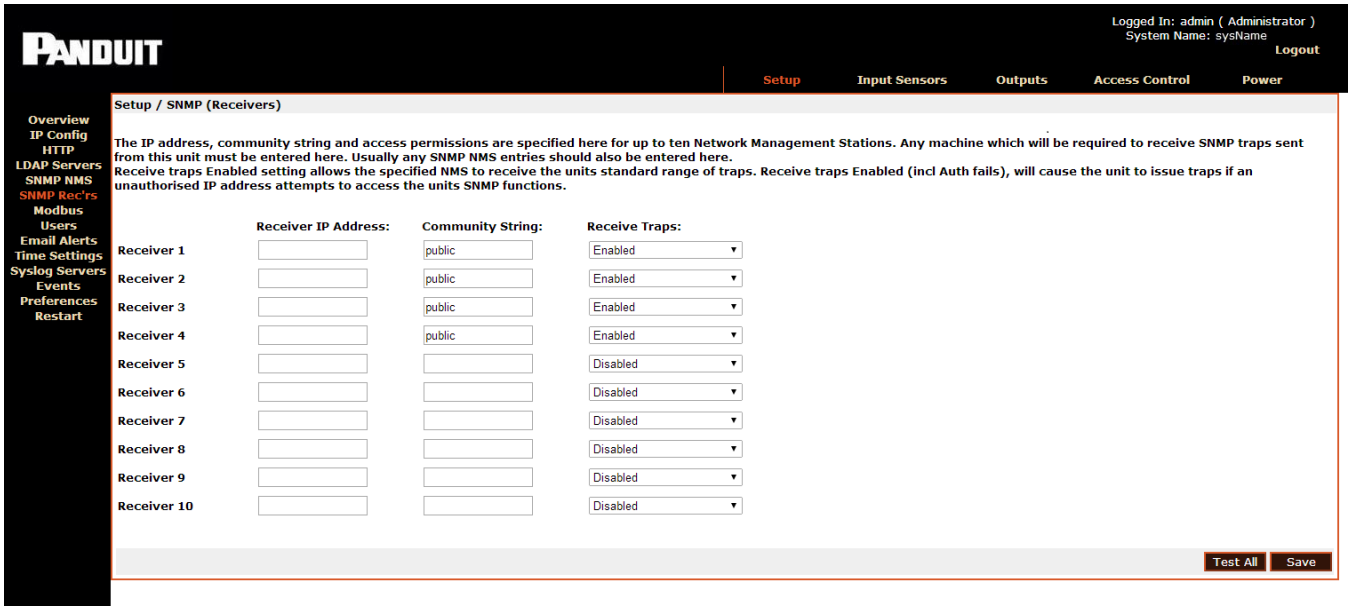
You must enter the required community string here. The default for many devices is **public**. It is recommended that the community string be changed, because it serves as an access password.

## NMS Access

Read-only access permits the NMS to use only GET commands. Read/Write access permits the NMS to use both GET and SET commands.

# Setup - SNMP Receivers

Specify the IP address, community string, and access permissions for up to 10 Network Management Stations here.




## Receiver IP Address

You must enter any machine that is required to receive SNMP traps sent from this unit. Usually any SNMP NMS entries should also be entered.

## Community String

The required community string must be entered here. The default for many devices is **public**. The community string should be changed, because it serves as an access password.

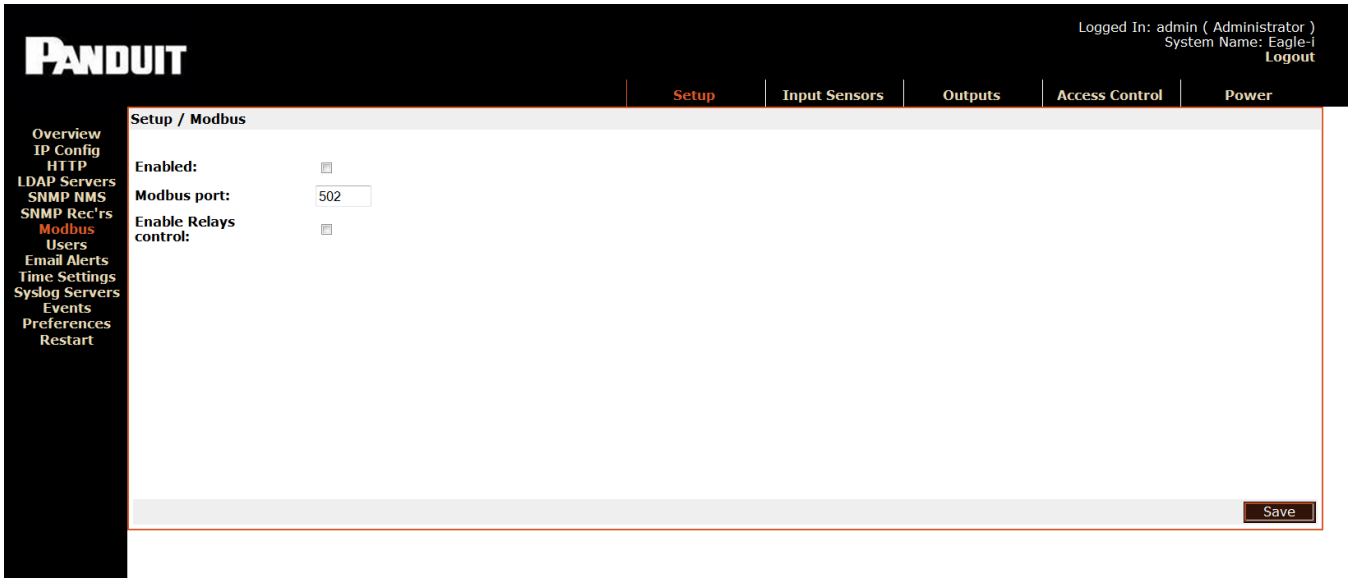
## Receive Traps

The Receive Traps **Enabled** setting allows the specified NMS to receive the unit's standard range of traps. Receive Traps **Enabled (incl Auth fails)** will cause the unit to issue traps if an unauthorized IP address attempts to access the unit's SNMP functions.

Receive Traps **Disabled** prevents traps from being sent to the specified NMS IP address.

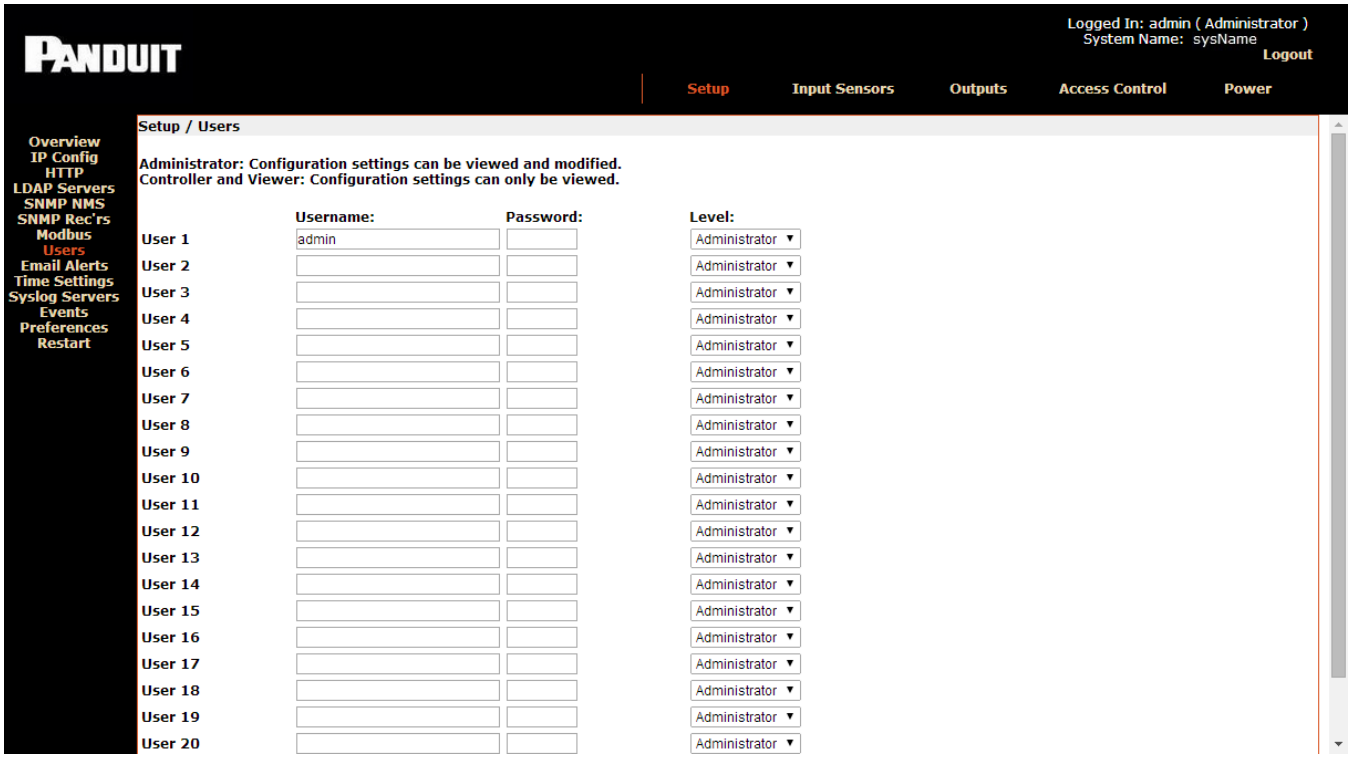
# Setup - Modbus

You can enable a Modbus communications protocol, specify the Modbus port number, and enable relays control at this window.



# Setup - Users

You can add users with permission to access the Web Management Interface here. Access passwords are also specified along with users' access permissions.




## Username

Enter the required username. This is the username that will be required to login to the Web Management Interface.

## Password

Enter access passwords on a per-user basis.

## Level

Three user levels are available for assignment.

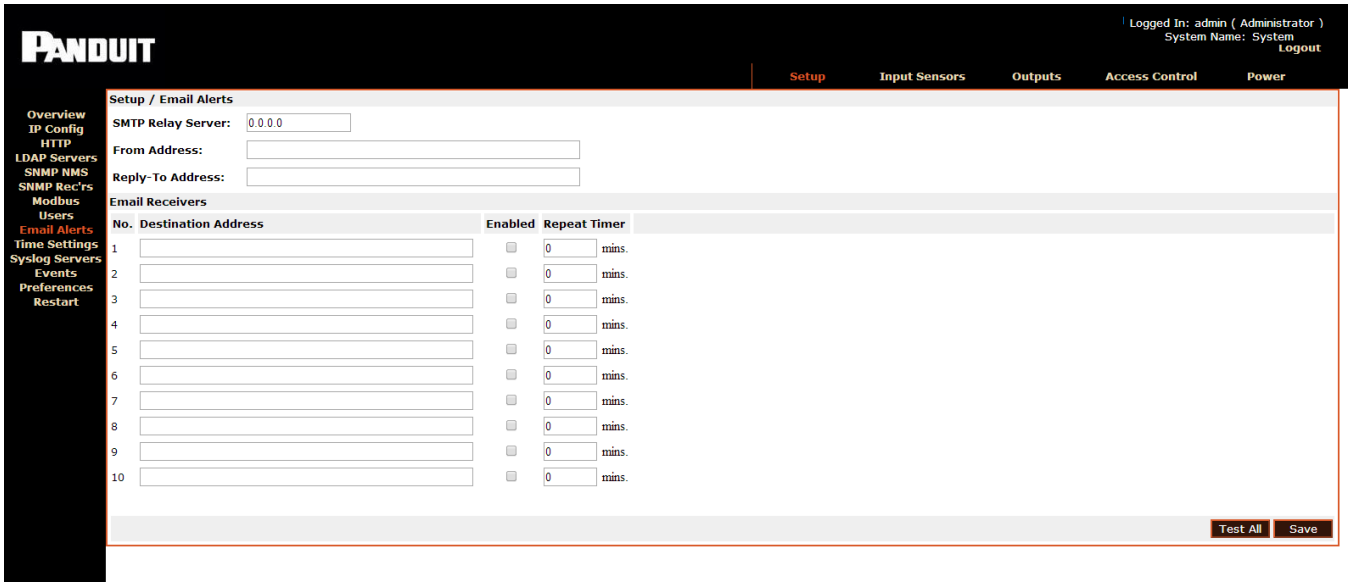
- **Administrator** : Administrators have full control of SmartZone Gateway configuration settings.

- **Controller** : Controllers can view configuration settings.
- **Viewer** : Viewers can view configuration settings.

**Warning**: User 1 / admin is the master administrator. It is possible to remove administrator rights from the admin user. Doing this is not recommended as it may result in no one having administrator access. In this situation, a reset to factory defaults is the only solution. Details on how to do this can be found in the Troubleshooting section.

# Setup - Email Alerts

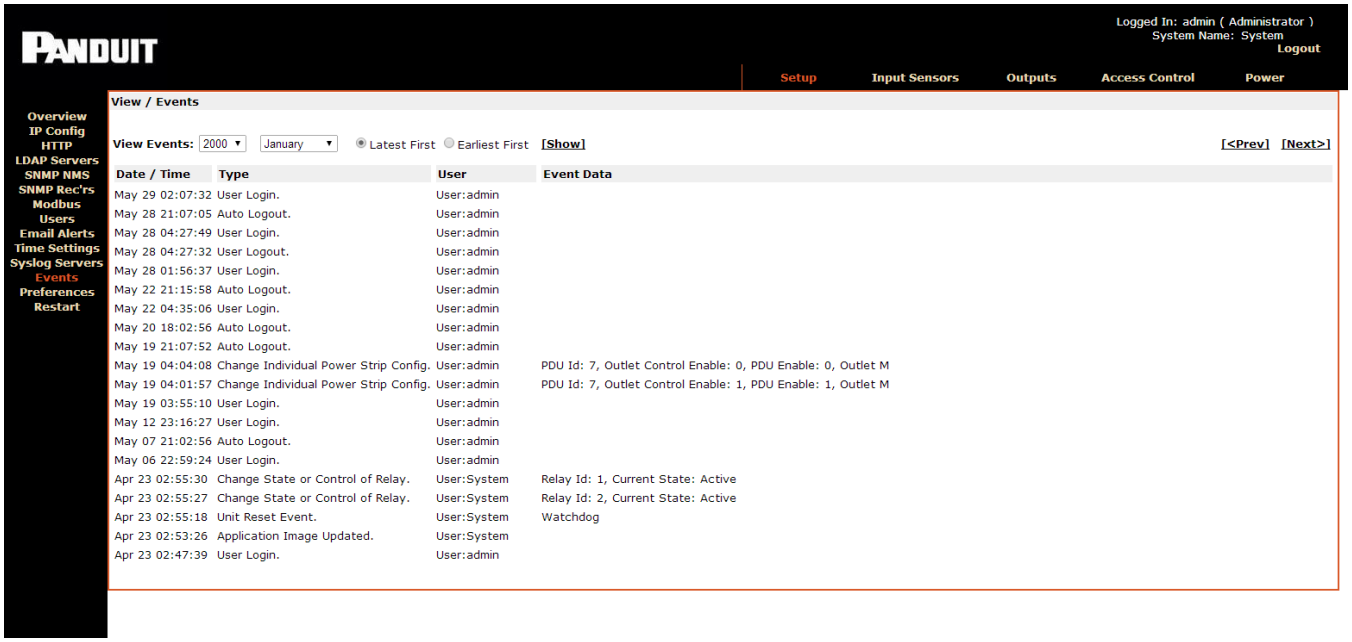
On this page, you can edit email alert settings for traps. You may set up to 10 email receivers.




| Email Alerts | |
|---|---|
| SMTP Relay Server | The IP Address of the SMTP Server |
| From Address | Address from which the alert emails are sent |
| Reply-To Address | Address to which the email receivers can reply |
| Destination Address | Address that will receive the email alerts |
| Enabled | Toggle the check box to enable or disable alerts to each address |
| Repeat Timer | Number of minutes after which the email alert will repeat |

# Setup - Events

The **Events** page shows a history of events that have occurred, along with specific details about each event.



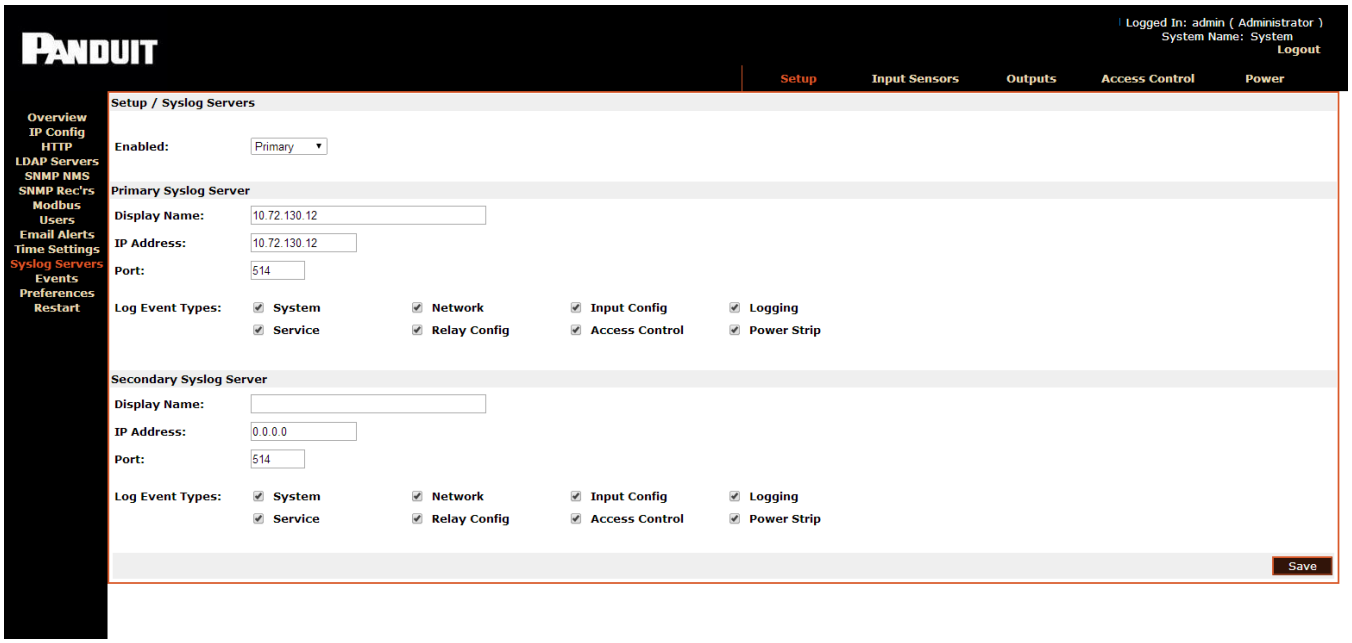

To specify a range of events to view, select the desired year and month from the drop-down menus, then click **Show**.

Date/Time, Type, User, and Event Data for each event are displayed.

Events can be ordered **Latest First** or **Earliest First** by clicking the corresponding radio button.

# Setup - Syslog Servers

This page allows you to view or edit information about the Syslog Servers currently being used.

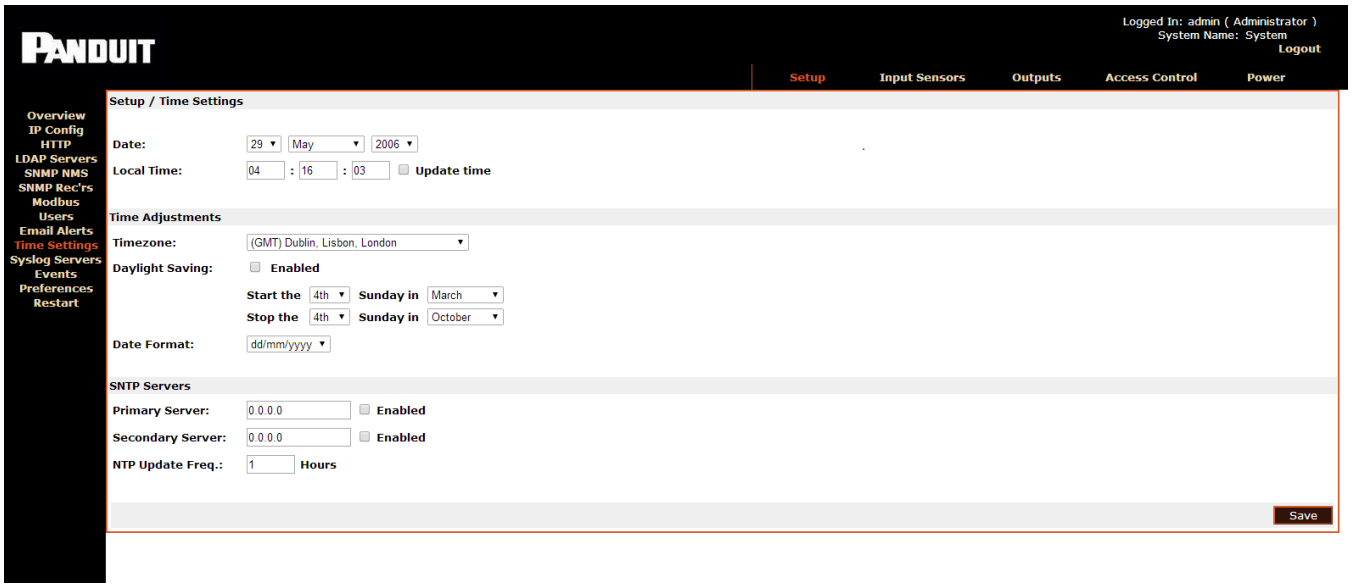



From the Enabled drop-down menu, you can choose which syslog servers are enabled. Fill in the following fields for each Syslog server.

| Syslog Server Setup | |
|---|---|
| Display Name | The name of the Syslog server |
| IP Address | The IP address of the Syslog server |
| Port | The number of the port being used |
| Log Event Types | Click the check boxes to choose which events to log |

# Setup - Time Settings

The **Time Settings** page allows you to view or edit the current date and time.




Select the correct day, month, and year from the dropdown menus, and verify the local time. If you want to change the time, you must check the Update time checkbox.

# Time Adjustments

Select the correct time zone from the drop-down menu.

- **Daylight Saving** can be enabled or disabled by clicking the check box. If Daylight Saving is enabled, select start/stop dates from the subsequent drop-down menus.
- **Date Format** allows the administrator to choose whether the date is displayed with the day or month first. For example, the date August 20, 2013 can be displayed in one of two ways:

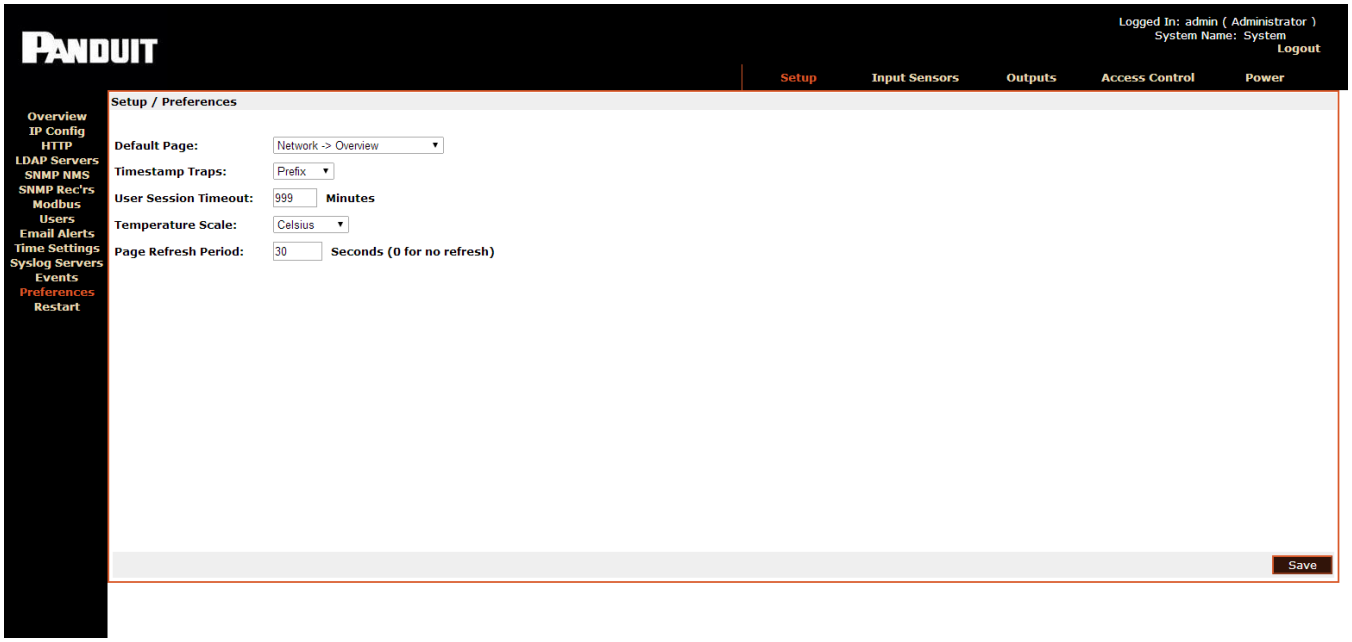
  20/08/2013 (DD / MM / YYYY)
  or
  08/20/2013 (MM / DD / YYYY)

Select the desired format from the dropdown menu.

- **SNTP Servers - Simple Network Time Protocol** synchronizes the clocks of computer systems over a network. Enter the IP address of an SNTP server, and specify (in hours) how often the time should be updated.

# Setup - Preferences

The Preferences page allows you to edit system preferences.




| Preferences | |
|---|---|
| Default Page | From the dropdown menu, select the first page you want to open when a user logs in. The preset default page is the Overview page. |
| Time stamp Traps | Choose from the dropdown menu where the timestamp will be found on traps. There are three options:<br>• Prefix – timestamp at the beginning<br>• Append – timestamp at the end<br>• None – no timestamp |
| User Session Timeout | Enter a number of minutes, after which a session will be timed out if the user is inactive. |
| Temperature Scale | Select Celsius, Fahrenheit, or Kelvin from the drop-down menu. |
| Page Refresh Period | Enter a number of seconds, after which the page will auto matically refresh. If 0 is entered, the page will not refresh automatically. |

# Setup – Restart

A unit may be rebooted or reset to factory defaults here.

## Restart Unit

### Restart Now

Selecting **Restart Now** commands the unit to reboot. Rebooting the unit will cause any outstanding configuration changes to take effect.

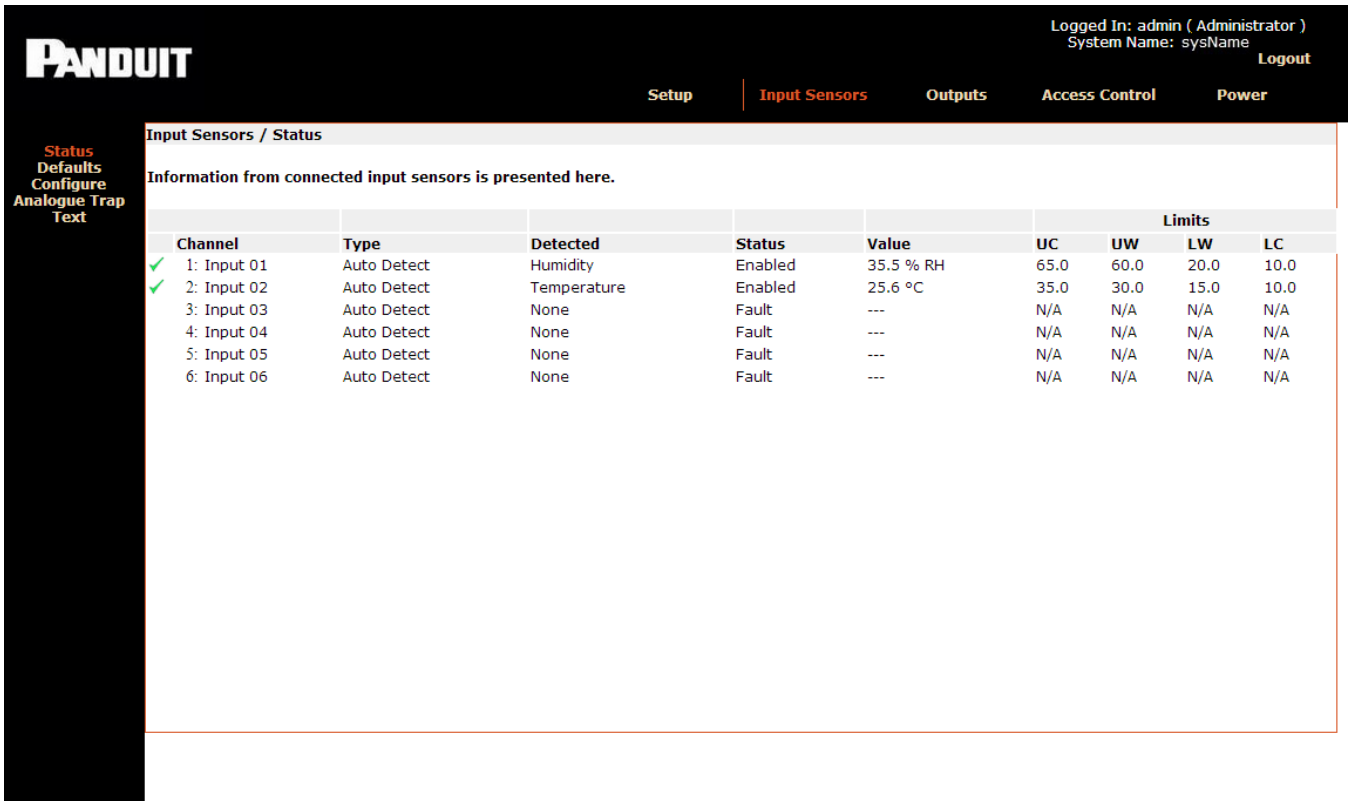
### Reset to Factory Defaults

See Troubleshooting for instructions on resetting the factory default settings for the unit.

# Input Sensors – Configuration and Status

## Status

The Input Sensors Status page presents an overview of the input ports. This page displays the input channel number, name, type of input sensor, status, current readings, and thresholds.




### Status Indicators

Three status indicators are displayed next to input channels to allow quick determination of normal, warning, and critical alarm statuses:

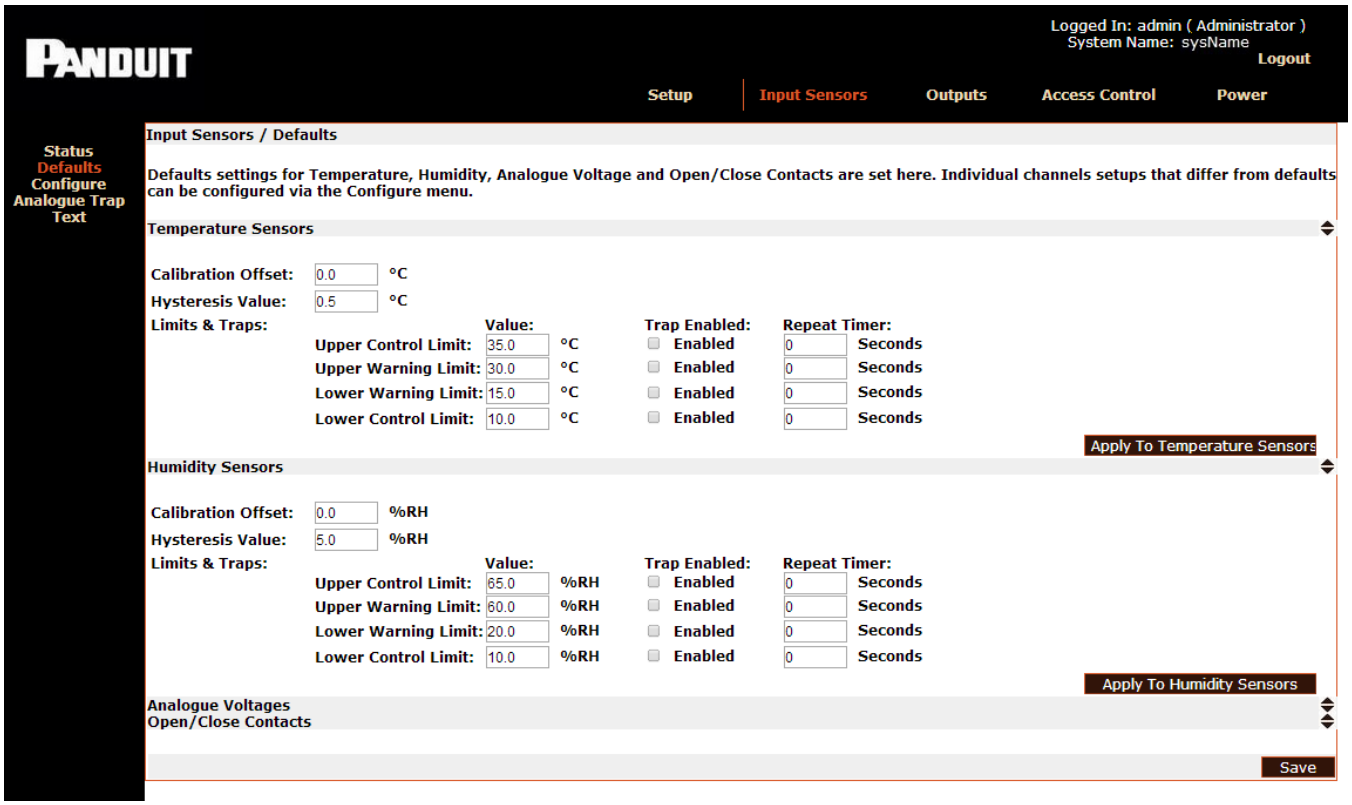
| | |
|---|---|
| ✓ | Channel reading currently within threshold limits. |
| ⚠ | Upper or lower Warning limit reached or exceeded. |
| ⊗ | Upper or lower Critical limit reached or exceeded. |

# Input Sensors – Defaults

The **Input Sensor Defaults** menu allows configuration parameters for input sensors of specific types to be defined and applied to all inputs of that type.

The types of input sensors are:

- Temperature
- Humidity
- Analog (Voltage)
- Open/Close Contacts (digital inputs)




The configurable defaults are described below.

## Calibration Offset

The value entered here alters the actual reading of a sensor by the amount specified.

For example, if a Calibration offset of 6 was used and a sensor's true reading was 36, the indicated reading used for display and alarm purposes would be 42. This works the same way for both temperature and humidity sensors.

## Hysteresis Value

The hysteresis default value to be applied to sensors is specified here. The value specified is an offset from a sensor's threshold values.

For example, a hysteresis value of 5 would mean that, in the case of an Upper Control Limits alarm, the alarm value would have to reduce to 5 below the threshold value before another alarm is issued.

Please see Appendix B: Hysteresis Demystified for detailed information.

## Limits and Traps

You can set default values for sensor alarm thresholds here. You also can set the default settings for alarm threshold traps here.

The following thresholds can be set:

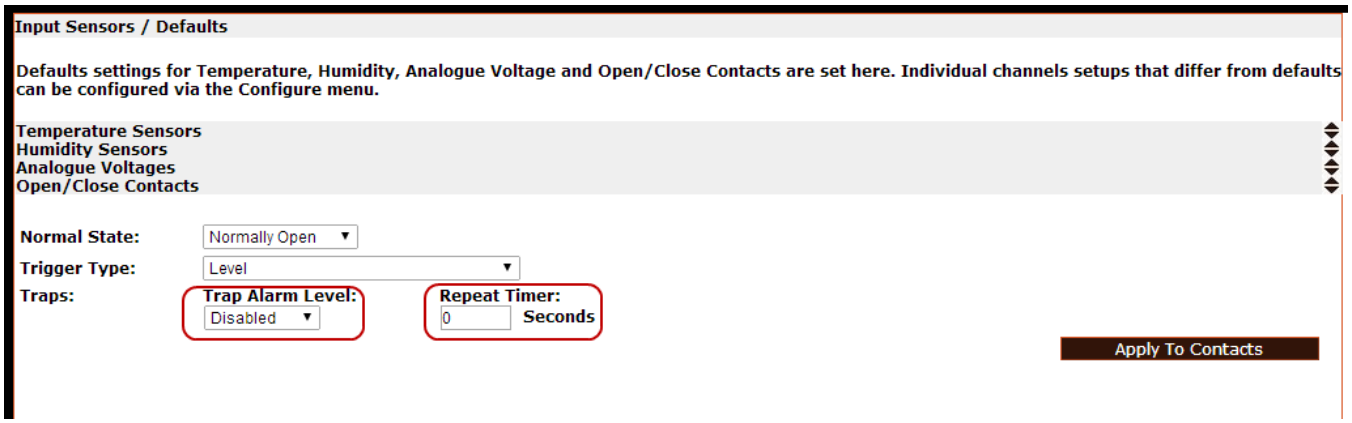
- Upper Control Limit
- Upper Warning Limit
- Lower Control Limit
- Lower Warning Limit

You can apply default trap settings for all of these thresholds by selecting the **Trap Enabled** check boxes. With the **Trap Enabled** check box deselected, no SNMP alarm traps will be generated, even when an alarm condition exists for that threshold.

## Repeat Timer

The repeat timer causes alarm traps to be reissued after a specified amount of time if the alarm condition persists.

Setting the repeat timer to 0 will disable the repeat traps.




# Open/Close Contacts

The defaults that can be set for Open/Close contacts differ from the Temperature and Humidity settings.

## Normal State

Normal state specifies the condition in which a contact is considered to be in a Normal, Non-alarmed state.

Devices such as smoke alarms and air conditioning units often have normally open contacts. To receive alarm indications from these types of units would cause alarms to be issued when a monitored contact closes.

Setting normally closed in the case of a rack or cabinet door would cause an alarm condition when the door was opened.

## Trigger Type

The trigger type defaults for Open/Close sensors are specified here.

The three available options for trigger types are:

### Level

Level triggering is the default mode. When an input physically transitions from a Normal to Non-Normal state, an alarm is triggered. However, the alarm persists only while the input remains in a Non-Normal state. When the input returns to a normal state, the alarm is cleared.

**Normal to Non-Normal (Positive Edge)**

This type of triggering may be used in situations where a momentary type input (for example,: a shock sensor or PIR) is used. Since these types of inputs are momentary, any alarm condition that occurs will persist until manually cleared.

Positive Edge triggering is used when an alarm is required to persist after an input changes from the Normal state to the Non-Normal state.

**Non-Normal to Normal (Negative Edge)**

This type of triggering may be used in situations where a momentary type input (for example, a shock sensor or PIR) is used. Since these types of inputs are momentary, any alarm condition that occurs will persist until manually cleared.

Negative Edge triggering is used when an alarm is required to persist after an input changes from the Non-Normal to the Normal state.

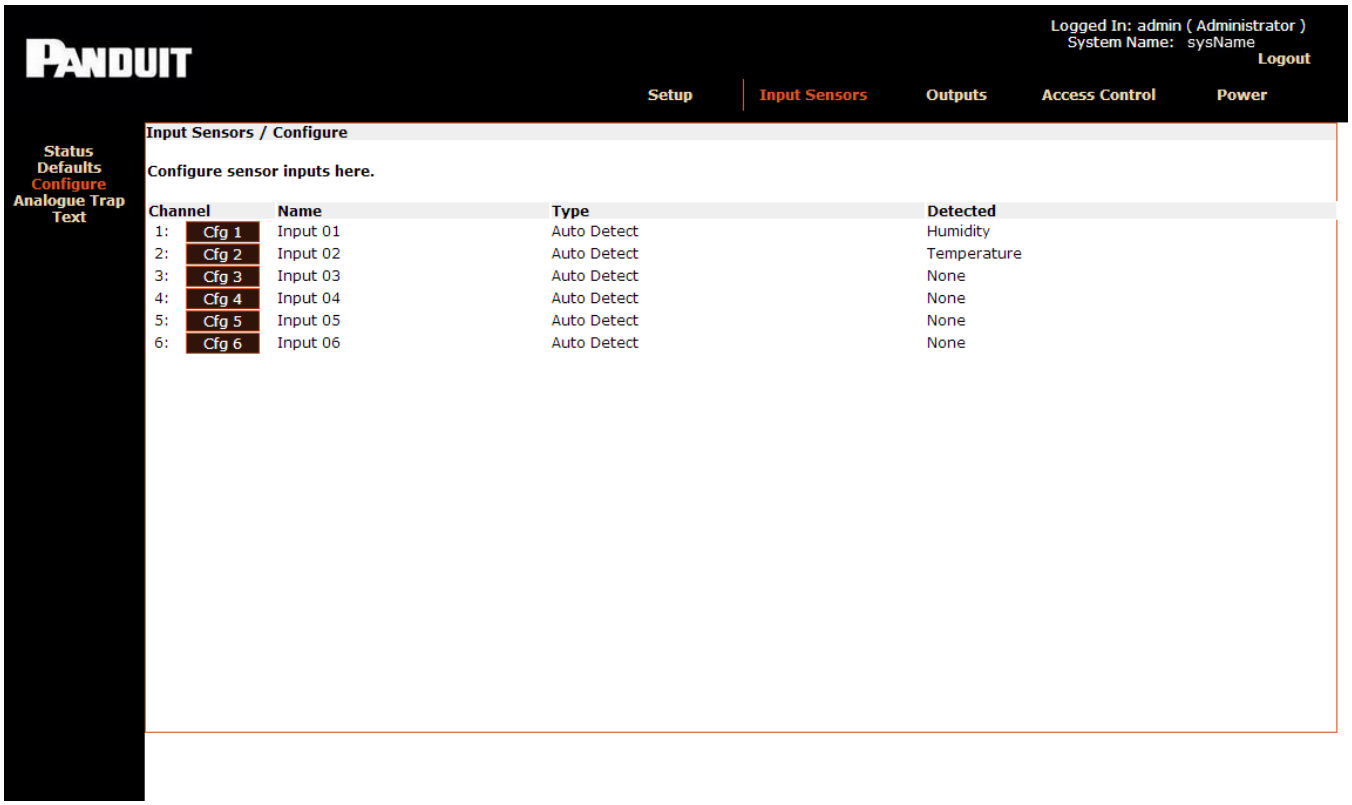
### Trap Alarm Level

Select the **Trap Alarm Level**. Options include:

- Information
- Disabled
- Critical
- Warning

## Input Sensors - Configure

You can configure the individual sensor channels in this window.




Select the **Config** option to open a detailed configuration page for the selected sensor.

The difference between the menus presented here and the menus presented on the Defaults page is that settings are applied to individual channels.

The submenus contain all the options in the Defaults menu, plus two additional options:

## Name

Sensor channels can be assigned names for ease of identification (for example, “Server Room Sensor” or “UPS Battery Fail”).

## Type

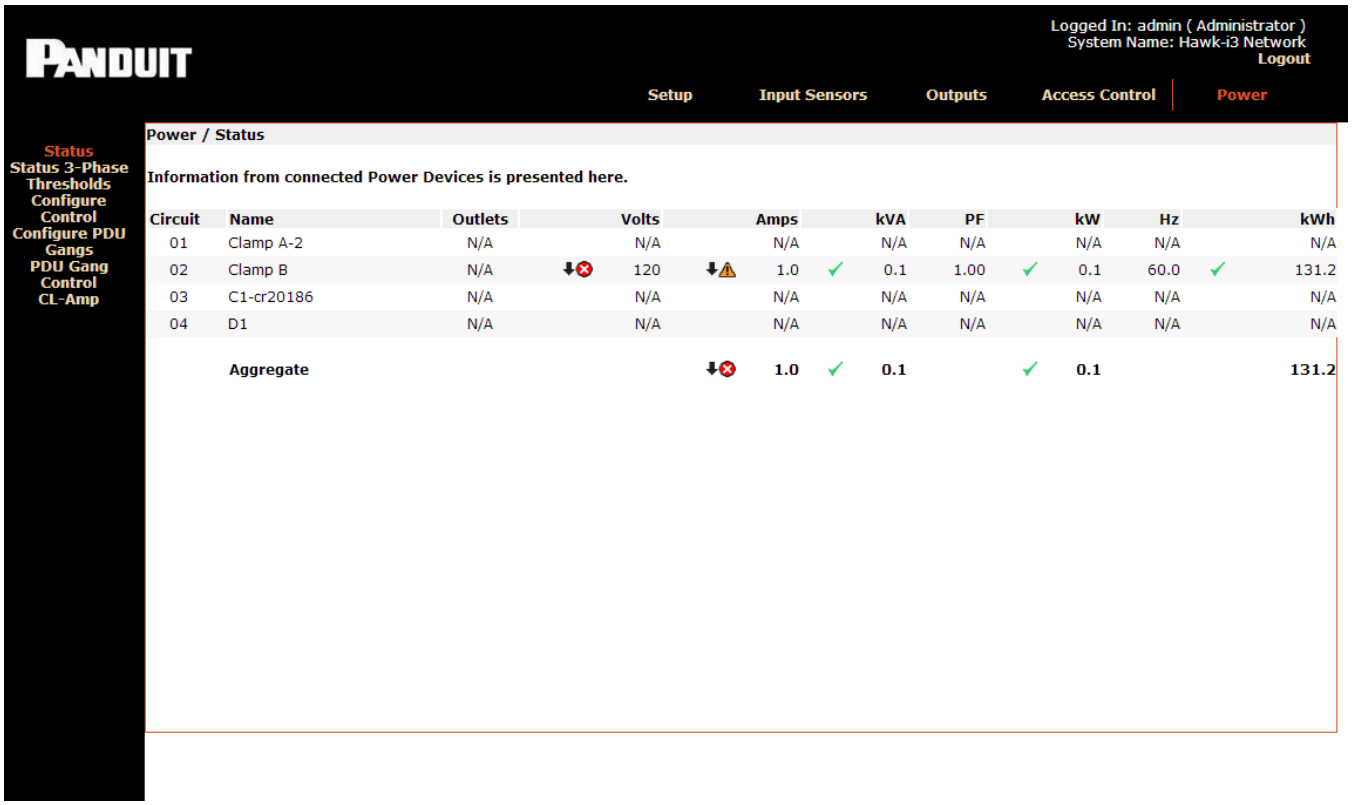
The type of connected sensor is specified here. The sensor channels can be set to auto detect, temperature, humidity, contact, or disabled.

**Note**: Occasionally, clear traps will be sent to the NMS trap receivers while a sensor is being connected to a device. This is considered normal behavior, because some voltage surges may be produced when input sensors are physically connected to the gateway. In normal operation, the sensors will always be connected to the device and the sensor voltages will stay within normal expected values

# PDUs – Configuration and Status

## PDU Status

The PDUs Status page presents an overview of connected SmartZone Rack PDUs. The page displays the PDU channel number, name, voltage, and current thresholds.




### Status Indicators

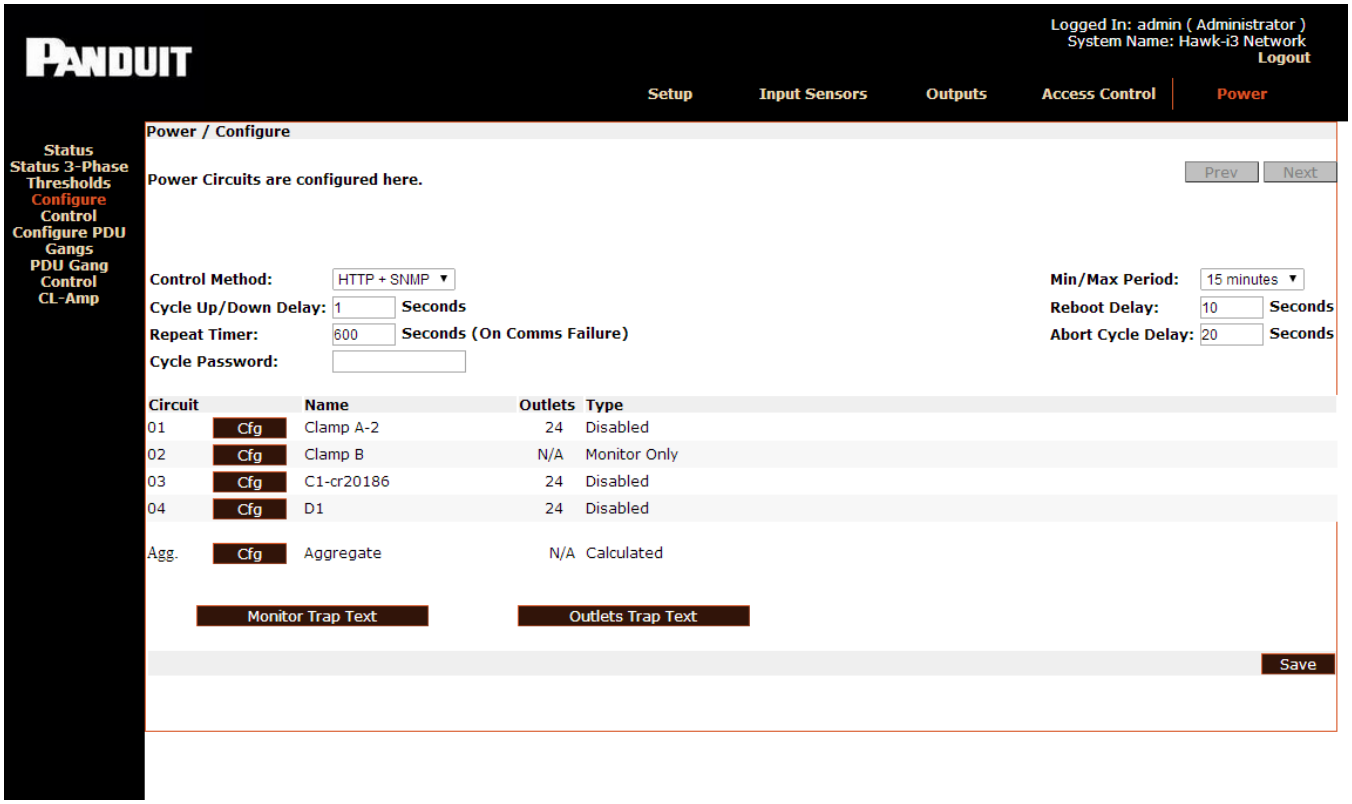
Three status indicators are displayed next to PDU channels to allow quick determination of normal, warning, and critical alarm statuses:

| | |
|---|---|
| ✓ | Channel reading currently within threshold limits. |
| ⚠ | Upper or lower Warning limit reached/exceeded. |
| ⊗ | Upper or lower Critical limit reached/exceeded. |

# Configuring PDUs

The PDU Configuration menu provides the ability to configure individual PDU options. You can configure the PDU channels individually by selecting the **Config** option next to each channel.

A summary of several current configuration parameters is displayed on a per-PDU channel basis.




## Control Method

The Control Method parameter specifies which control methods are available to control the outlets on PDUs attached to the unit.

## HTTP + SNMP

The Web Management Interface and SNMP can be used to command PDU outlets.

## HTTP Only

This option allows only the Web Management Interface to command PDU outlets. This effectively disables SNMP PDU outlet control.

## SNMP Only

This option allows only SNMP to command PDU outlets.
This effectively disables the Web Management Interface PDU outlet control.

## RS232 Only

This option allows PDU control commands to be issued directly to a unit via the onboard RS232 port. This option disables the Web Management Interface and SNMP control.

## Cycle Up/Down Delay

This parameter specifies the interval in seconds between switching on and switching off outlets when an entire PDU strip is cycled (all outlets commanded on or off).

## Repeat Timer (on Comms Failure)

This parameter specifies the interval in seconds between when an initial PDU comms failure trap is produced and a repeat trap is issued.

## Reboot Delay

This parameter specifies how long (in seconds) an outlet remains off after a reboot before switching back on.

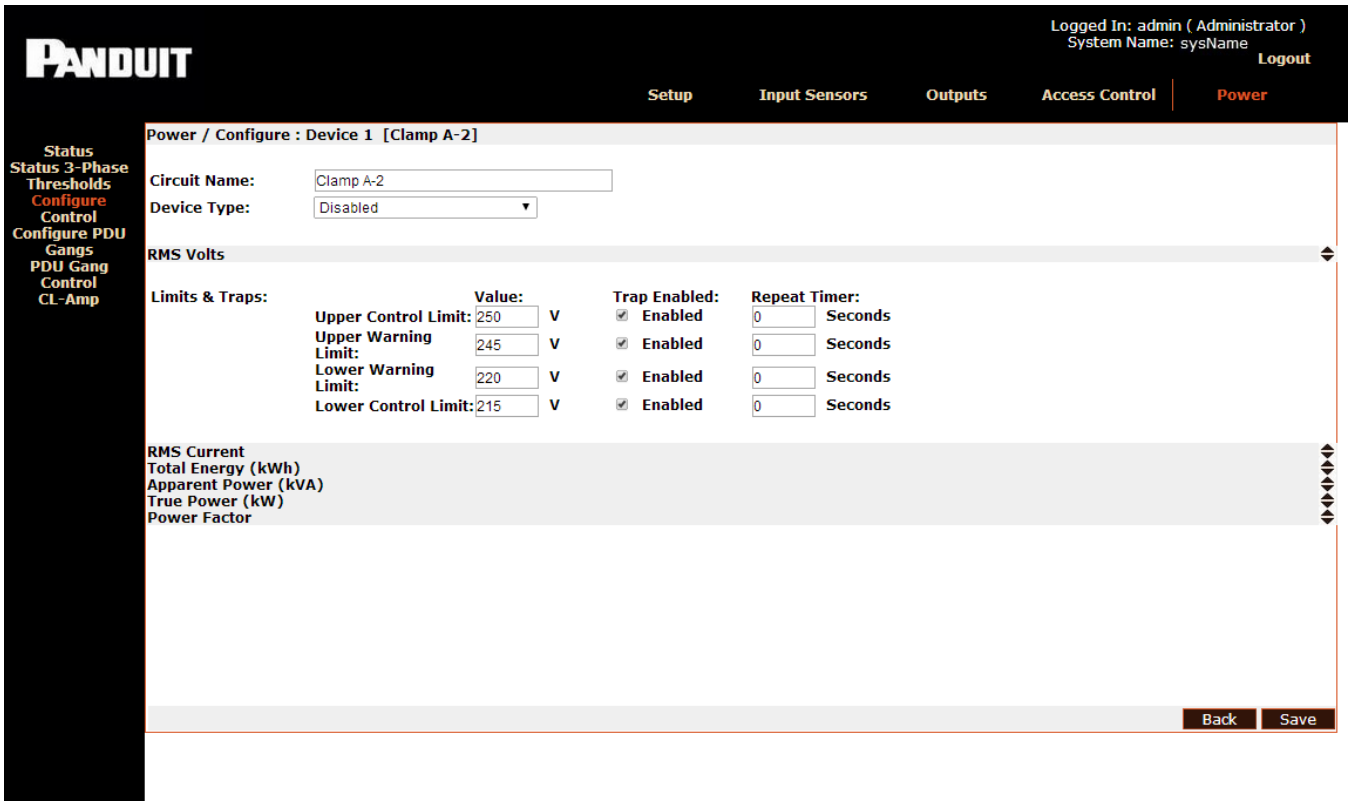
## Abort Cycle Delay

This parameter specifies how many seconds must elapse before a commanded cycle begins on a PDU. This delay gives the user time to reverse the decision to cycle a PDU before any outlet states are changed.

If you do not want to use this functionality, set the delay to zero.

## Power – Configure Menu

When you click the **Config** button next to a device in the **Power/Configuration** tab, a menu displays that allows you to specify all the available options for an individual device.



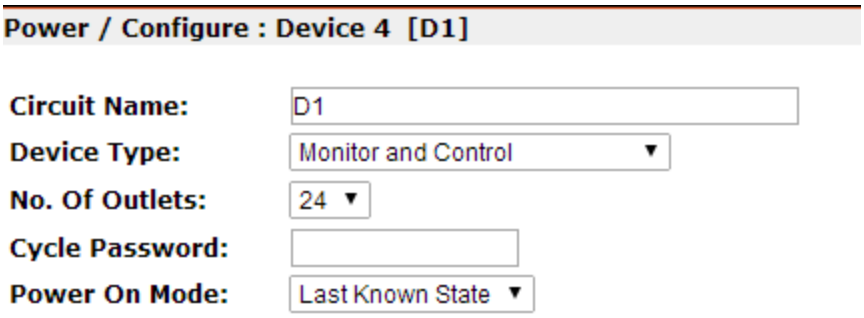

### Circuit Name

Individual PDUs can be assigned names for ease of identification (for example, “Rack 5 PDU Sensor” or “Comm Room”).

### Device Type

Specify the type of PDU connected to channel here.

- **Disabled**: No monitoring or control will be performed on this PDU channel.
- **Monitor Only**: The monitoring of power values will be performed on this PDU channel.
- **Monitor and Control**: Both outlet control and power monitoring will be enabled on this PDU channel.
- **Per Outlet Monitor**: This option enables PDU-level monitoring and monitoring of each individual PDU outlet.
- **Per Outlet Monitor and Control**: This option enables PDU-level monitoring and monitoring of each individual PDU outlet, plus outlet control.
- **Number of Outlets**: This parameter specifies the number of controllable outlets present on a PDU. This is required when the **Control Only** or **Monitor and Control** options have been selected.




For example, if you have a PDU consisting of 24 Outlets, one of which is a permanent live (non-switching) outlet, 23 outlets would be specified.

**Warning**: Failure to specify the correct number of outlets can lead to the incorrect outlet being switched on or off.

During unit setup and deployment, you should select the **Control Only** or **Monitor and Control** options before critical loads are connected to outlets.

**Cycle Password**
This field specifies the password required to set a power cycle of outlets on a controllable strip. This password is used when switching outlets using SNMP, not when switching via the web interface.

**Power on Mode**
In the event that power to the PDU is lost, this parameter specifies how the outlets will be switched back on once power is restored.

# RMS Volts

**Repeat Timer**
In the event of a communications failure with a connected PDU, this entry specifies how often (in seconds) Comm Fail traps will be generated.

**Limits and Traps**
You can specify values for voltage, current, and total power thresholds here. You also can enable or disable traps for each threshold.

The following thresholds can be set:

- Upper Control Limit
- Upper Warning Limit

- Lower Warning Limit
- Lower Control Limit

**Note**: There are no lower limits for total power, because total power consumption can only go up, not down.

### RMS Current

(See options for RMS Volts above)

### Total Power

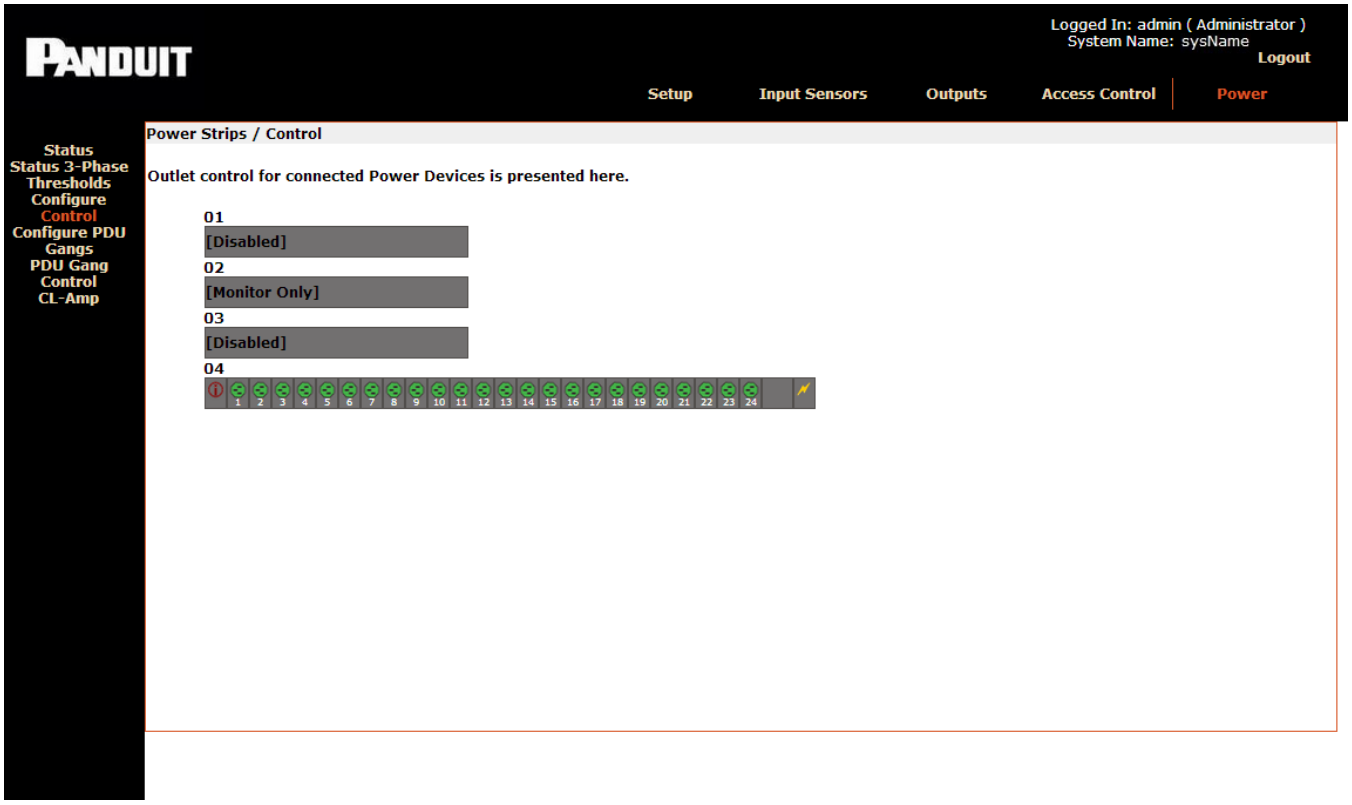
(See options for RMS Volts above)

### PDU Outlets

(See options for RMS Volts above)

## PDUs – Control

Individual outlets or all outlets on a given strip can be switched on and off using this screen.



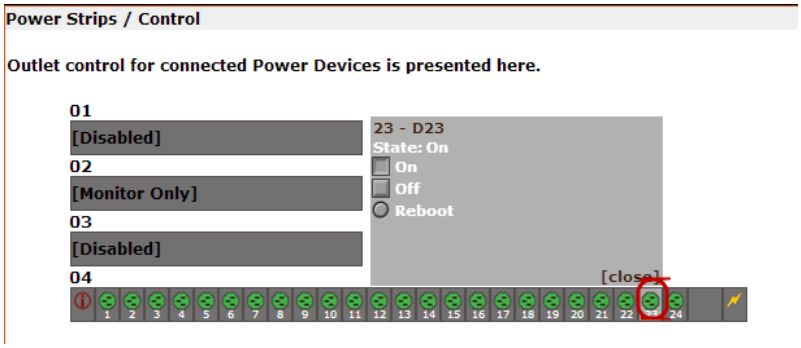
The display consists of a visual representation of PDUs that have **Control** or **Monitor and Control** enabled on the Configure page.

PDUs that are **Disabled** or in **Monitor Only** status do not display any outlet graphics and are displayed with appropriate text.

PDU inputs are numbered 1 to 2 in ascending order. PDU numbers correspond to the physical input ports on the rear of the SmartZone Gateway unit.

## Switching Individual Sockets

When you click on a socket, a control menu above the socket displays further information. Three control options are also presented:



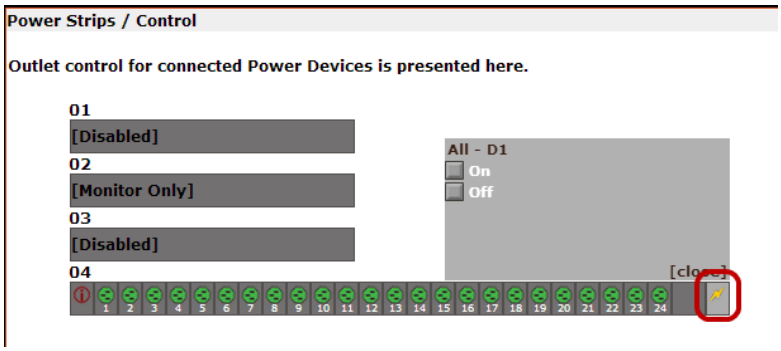

**On**
Selecting this option commands the selected outlet to switch On.
If the outlet is already on this will have no effect.

**Off**
Selecting this option commands the selected outlet to switch Off.
If the outlet is already off this will have no effect.

**Reboot**
The reboot option commands the selected outlet to switch off. After the time specified by the Reboot Delay timer has elapsed, the outlet will automatically switch itself back On.

## Switching an Entire Strip

You can switch all the outlets on any strip Off or On with a single command by clicking the **Lightning Bolt** symbol on the end of a PDU graphic.

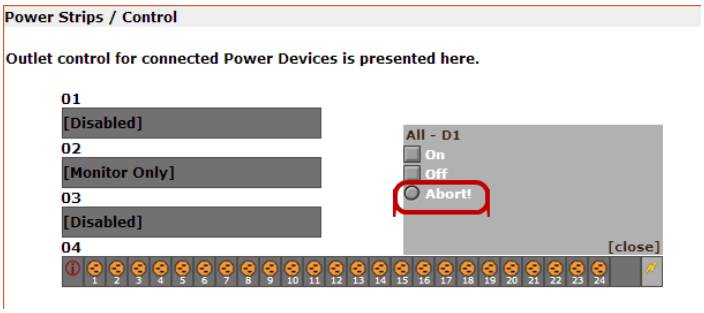



A small dialog displays, offering the following options:

**On**
This option commands all outlets on a selected PDU to switch on. Any outlets already on will remain on; any currently off will be switched on.

**Off**
This option commands all outlets on a selected PDU to switch off. Any outlets already off will remain off; any currently on will be switched off.

**Abort!**
Once a command has been issued to turn all outlets on a PDU on or off, you can click the **Abort!** button to abort the command.




The Abort Cycle delay option on the PDUs – Configure – Config menu specifies the time allowed in seconds for an abort to be issued.

# LDAP

## SmartZone Gateway LDAP Overview

The SmartZone Gateway unit implements a Lightweight Directory Access Protocol (LDAP) client. This allows the Gateway unit to authenticate user logins to the Web Management Interface using an LDAP Directory.

If LDAP is used for authentication, it is first consulted when a user attempts a login. If the user is not found or LDAP denies access, then the credentials are checked against the Gateway unit internal user list.

**Note**: Configuration of LDAP is an advanced topic and requires existing knowledge of LDAP function and setup.

## SmartZone Gateway LDAP Structure

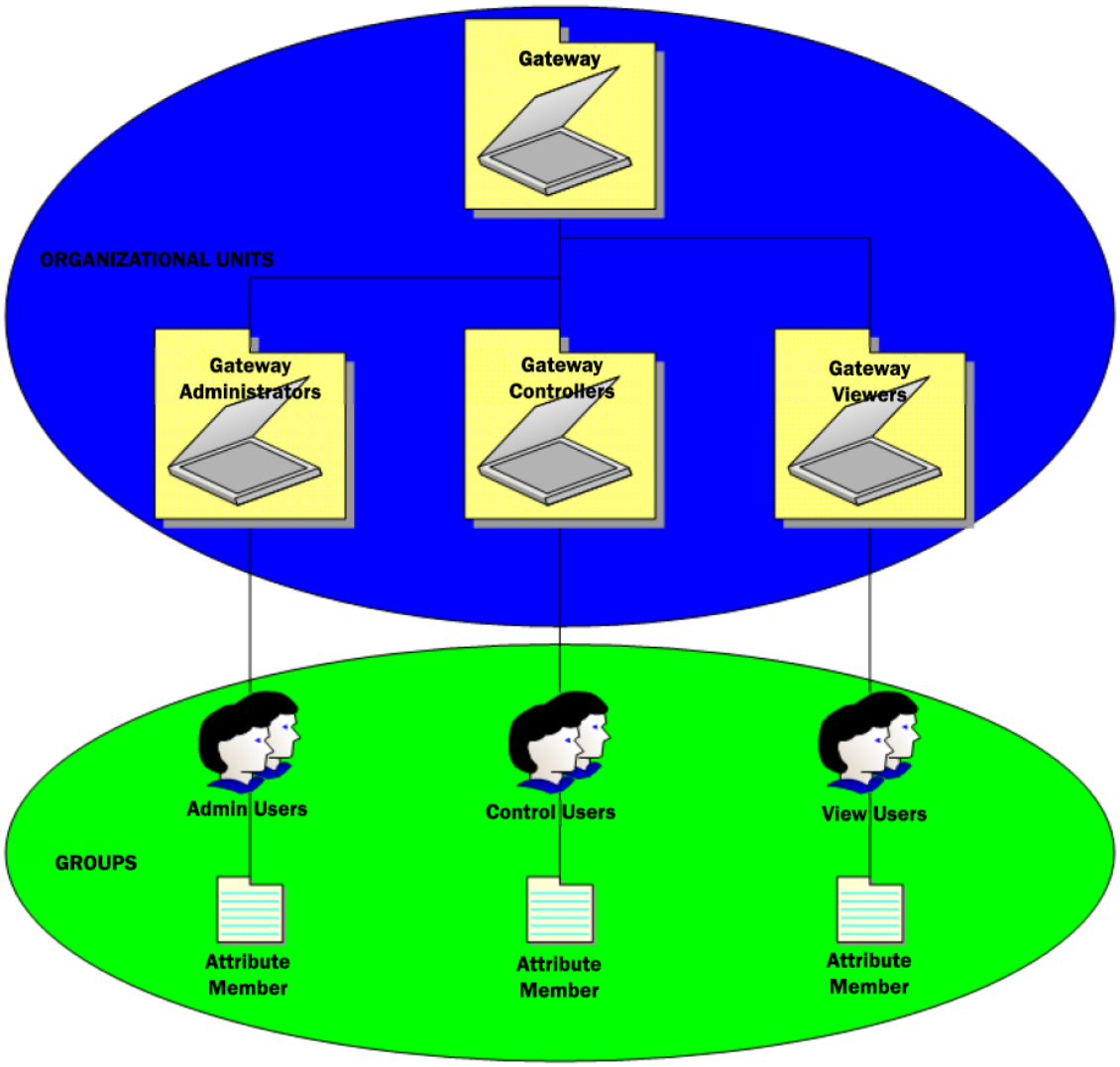
For a Gateway unit to successfully authenticate a user for Web Management Interface login, it needs to be pointed to a specific structure within a directory. You can point a unit to this structure within a directory by specifying the **Unit Base DN** on the Network Setup – LDAP page.

You will need to create the following Organizational Units:

- Gateway (this can be named anything)
- Gateway Administrators
- Gateway Controllers
- Gateway Viewers

**Note**: Groups are found in the Active Directory schema. However, any implementation which provides a group with a **Members** attribute may function.

The following figure depicts the Gateway LDAP authentication structure:




Once the required LDAP structure has been created, the Distinguished Name (DN) of users should be added to either:

- Gateway AdminUsers
- Gateway ControlUsers
- Gateway ViewUsers

## Group Membership and Access Level

Membership in these groups grants the following permissions on Gateway units:

### Gateway AdminUsers

Users placed into this group will have Admin privileges on Gateway units.

### Gateway ControlUsers

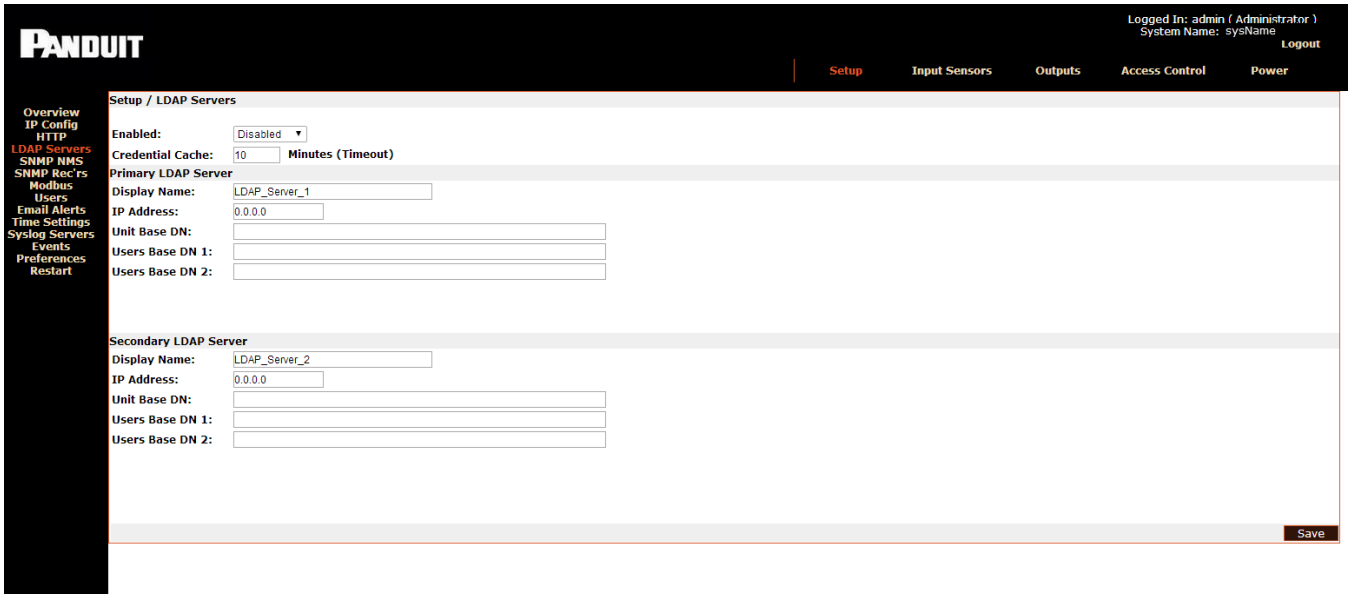
Users placed into this group will have Controller privileges on Gateway units.

### Gateway ViewUsers

Users placed into this group will have View privileges on Gateway units.

## SmartZone Gateway Unit Configuration

For LDAP authentication to function, you need to provide certain configuration values for each Gateway unit.




To enter the configuration values, perform the following steps.

1. If one LDAP server is to be used, select **Enabled – Primary**.
2. Enter a descriptive name (for example, AD_Server_1) into the **Display Name** field.
3. Enter the complete DN of the top level OU.
4. Enter the DN of where users that are members of Gateway access groups can be found in the Directory. These DNs can be entered into **User Base DN 1** and **User Base DN 2.**
5. Click **Save**.

# Temperature Sensor Adapter Installation

Follow the instructions below to install the ZAHTLADT-02 v1.01.01 temperature sensor adapter module. This adapter allows legacy sensors to provide more accurate temperature readings.

**Note**: This adapter does not work with the ZETHL-14 temperature sensor.

## New Installations

Follow these instructions when you are installing a standard temperature sensor, but the upgraded sensor input is required.

1. Plug the adapter directly into the back of the gateway, at the sensor port to be used for temperature.
2. Plug the temperature sensor connector into the adapter.


3. Update the gateway firmware to the latest release.

# Existing Installations.

Follow these instructions when the sensor is already installed along with the gateway.

1. Unplug the current temperature sensor from the gateway, noting the location where it resided.
2. Insert the adapter into that location.
3. Plug the sensor into the end of the adapter.
4. Perform these steps for all other temperature sensors to be changed.
5. The gateway firmware must be updated to the latest firmware.

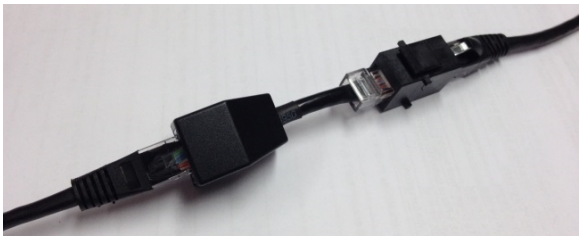
Before the adapter is fitted:

After the adapter is fitted:

# Fitting the Adapter In-line.

This procedure is not recommended, but it may be the only solution in some cases.

1. Using a patch lead from the gateway and an RJ45 Jack to Jack through connector on its non-gateway end, plug the adapter RJ45 Plug into the through connector.
2. Plug either the RJ45 plug of a temperature sensor into the jack on the adapter or a patch lead with the temperature sensor on the end.



# Troubleshooting

## Resetting the SmartZone Gateway to Factory Default Settings

To reset the Gateway unit to factory defaults, perform the following steps:

1. Press and release the **Reset** button on the front of the unit. The Alarm LED will flash twice (off/on, off/on).
2. Immediately press and hold the **Mode** button until the alarm LED goes off.
3. Immediately press and release the **Reset** button.

**NOTE**: The unit will now restart. The Status LED will start flashing after around 1 minute. The reset process is complete, and the IP address is set to the default 192.168.0.253.

## Problem: The NMS Cannot Poll the SmartZone Gateway Unit

- **Solution**:Make sure the network is properly connected to the Gateway unit.
- **Solution**:Make sure the cable is in good condition.
- **Solution**:Try pinging the Gateway unit from another computer on the same network segment as the Gateway unit.
- **Solution**:Ensure that the NMS IP Address is in the NMS table of the Gateway unit.
- **Solution**:Ensure that the community string has been set for the NMS via the Web Management Interface.

# Technical Support

For technical support for the SmartZone EPA064 system, please contact Panduit Technical Support using one of the following methods:

- 1-866-721-5302 (toll-free)

- Orland Park, USA:  6:30am – 8:00pm CST
- Mumbai, India: 6:30am – 5:00pm IST (8:00pm – 6:30am CST)
- On Call Support on Weekends

- systemsupport@panduit.com

# Appendix A: Technical Details

## Factory Default Settings

| | |
|---|---|
| IP Address | 192.168.0.253 |
| Subnet Mask | 255.255.255.0 (/24) |
| Default Gateway | 192.168.0.1 |
| Web Management Address | http://192.168.0.253/ |
| Default username | admin |
| Default password | admin |

## Operating Information

| | |
|---|---|
| Input Power | 100 to 240VAC 50Hz / 60 Hz<br>0.5 Amp Maximum |
| Input Power | 36 to 60 VDC 0.5 Amp Maximum |
| Operating Temperature | 0 $^{O}$C to 40 $^{O}$C |
| Storage Temperature | -10 $^{O}$C to 70 $^{O}$C |
| Operating Humidity | 5% to 90% Relative Humidity |
| Storage Humidity | 5% to 100% Relative Humidity |

**CAUTION**: There is a risk of explosion if the battery is replaced by an incorrect type. Dispose of used batteries according to the instructions.

# Unit DimensionsAC)

| | |
|---|---|
| Height | 37mm [1.5” ] |
| Width | 233mm [9.2” ] |
| Depth: (including earth stud and connectors) | 85.2mm [3.4” ] |
| DepthL (Case only) | 79mm [3.1” ] |
| Width including Mounting brack-ets | 285mm [11.2” ] |
| Unit net weight | 760gm [26.8 oz] |

# Unit Dimensions (-48VDC)

| | |
|---|---|
| Height | 37mm [1.5” ] |
| Width | 242.6mm [9.6” ] |
| Depth: (including earth stud and connectors) | 104.4mm [4.1” ] |
| DepthL (Case only) | 80.4mm [3.2” ] |
| Width including Mounting brack-ets | 295mm [11.6” ] |
| Unit net weight | 828gm [29.2 oz] |

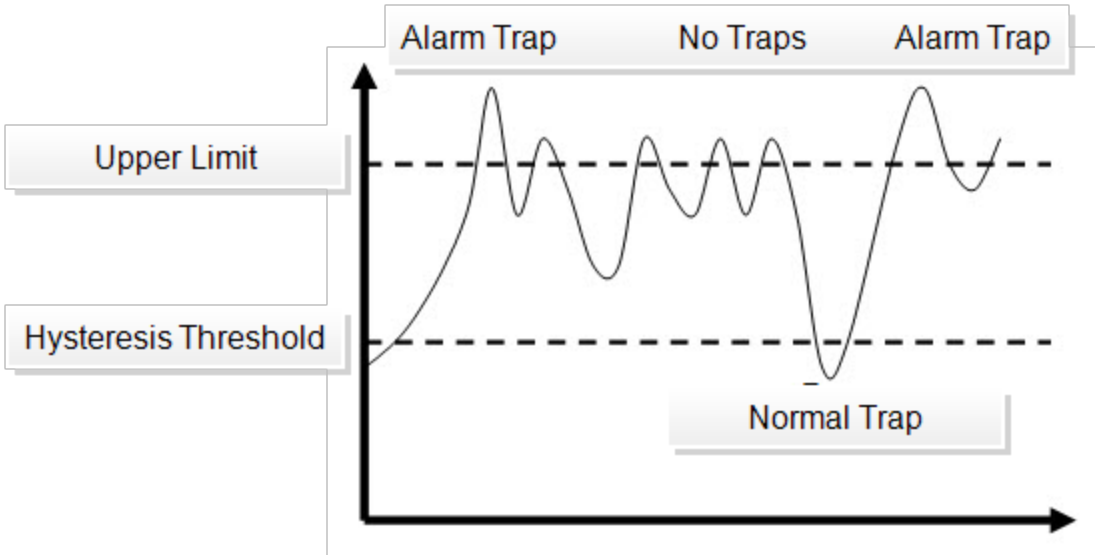
# Appendix B: Hysteresis Demystified

When a temperature or humidity limit is reached and the relevant limit has its OFF to ON Trap enabled, an alarm trap is issued by the SmartZone Gateway unit.

With a zero hysteresis setting, the traps will continue to be generated each time the limit is reached.

This may be undesirable in a situation where the temperature or humidity level measure has reduced by only a small amount before rising again and triggering further traps.

The hysteresis function is provided to prevent further alarm traps from being generated until the measured value has fallen to a satisfactory level.




As shown in image above, the humidity first rises past its upper warning threshold, which generates an alarm trap.
The humidity then reduces slightly but does not reduce to the hysteresis level, which is 1.5% relative humidity lower than the alarm setting (1.5% relative humidity lower as an absolute measured value, rather than 1.5% of currently measured value).

Humidity then increases and decreases again. However, on the second decrease of humidity the level drops below the hysteresis level. The Humidity falling below the hysteresis level re-enables alarm traps for the next alarm event. An upper limit of 25 and a hysteresis threshold of 1.5 yield a threshold limit of 23.5.

The humidity level again begins to rise and again exceeds the upper limit, however this time an alarm trap is generated again.

The Hysteresis feature acts on the following Temperature and Humidity thresholds:

- Upper Control Limit (UCL)
- Lower Control Limit (LCL)
- Upper Warning Limit (UWL)
- Lower Warning Limit (LWL)

The inverse of the above description is true when applied to Temperature and Humidity lower control and warning limits.

You can configure the hysteresis threshold by using the menu options.

# Appendix C: Encryption and Security

The Gateways support HTTPS encryption, and they support the following cipher configurations.

- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_DES_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA