SmartZone™ Gateway E24
User Manual

Release 1.0
Issue 2

Table of Contents

Introduction

Overview

The SmartZone™ Gateway E24 is a compact device used to monitor up to twenty four input sensors (Temperature, Humidity, Digital or Analog voltage).
The unit comprises both an SNMP interface and a secure web-based interface for monitoring and management.
Some of the main features of the E24 unit are:

- Secure web management and configuration interface.
- SNMP enabled.
- Twenty Four sensor channels.
- Optional LCD Status module.

Safety and Installation Statement

Grounding

This is a Class II product that uses double insulation to provide electrical safety of the product from the main power source.

To ensure correct operation, compliance with Class A and Class B electromagnetic emission standards, and optimal safety, connect the 4mm grounding stud (labeled “Earth” on rear face of unit) to an electrical ground.

If the network covers an area served by more than one PDU, 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.

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 organisation 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, Authorisation & Restriction of Chemicals. (REACH)

The equipment:**E24**
Model Numbers:**ZAEH2-01**
Is in conformity with the applicable requirements of the following documents:

Reference No.	Title
BS EN 55022:1998	Information technology equipment. Radio disturbance characteristics. Limits and methods of measurement. Class A.
BS EN 55024:1998+A2:2003	Information technology equipment. Immunity characteristics. Limits and methods of measurement.
BS EN 60950-1:2006	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.

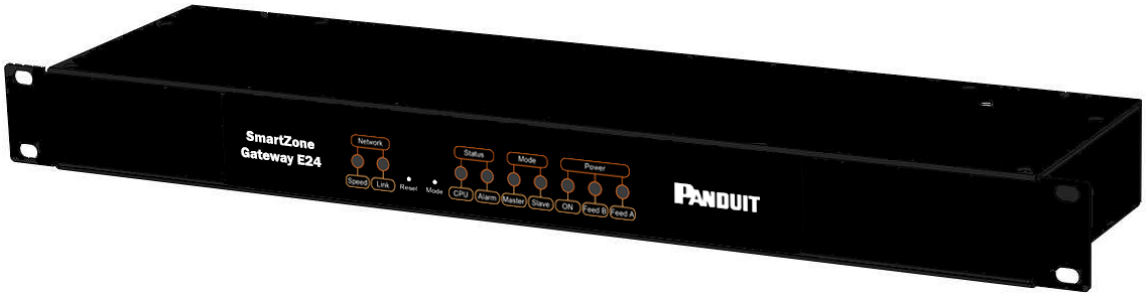
E24 Package

The standard E24 package contains a E24 unit with supporting hardware:

- E24 I Unit
- Mains voltage cable
- Rack mounting kit
- Supporting CD-ROM including MIB file and manuals

LEDs

Nine LEDs can be found on the front of the E24. Their purpose is described below the illustration of the unit below:



Network

- **Speed:** Illuminates when 100Mb/s network connected
- **Link:** Iluminates when a network connection is present

Status

- **CPU** : Flashes when the unit is running normally
- **Alarm**: Illuminates when an alarm is present on the unit

Mode

- Reserved for future use

Power

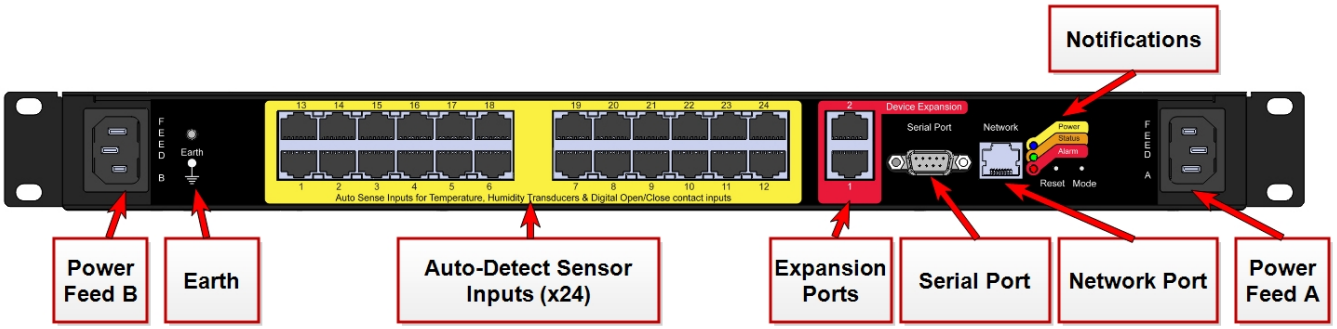
- **ON**: Illuminates when unit is powered.
- **Feed A**: Illuminates when Power is connected to Feed A
- **Feed B**: Illuminates when Power is connected to Feed B

Buttons

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

Rear of E24

The following image show the rear panel of the E24 unit:



Port Information

- **Power Feed B**:Redundant mains or -48v DC voltage power feed.
- **Earth**: Grounding stud.
- **Auto-Detect Sensor Ports 1 through 24:**Connect up to 24 sensors (such as Temperature, Humidity, Water, Door Contacts, and More).
- **Expansion Ports**:Daisy Chain E24 Gateway to Other E24 Gateways for Additional Sensor Ports.
- **Serial Port**: Attach optional devices (such as LCD Status Monitor Unit).
- **Network Port**: An RJ-45 port to connect the Gateway to LAN/Network.
- **Notifications**: Reset/Mode/Power/Status/Alarm notifications duplicated from the Front Panel.
- **Power Feed A**: Mains or -48v DC voltage power feed.

Installation Requirements

- E24 unit.
- Mains power cables (supplied)
- 10/100 base T network connection.
- Network connected computer system to setup the E24 .
- 1 x network crossover cable
- Screwdrivers

Rack – Mounting

This section covers the basic rack-mounting of the E24.

Additional Equipment Required

You need to supply a number-2 Phillips screwdriver to rack-mount the E24.

Before You Begin

When determining where to install the E24, please verify that these guidelines are met:

- Airflow around the E24 is unrestricted.
- Clearance to the front and rear panels meet these conditions:
  - Front-panel LEDs can be easily read.
  - Access to ports is sufficient for unrestricted cabling.
  - AC power cords can reach the E24.
  - The 10/100 network cabling does not exceed 100 meters from the E24 to the Network switch.
  - Temperature around the E24 does not exceed 40 deg.C
  - Humidity around the E24 does not exceed 90 percent.

Installation Warning Statements

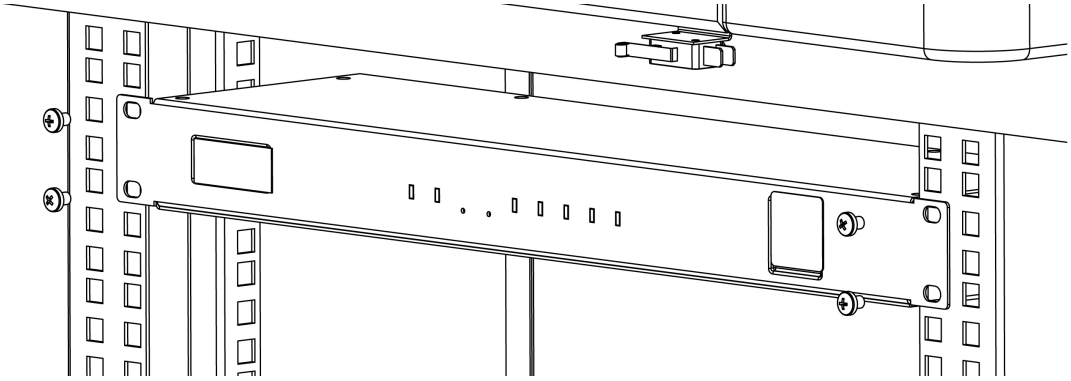
This section includes the basic warning statements.

- Only trained and qualified personnel should be allowed to install, replace, or service this equipment.

- To prevent the E24 from overheating, do not operate in an area that exceeds the maximum recommended ambient temperature of 40° C.
- Installation of the E24 must comply with local and national electrical codes.
- To prevent personal injury when mounting or servicing the E24, you must take care to ensure the system remains stable.
- The rack or cabinet should be adequately secured to prevent it from becoming unstable and/or falling over.
- Circuit Overloading - Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of circuits might have on over current protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.
- Reliable earthing of rack mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (use of a PDU, etc.)

Rack-Mount the E24

Hold the E24 and attach the bracket to rack using two 12-24 screws.



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

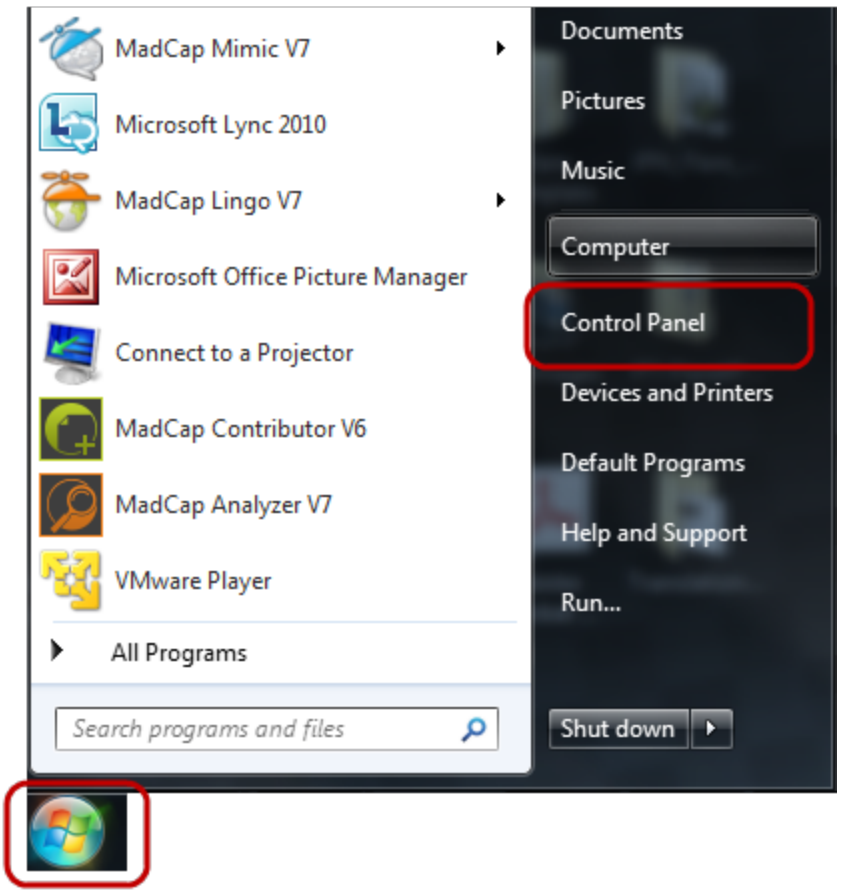
The SmartZone Gateway monitoring solution can be configured entirely using the built-in Web Management Interface.

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.

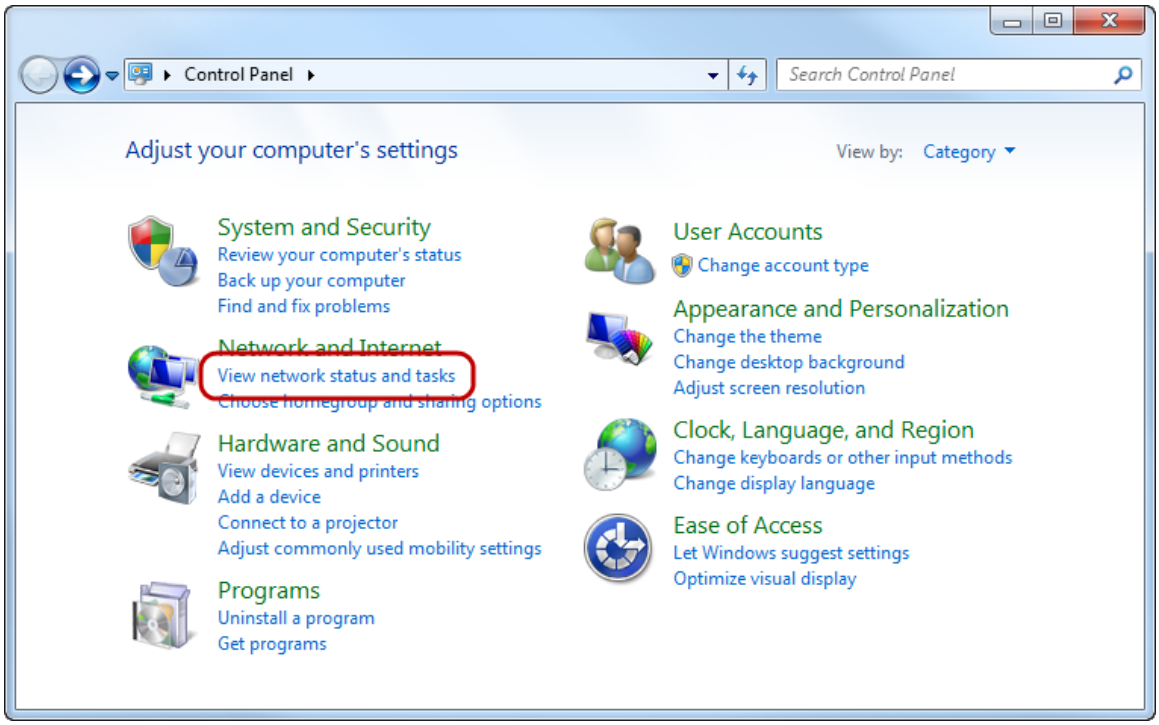
Changing your PC's IP Address

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

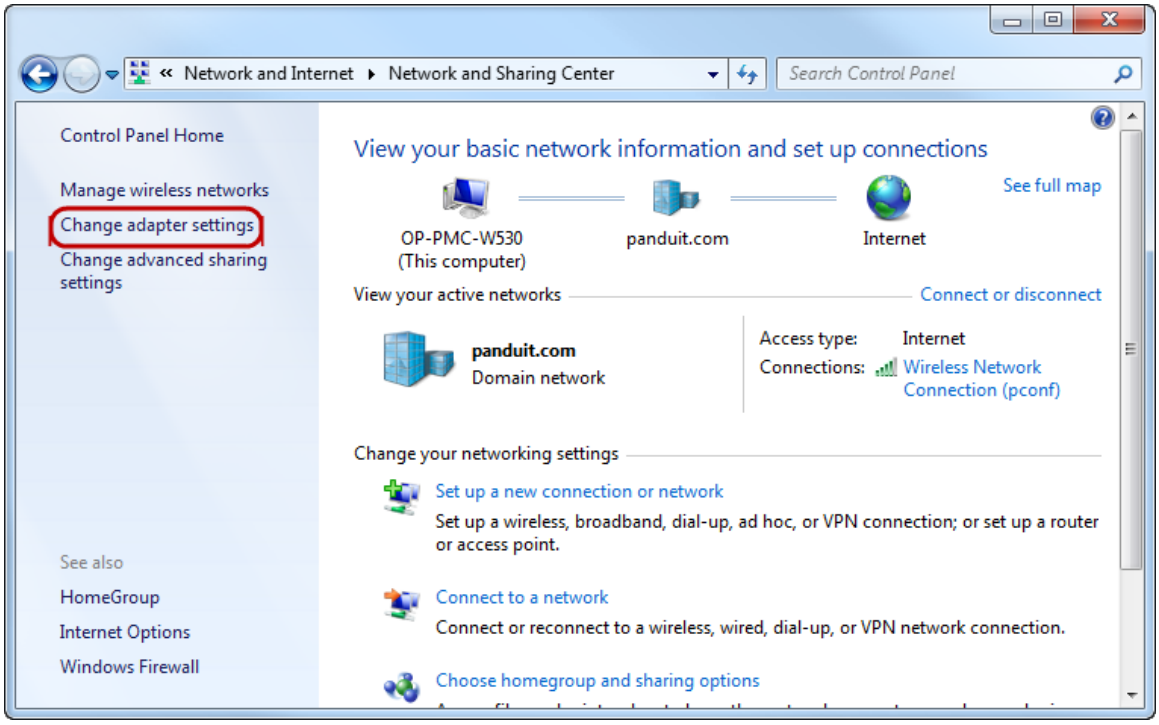
1. Click the Windows button and select **Control Panel**.



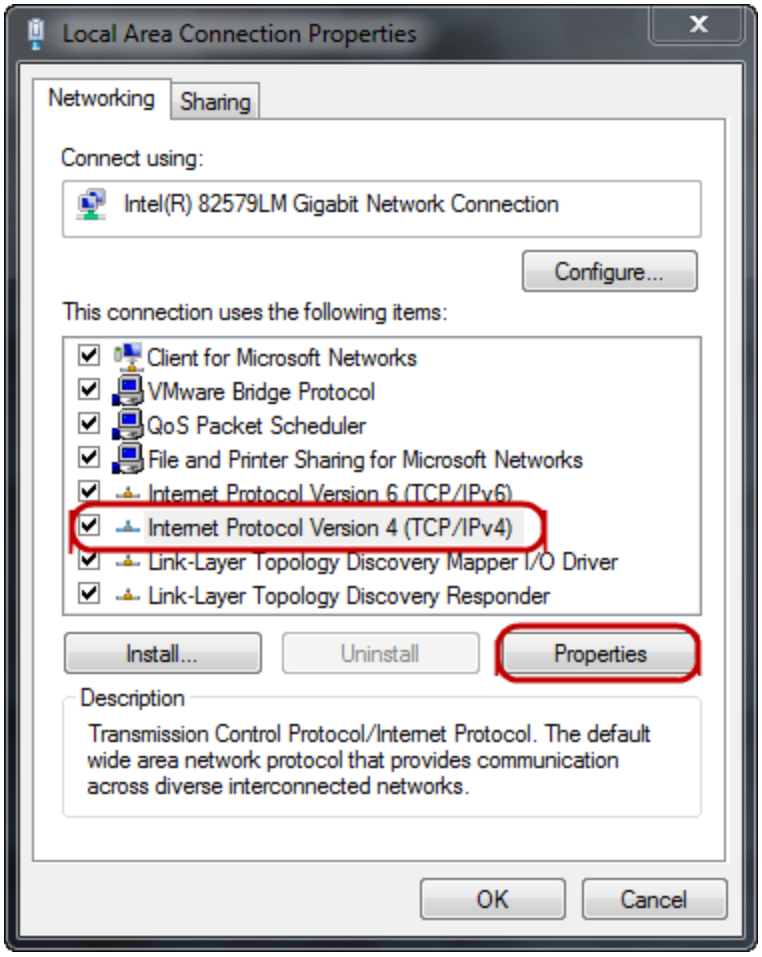
2. In the Control Panel window, select **View network status and tasks** under the Network and Internet heading.



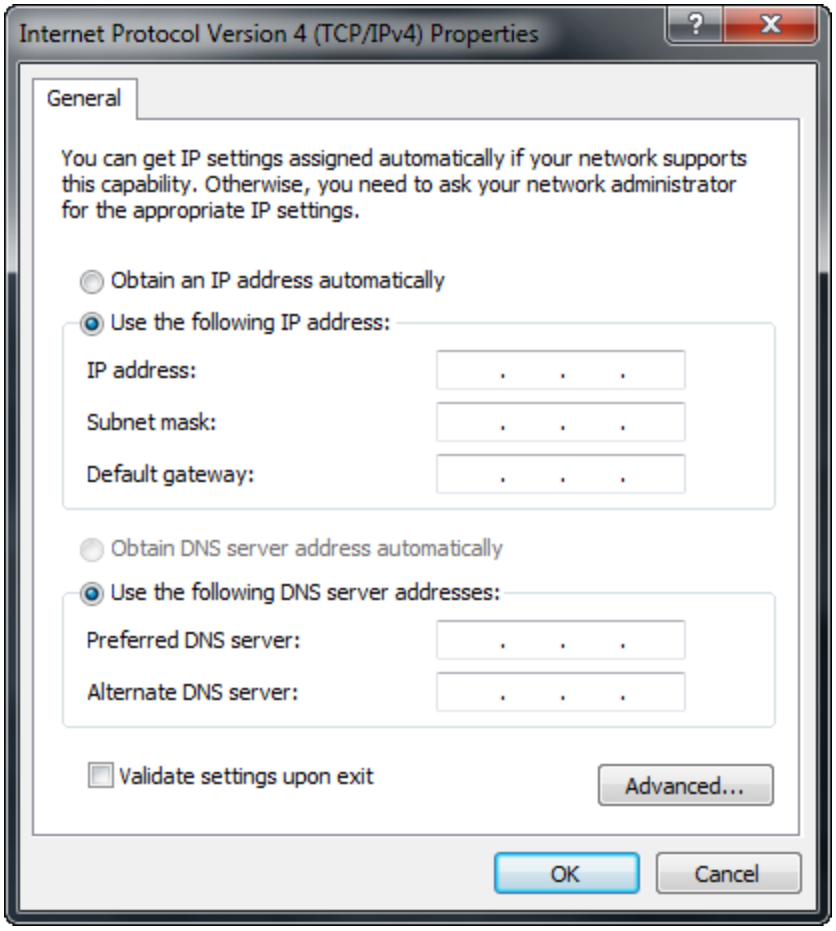
3. Select **Change adapter settings** from the menu on the left.



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



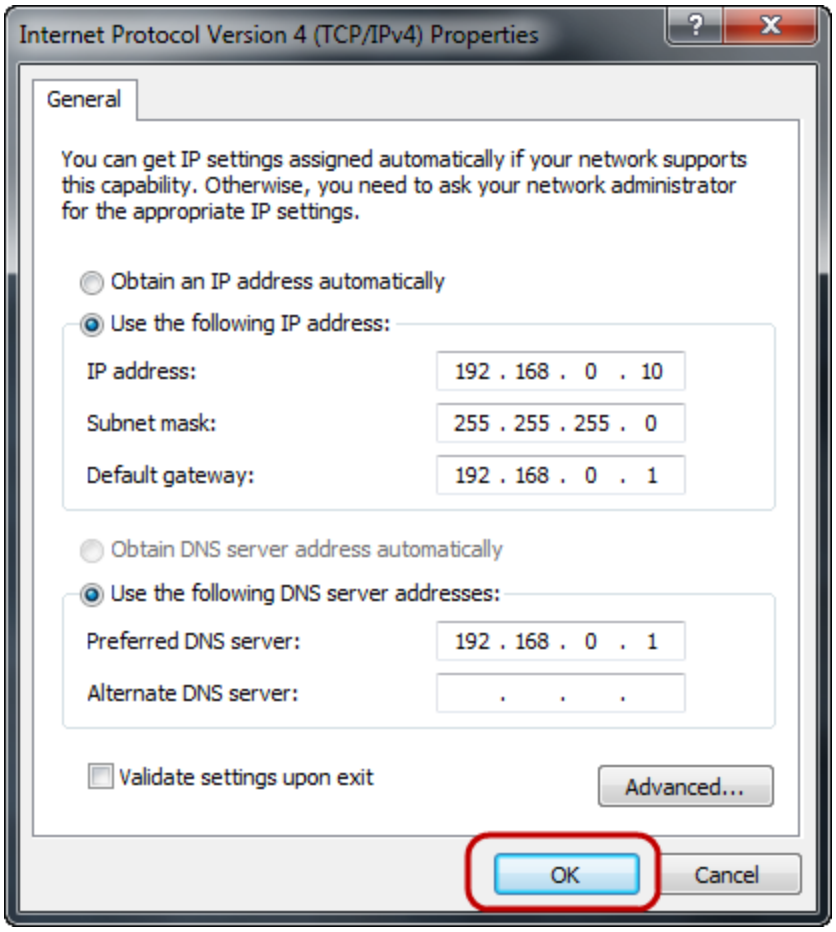
6. Select the **Use the following IP address** radio button.The **Use the following DNS server addresses** radio button then selects automatically.



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.

Initial Network Setup

This section provides details on preparing the unit for network access and allowing SNMP network management.

Connection to the Web Management Interface is required.

Entering NMS Details

1. Click the **Network Setup** tab on the top menu bar then select the **SNMP NMS** link on the left menu bar.
2. Enter the IP address, chosen community string, and required NMS access permissions of the Network Management Stations to be used.
3. Click **Save** to confirm the changes.

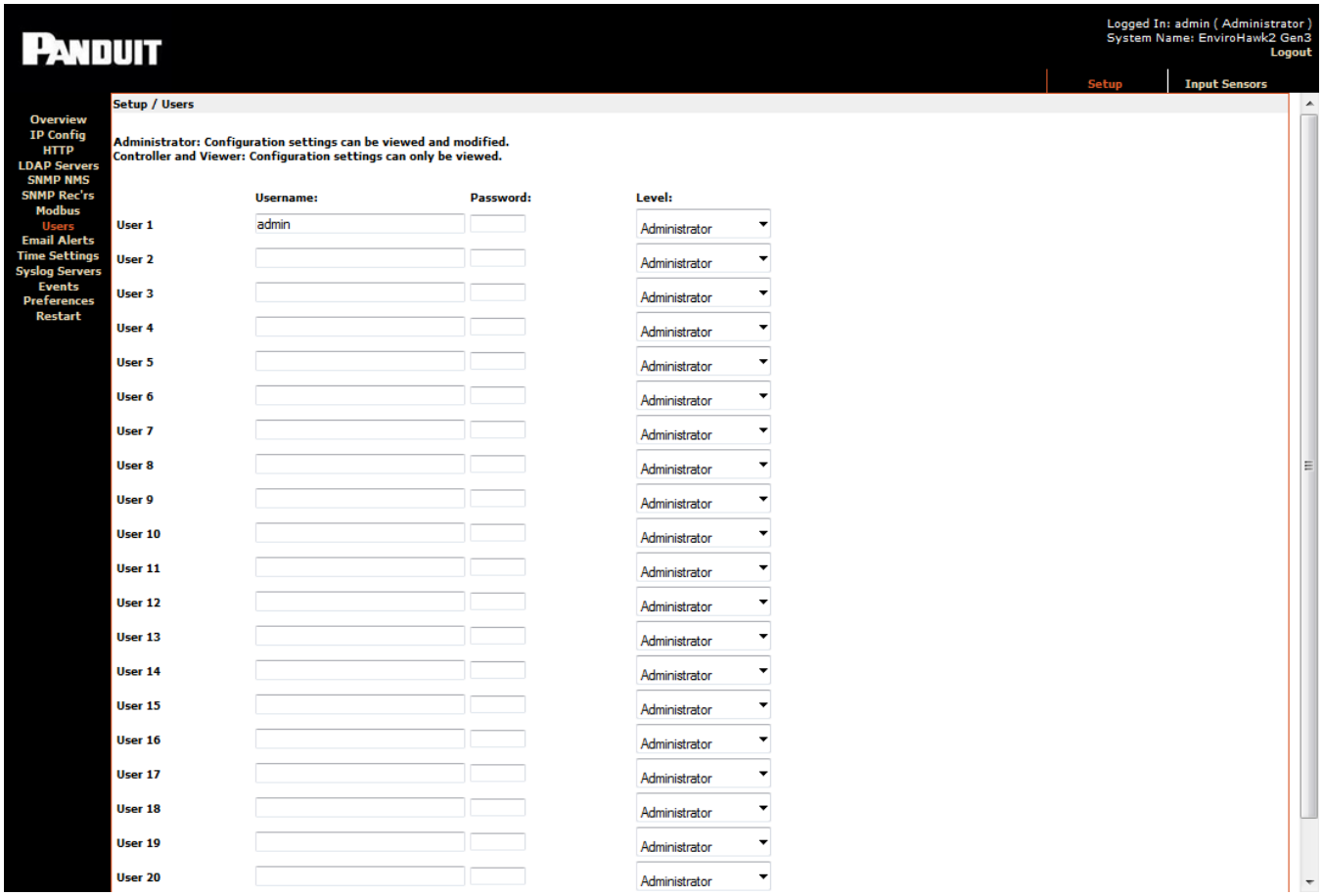
4. To disable an NMS, select the **Disabled** option from the **NMS Access** drop-down list.

Entering Trap Receiver Details

1. Click the **Network Setup** tab on the top menu bar.
2. Select the **SNMP Rec'rs** link on the left menu bar.
3. Enter the IP address, chosen community string, and required trap types for the Network Management Stations to be used.
4. 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.

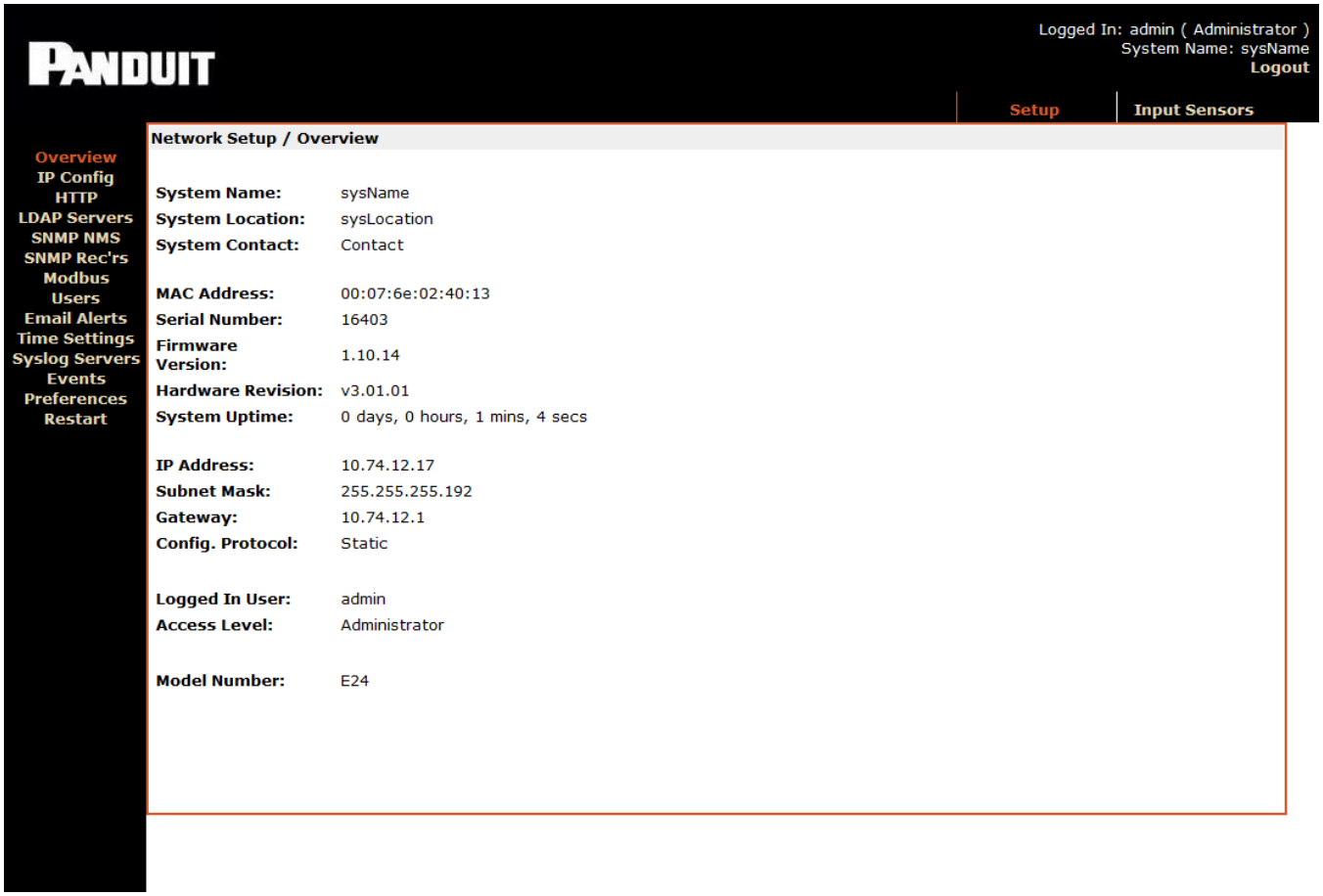
Web Management Interface

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

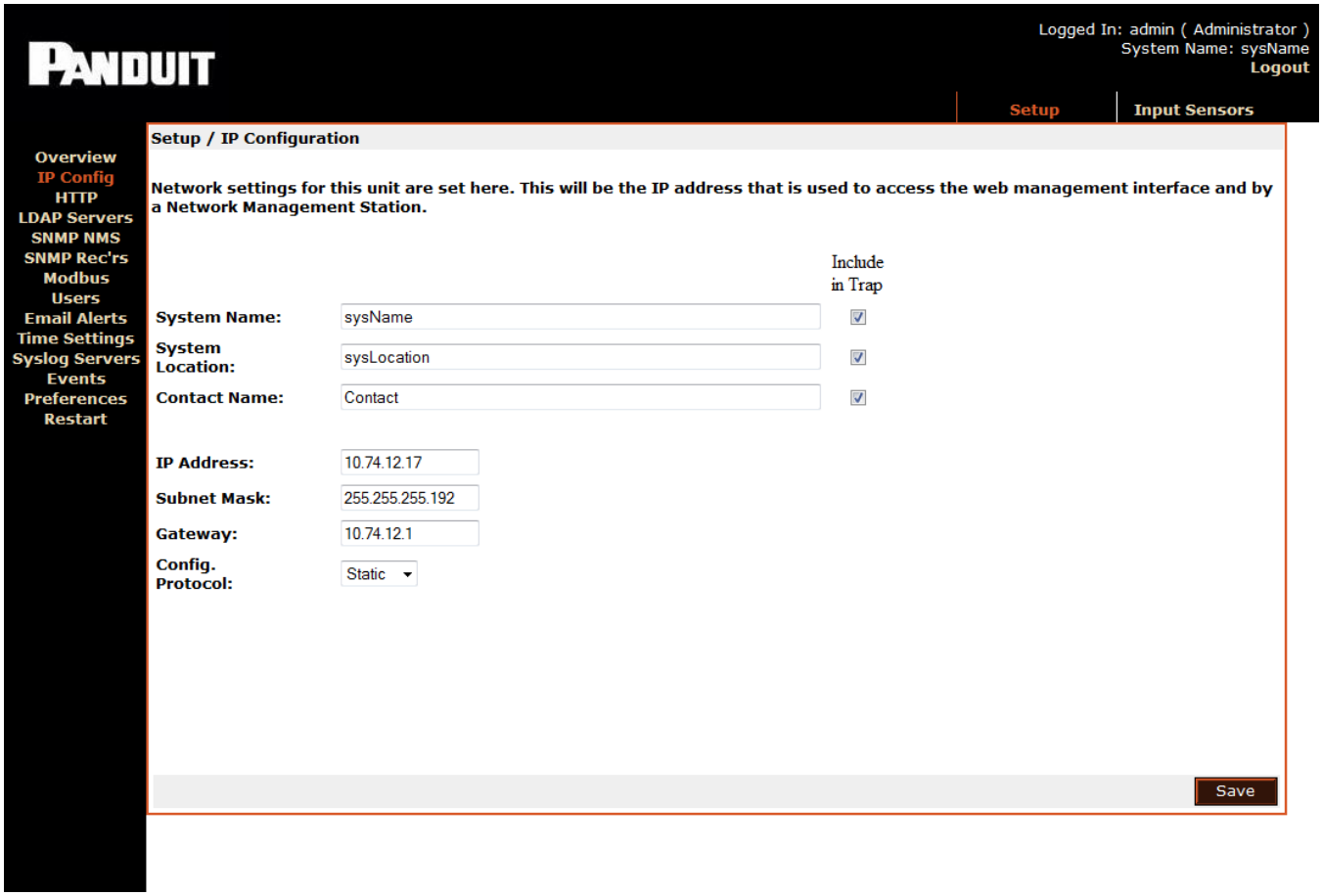
The Overview page is the first page displayed and provides the user with an overview of the Gateway unit's current status.



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.

The system name 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 specified.

The system location 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. The contact name 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 dotted decimal format (for example: 192.168.0.1 or 11.2.24.103).

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

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

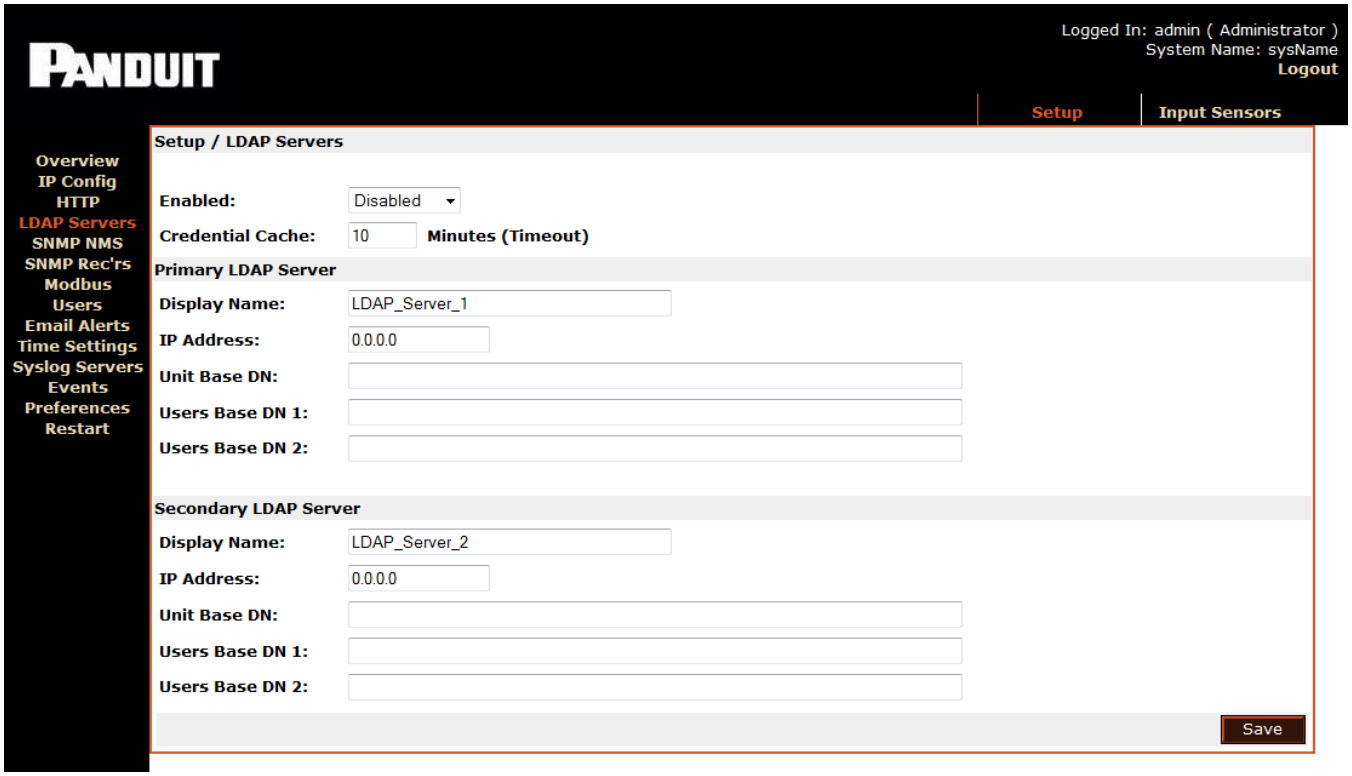
Select the access method for the Web Management Interface here. Both HTTP and HTTPS access modes are available by default. Selecting the HTTPS radio button will allow only HTTPS configuration.
Use of HTTPS is recommended for security, because the connections will be encrypted.

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: Selecting 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.

Disabled

No LDAP servers will be queried to verify user login credentials access and privileges. Only internal users will be able to log in.

Primary

Only the Primary LDAP Server specified will be queried to verify user login credentials' access and privileges.

Secondary

Only the Secondary LDAP Server specified will be queried to verify user login credentials' access and privileges.

Both

Both LDAP Servers specified will be queried (with priority given to the Primary) to verify user login credentials' access and privileges.

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.

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.

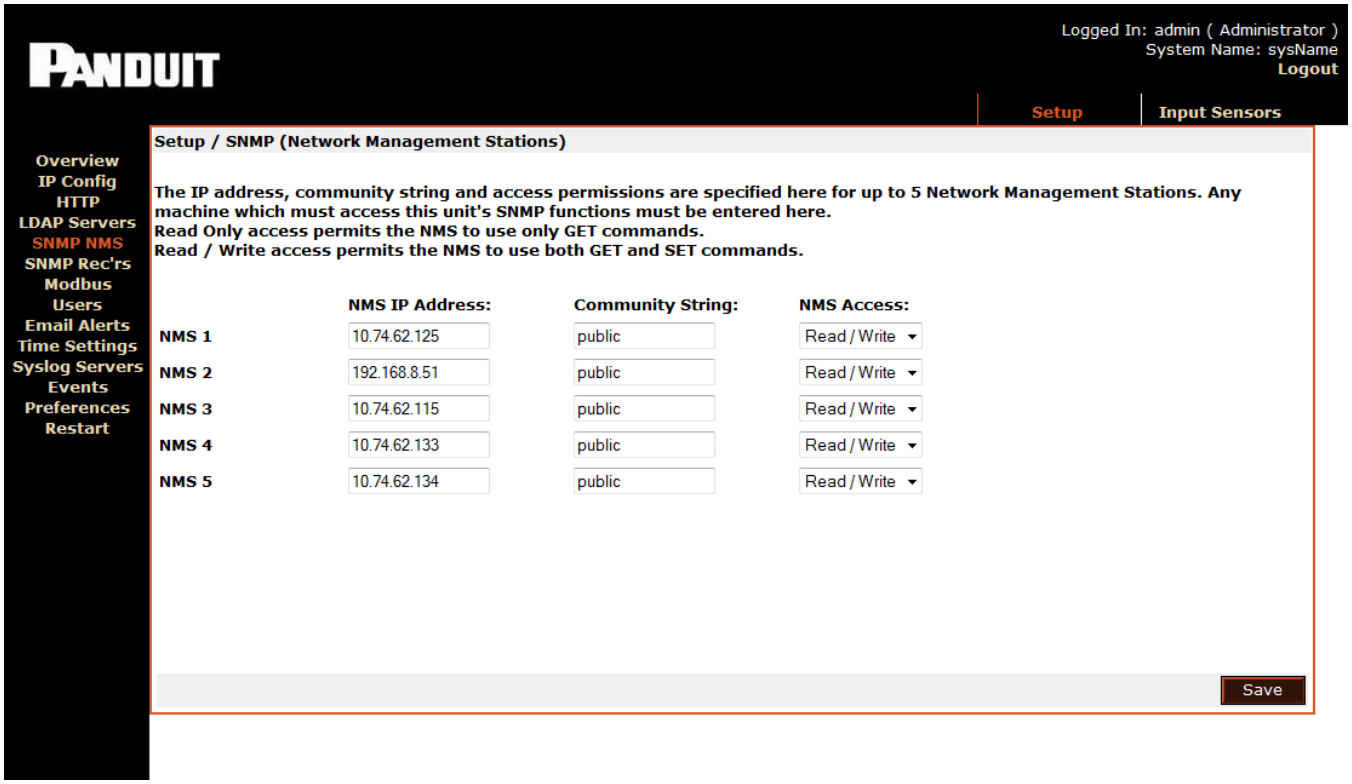
Users Base DN 2

You can specify the Distinguished Name (DN) of the directory object containing directory users for authentication here. This field is optional for LDAP function providing 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.



IP Address

Enter the IP address of the NMS machine here.

Community String

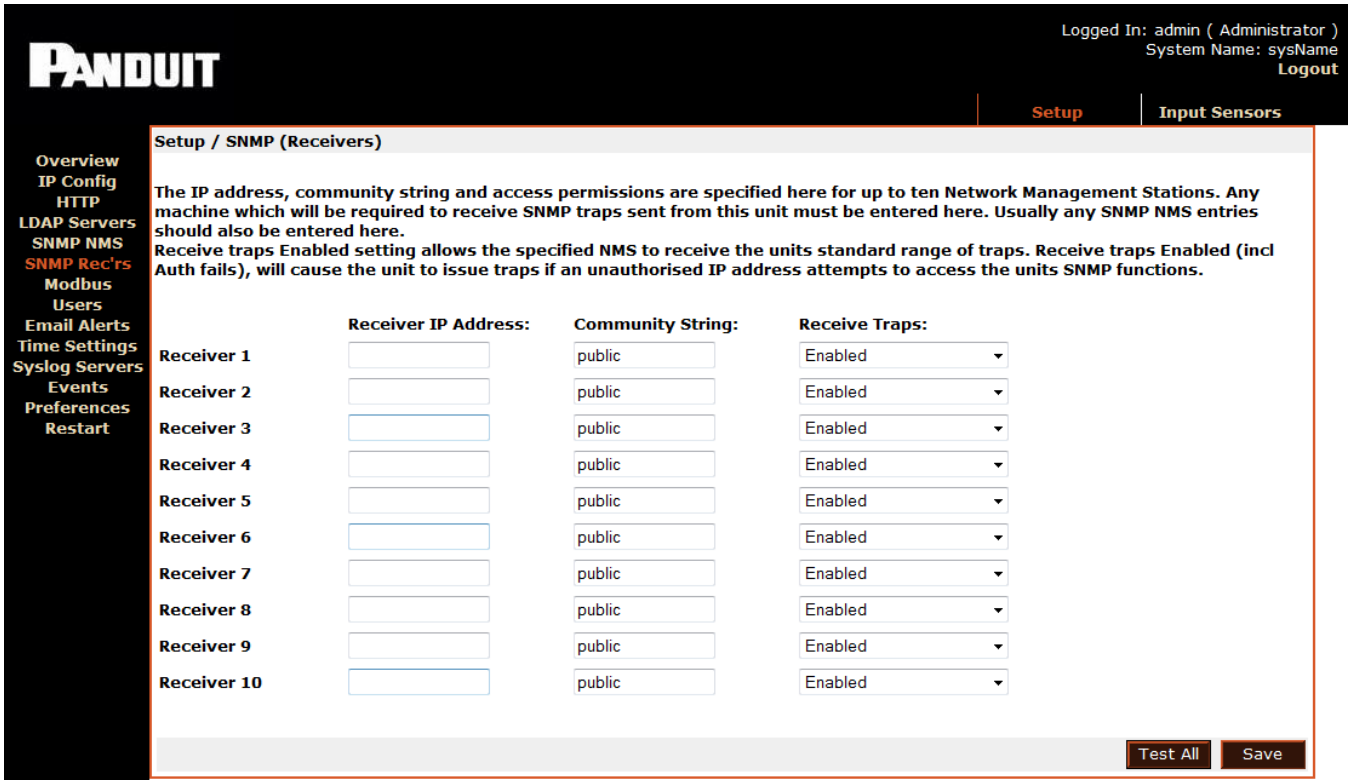
You must enter the required community string here. The default for many devices is **public**. It is recommended that the community string be changed, because it serves as an access password.

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 Trap Receivers

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



IP Address

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

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.

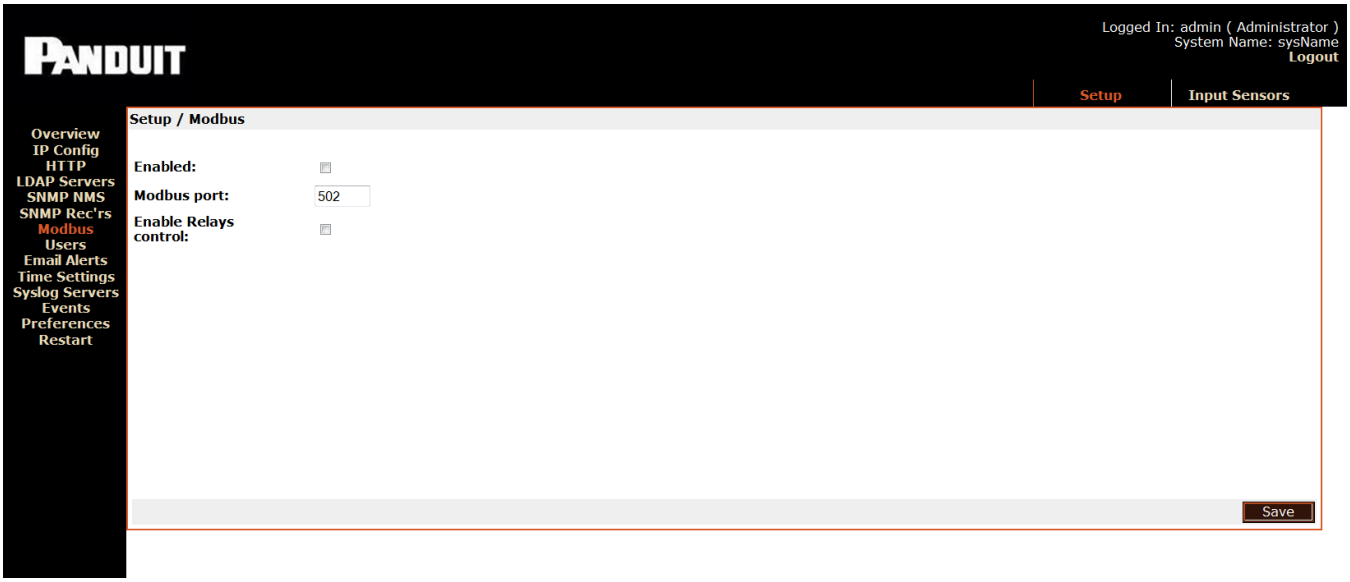
Receive Traps

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.

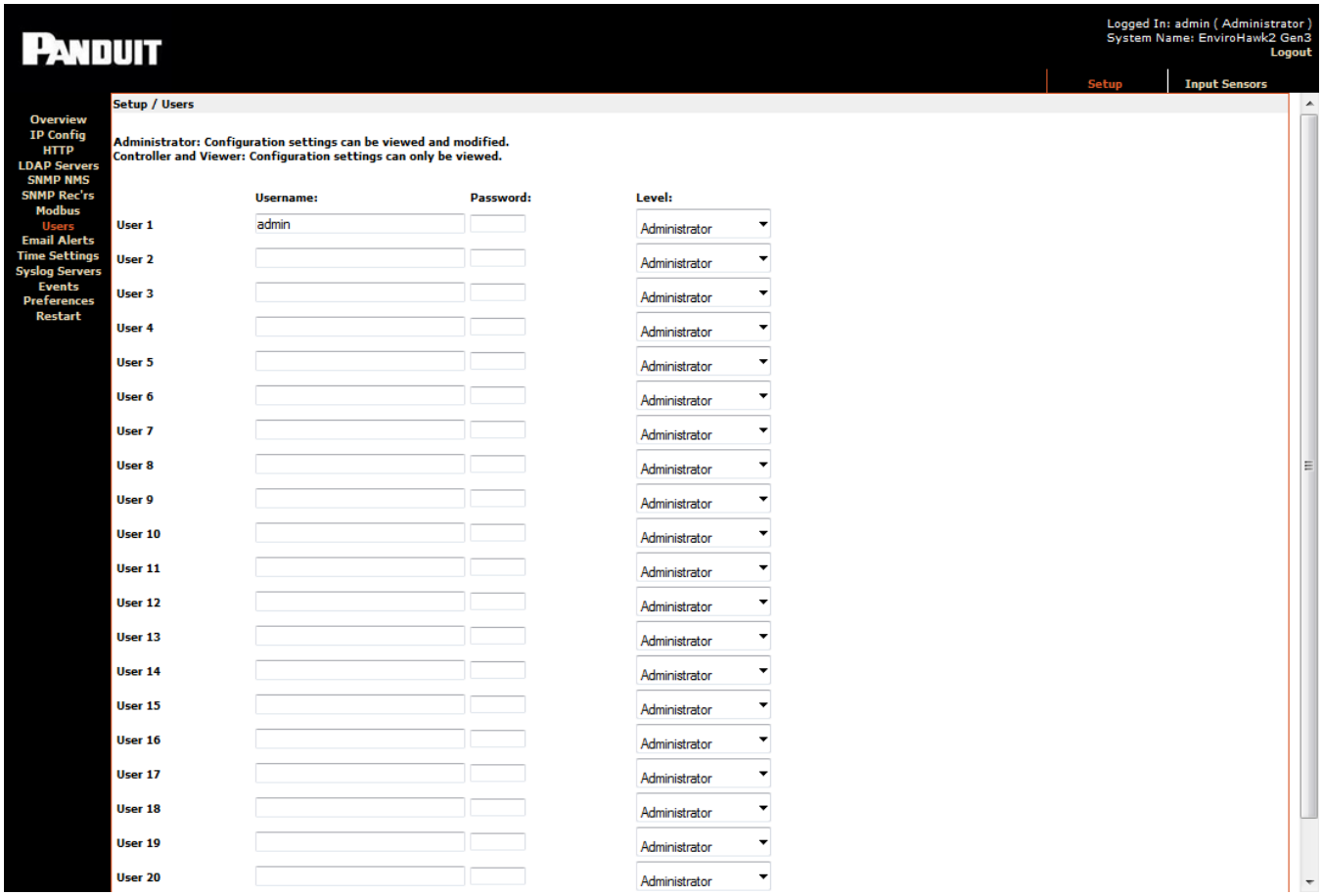
Setup - Modbus

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

Password

Enter access passwords on a per-user basis here.

Level

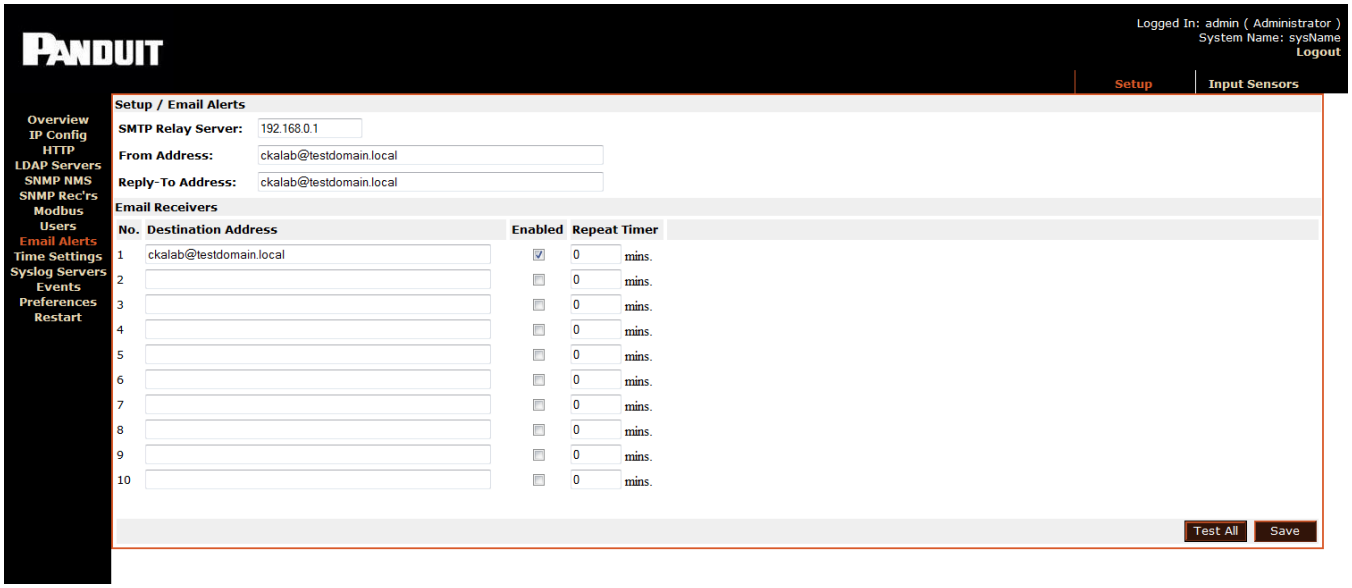
Three user levels are available for assignment.

- **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. If this happens, resetting to factory defaults is the only solution. Details on how to do this can be found in the Troubleshooting section.

Setup - Email Alerts

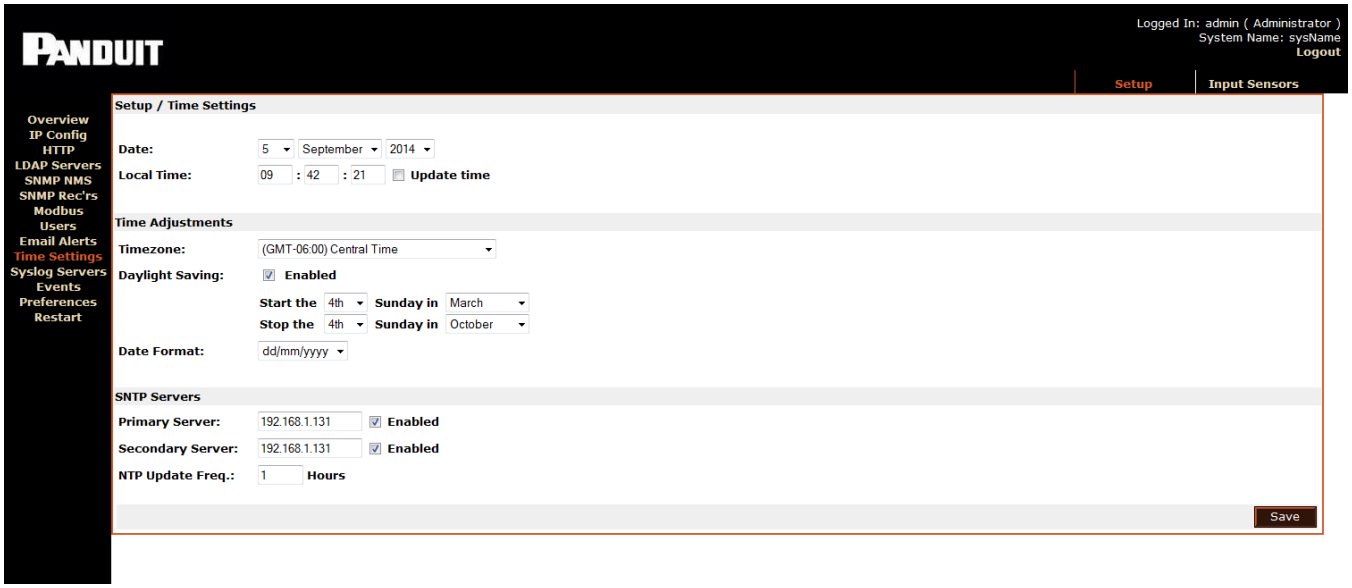
On this page, you can edit email alert settings for traps. You may set up to 10 email receivers.



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 - 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:

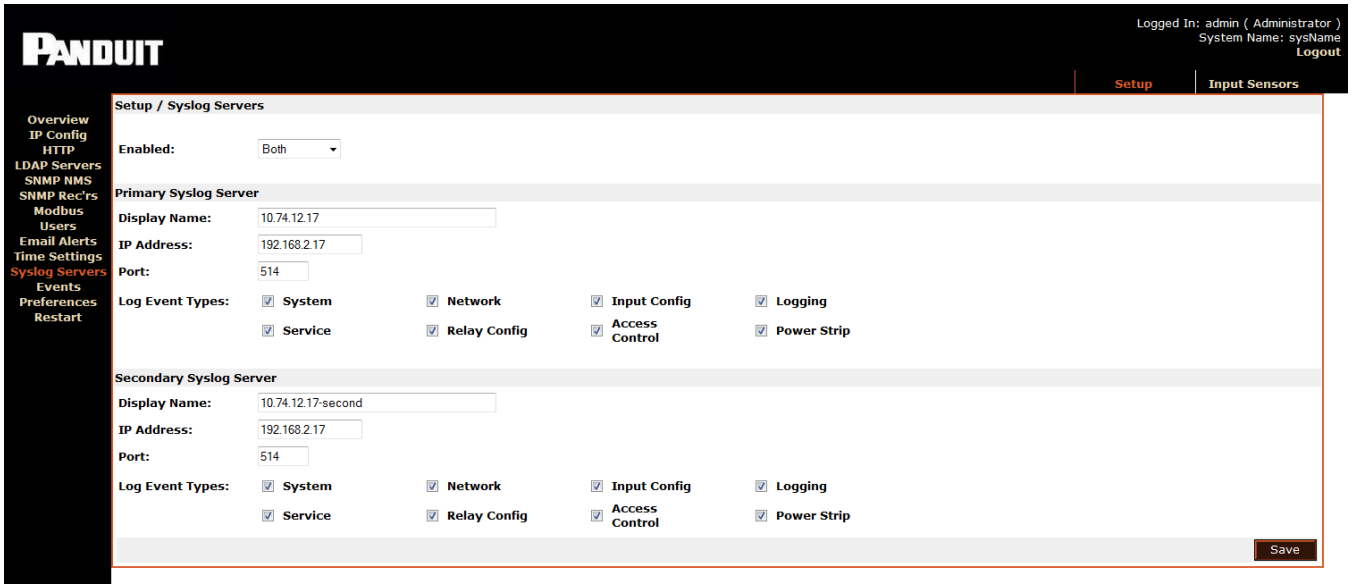
  20/08/2013 (DD / MM / YYYY)
  or
  08/20/2013 (MM / DD / YYYY)

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 - Syslog Servers

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

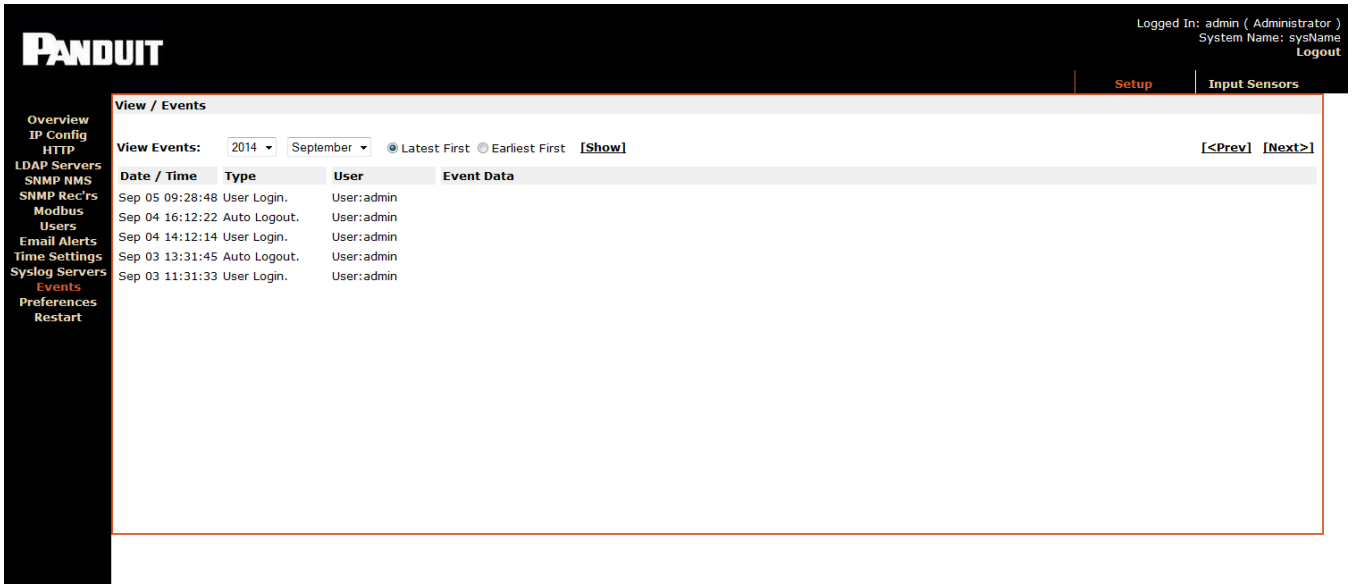


From the Enabled drop-down menu, you can choose which syslog servers are enabled. Fill in the following fields for each Syslog server.

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 - Events

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



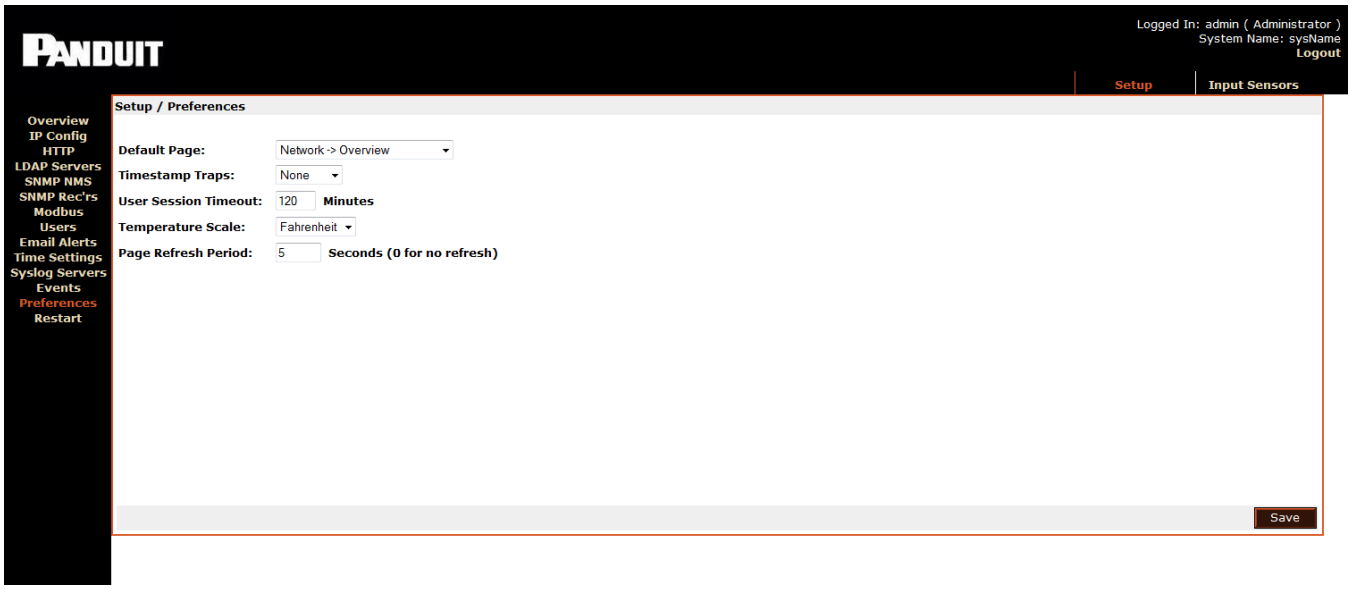
To specify a range of events to view, select the desired year and month from the drop-down menus, then click **Show**.

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 - Preferences

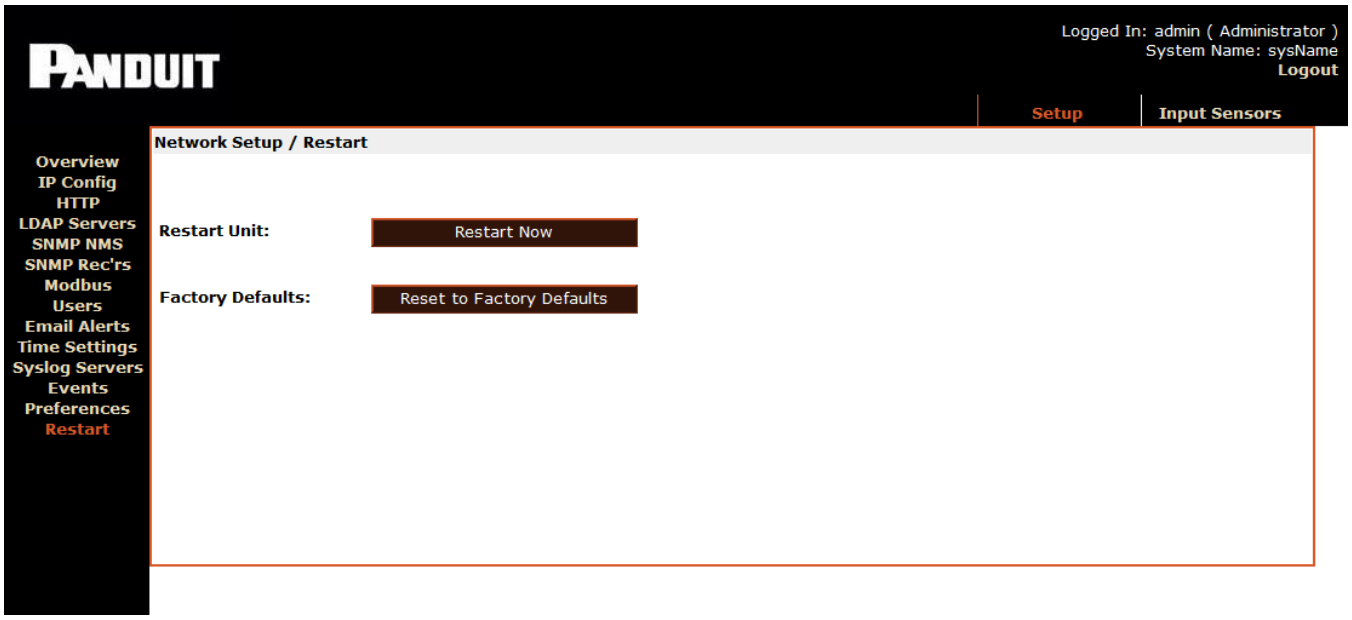
The Preferences page allows you to edit system preferences.



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: • Prefix – timestamp at the beginning • Append – timestamp at the end • 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.

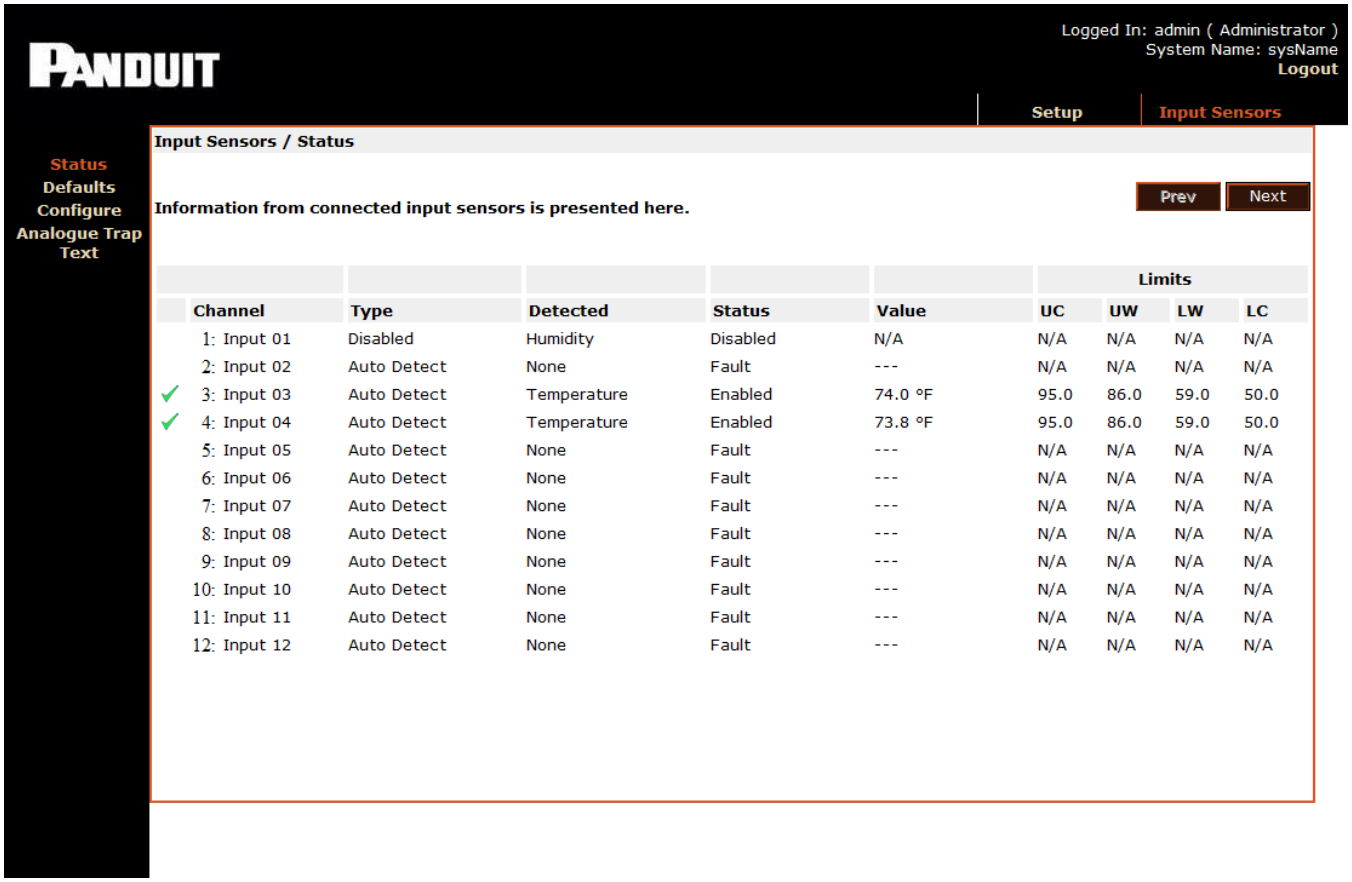
Reset to Factory Defaults

Selecting **'Reset to Factory Defaults'** instructs the unit to restore factory default settings. See the Troubleshooting section for details.

Sensor Inputs – 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.



	Channel	Type	Detected	Status	Value	Limits UC	UW	LW	LC
	1: Input 01	Disabled	Humidity	Disabled	N/A	N/A	N/A	N/A	N/A
	2: Input 02	Auto Detect	None	Fault	---	N/A	N/A	N/A	N/A
✓	3: Input 03	Auto Detect	Temperature	Enabled	74.0 °F	95.0	86.0	59.0	50.0
✓	4: Input 04	Auto Detect	Temperature	Enabled	73.8 °F	95.0	86.0	59.0	50.0
	5: Input 05	Auto Detect	None	Fault	---	N/A	N/A	N/A	N/A
	6: Input 06	Auto Detect	None	Fault	---	N/A	N/A	N/A	N/A
	7: Input 07	Auto Detect	None	Fault	---	N/A	N/A	N/A	N/A
	8: Input 08	Auto Detect	None	Fault	---	N/A	N/A	N/A	N/A
	9: Input 09	Auto Detect	None	Fault	---	N/A	N/A	N/A	N/A
	10: Input 10	Auto Detect	None	Fault	---	N/A	N/A	N/A	N/A
	11: Input 11	Auto Detect	None	Fault	---	N/A	N/A	N/A	N/A
	12: Input 12	Auto Detect	None	Fault	---	N/A	N/A	N/A	N/A

Status Indicators

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

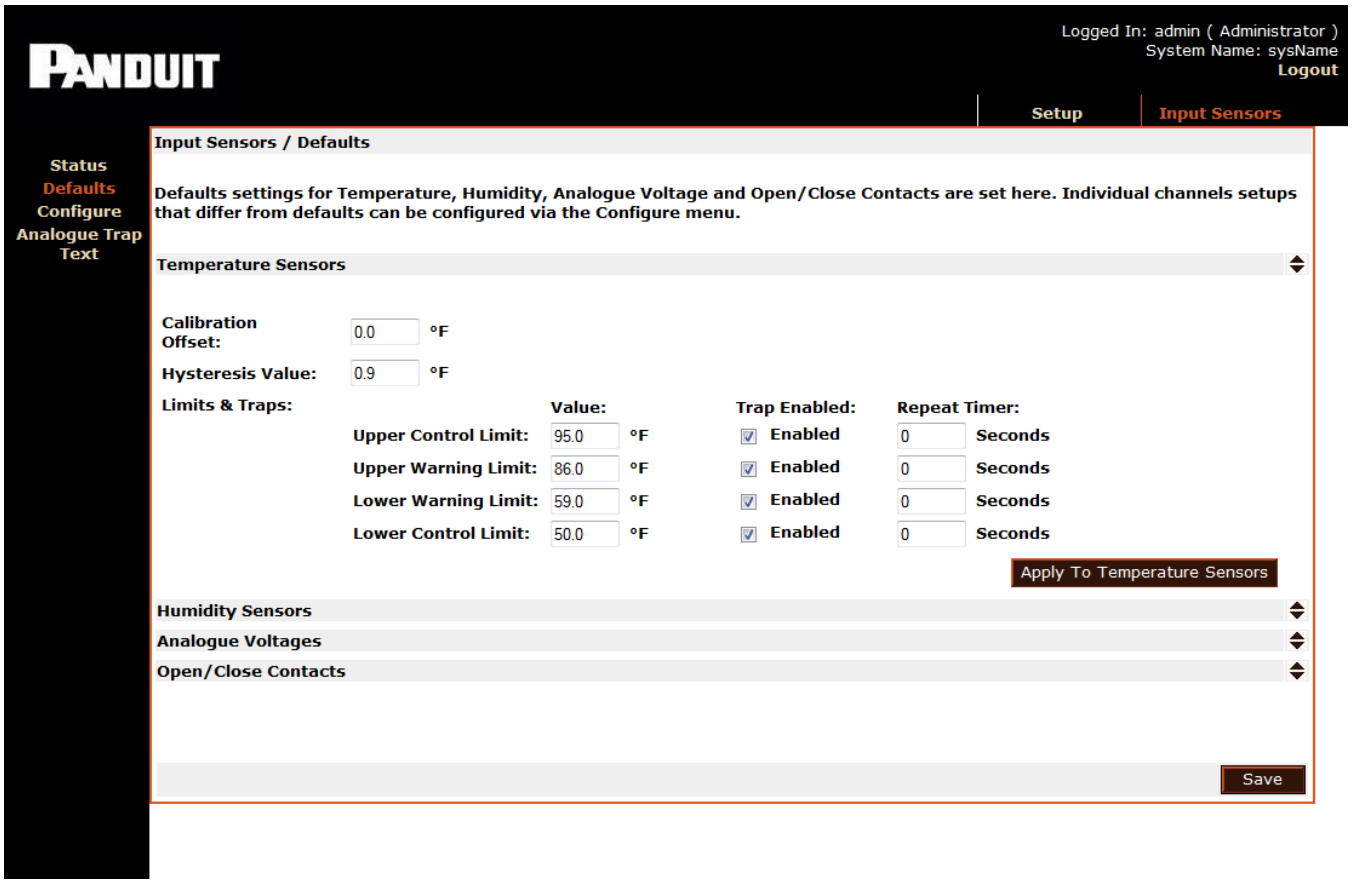
✓	Channel reading currently within threshold limits.
⚠	Upper or lower Warning limit reached or exceeded.
⊗	Upper or lower Critical limit reached or exceeded.

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:

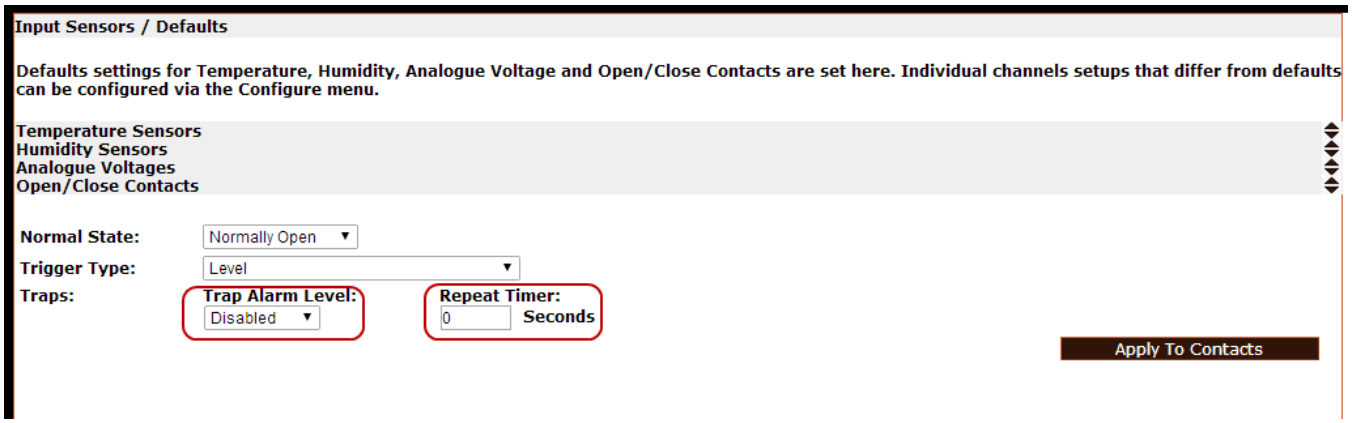
- Upper Control Limit
- Upper Warning Limit
- Lower Control Limit
- Lower Warning Limit

You can apply default trap settings for all of these thresholds. With the trap 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.



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.

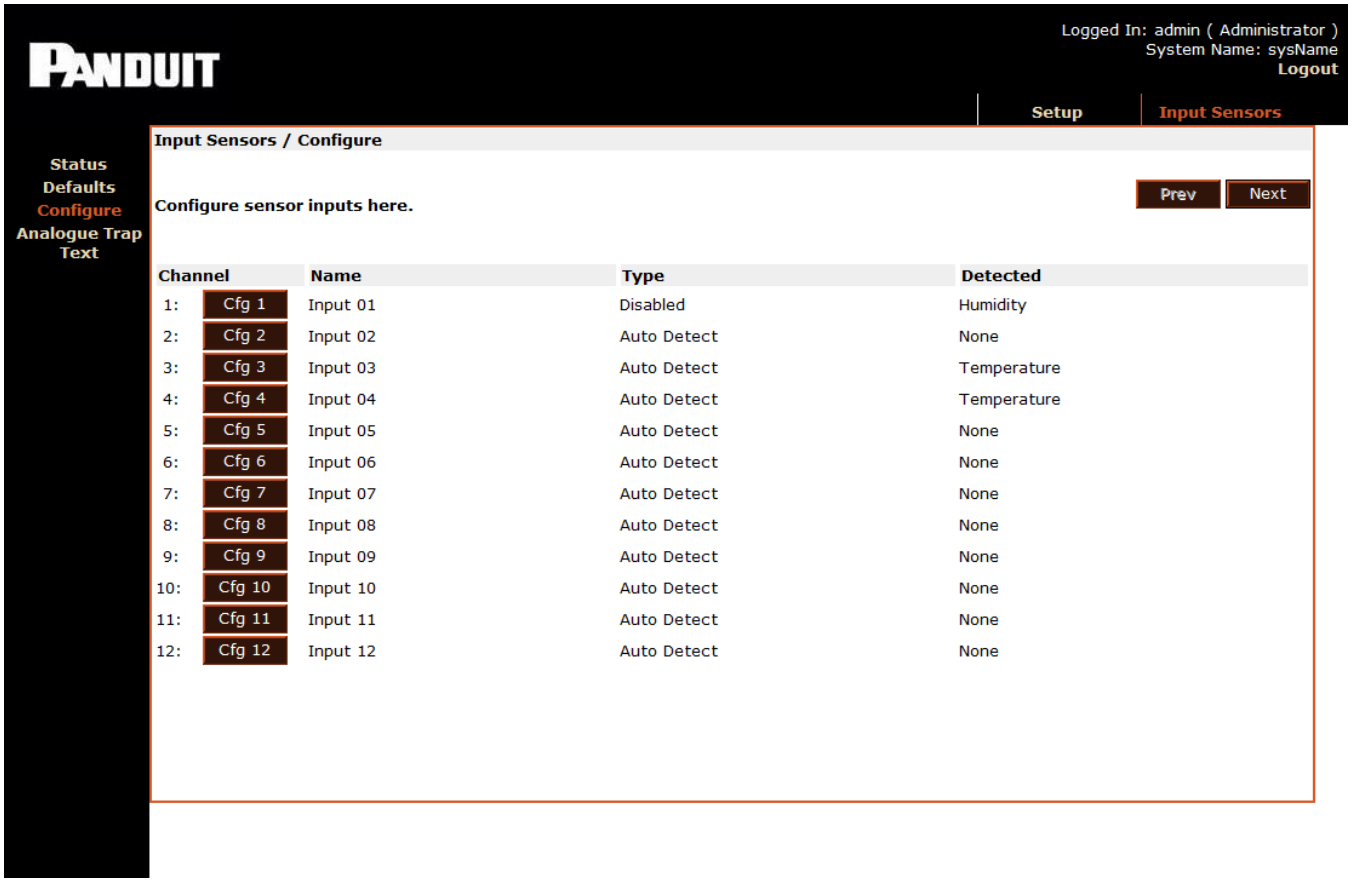
Non-Normal to Normal (Negative Edge)

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.

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

LDAP

E24 LDAP Overview

The E24 implements a Lightweight Directory Access Protocol (LDAP) client.
This allows the E24 unit to authenticate user logins to the Web Management Interface (WMI) 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 access is denied by LDAP then the credentials are checked against the E24 internal user list.
Note!Configuration of LDAP is an advanced topic and requires existing knowledge of LDAP function and setup (or access to personnel who do).

E24 LDAP Structure

In order for a E24 unit to successfully authenticate a user for WMI login it needs to be ‘pointed’ to a specific structure within a directory.
A unit is ‘pointed’ to this structure within a directory by specifying the Unit Base DN on the Network Setup – LDAP page.
The following Organisational Units will need to be created:

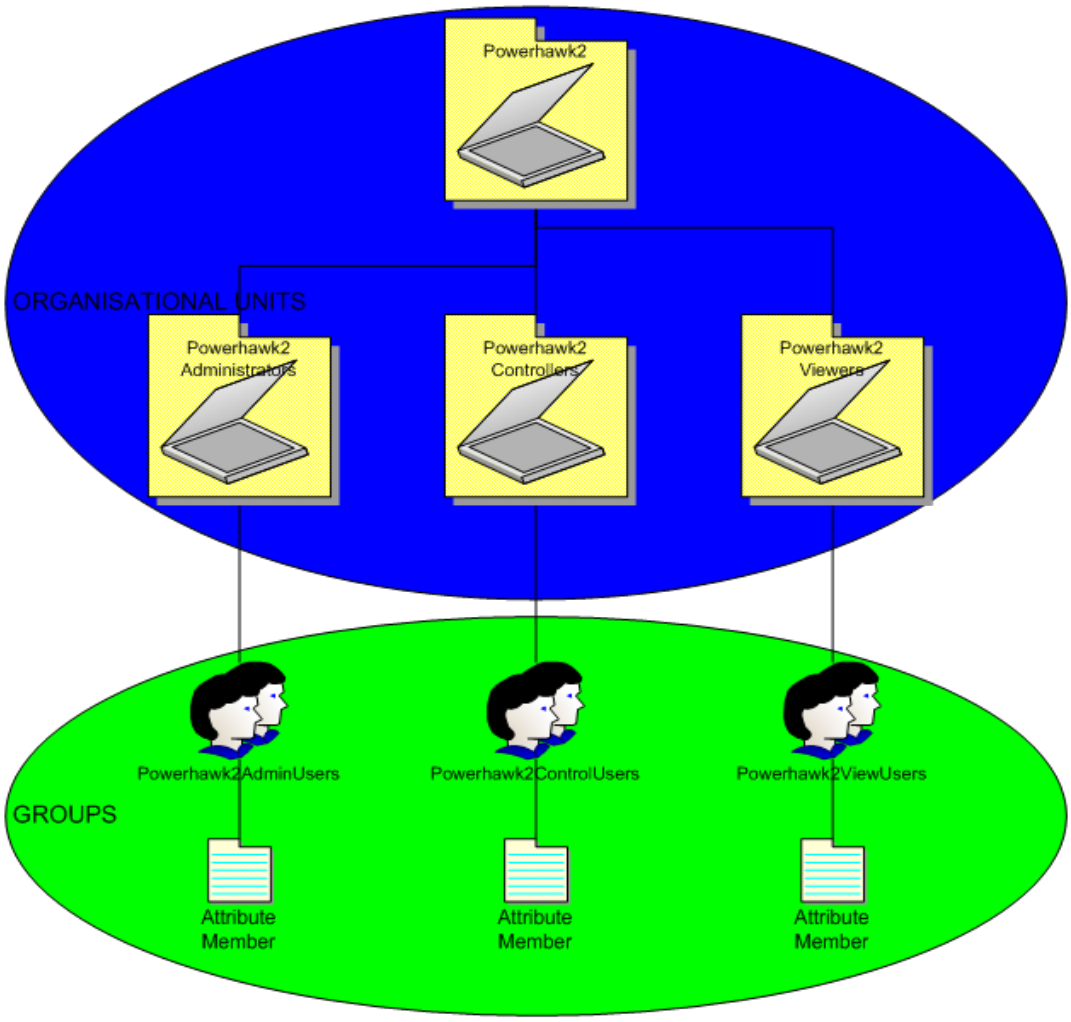
- E24 (this can be named anything)
- E24Administrators
- E24Controllers
- E24Viewers

The following Groups will need to be created:

- E24AdminUsers
- E24ControlUsers
- E24ViewUsers

Note: Groups referred to are groups as found in Active Directory schema. However any implementation which provides a group with a ‘members’ attribute may function.

The following figure depicts the E24 LDAP authentication structure:



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

- E24AdminUsers
- E24ControlUsers
- E24ViewUsers

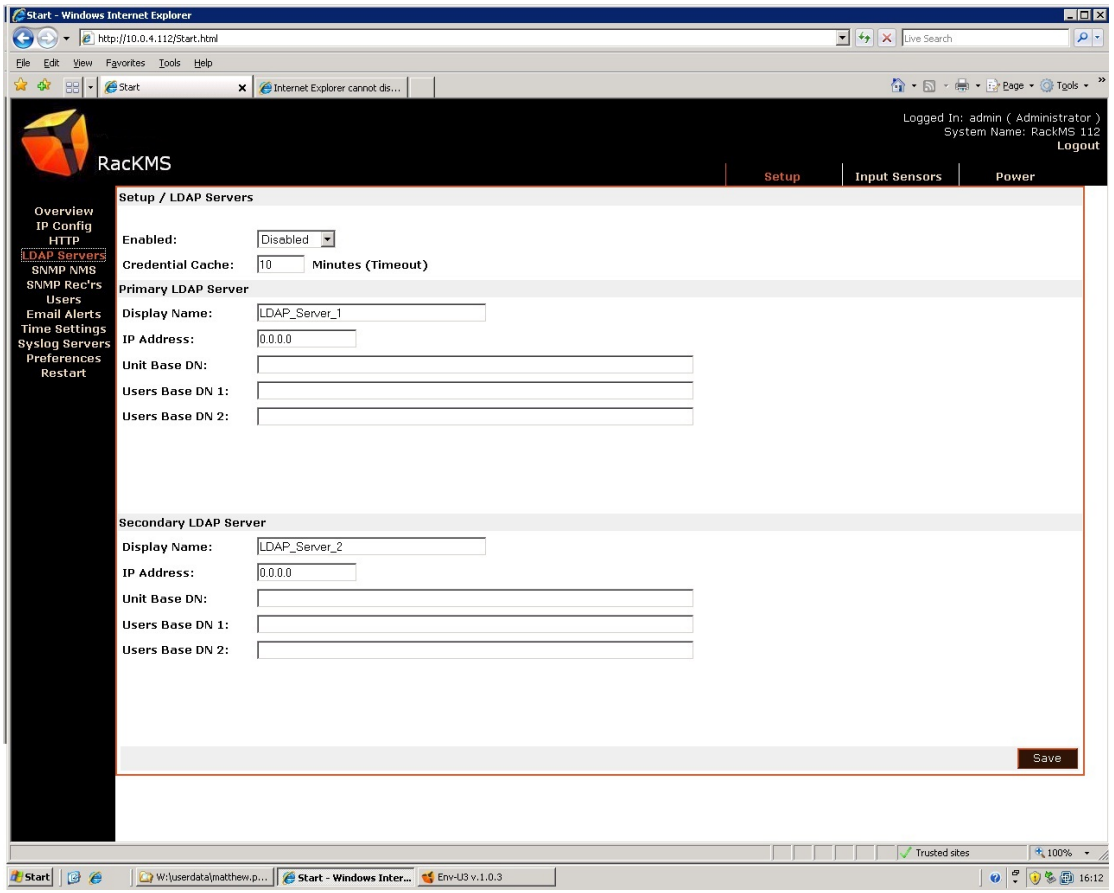
Group Membership and Access Level

Membership of these groups grants the following permissions on E24 units:

- **E24AdminUsers**: Users placed into this group will have Admin privileges on E24 units.
- **E24ControlUsers**: Users placed into this group will have Controller privileges on E24 units.
- **E24ViewUsers**: Users placed into this group will have View privileges on E24 units.

E24 Unit Configuration

For LDAP authentication to function, each E24 unit requires certain configuration values to be provided.



1. If one LDAP server is to be used select **Enabled – Primary**.
2. Enter a descriptive name, E.g: AD_Server_1 into **Display Name**.
3. Enter the complete DN of the top level OU as seen in LDAPLDAP.
4. Enter the DN of where users that are members of E24 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** to bring any changes into effect.

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.

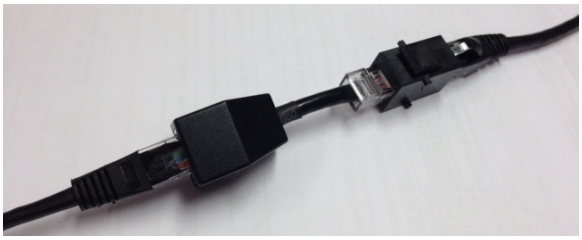
Before the adapter is fitted:

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 Gateway system, please contact Panduit Technical Support using one of the following methods:

- 1-866-721-5302 (toll-free)
  - Orland Park, USA: 6:30 a.m. – 8:00 p.m. CST
  - Mumbai, India: 6:30 a.m. – 5:00 p.m. IST (8:00 p.m. – 6:30 a.m. 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 ~ 240VAC 50Hz / 60 Hz 0.5 Amp Maximum
Operating Temperature:	0^{O}C to 40 ^{O}C
Storage Temeperature:	-10 ^{O}C to 70 ^{O}C
Operating Humidity:	5% to 90% RH
Storage Humidity:	5% to 100% RH

Caution: Risk of explosion if battery is replaced by an incorrect type. Dispose of used batteries according to the instructions.

Unit Dimensions

Heigth:	44mm(1U)[1.73”]
Width:	483mm[19”]
Depth:	114.4mm[4.5”]
Unit net weight:	2.08kg [73.36 oz]

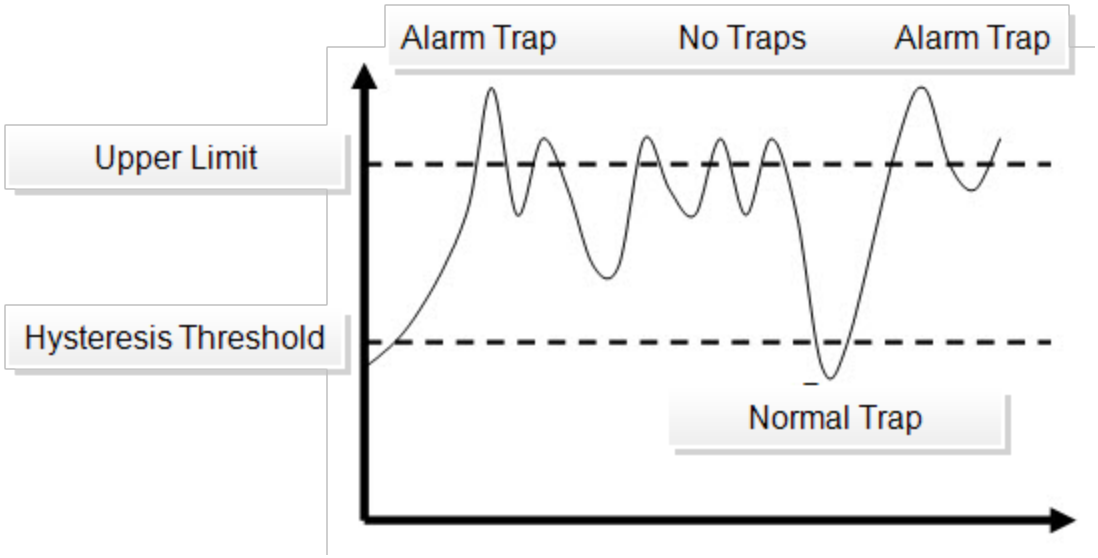
Appendix B: Hysteresis Demystified

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