USER MANUAL

EME160A, EME160A-UC, EME161A-R2

ALERTWERKS GATEWAY 4-PORT

24/7 TECHNICAL SUPPORT AT 1.877.877.2269 OR VISIT BLACKBOX.COM

BLACK BOX®

TABLE OF CONTENTS

TABLE OF CONTENTS

CHAPTER 1: SPECIFICATIONS

TABLE 1-1. GATEWAY SPECIFICATIONS

SPECIFICATION	DESCRIPTION
Inputs	(4) RJ-45 sensor ports for connecting AlertWerks sensors (1) RJ-45 Ethernet 10/100 ports
Outputs	(4) RJ-45 sensor ports (These ports can carry configurable output signals [0 VDC/5 VDC].)
Number of Users	100
Indicators	(1) Power LED, (1) Network Connectivity LED, (4) Sensor Status LEDS; (1) Buzzer for audible alert on sensor status
Power	5- VDC, 3-A
Mounting	Desktop Rackmounted or DIN-rail mounted
Max Sensors	Maximum of 150 online sensors, including Expansion Units and virtual sensors
Operating Environment	Temperature: -13 to +176˚ F (-25 to +80 ˚ C) Humidity: 20 to 80% noncondensing
MTBF	1,400,000 hours
Dimensions	1.25"H x 4.5" W x 2.5" D (3.2 x 11.4 x 6.4 cm)

CHAPTER 2: OVERVIEW

2.1 INTRODUCTION

This manual covers the main features and basic configuration of the AlertWerks Gateway.

The AlertWerks Gateway is a high-speed, accurate, intelligent environmental monitoring device, featuring a completely embedded host and operating system.

2.2 FEATURES

- IP based, including SNMPv3, HTTPS, VPN, and MQTT
- Send encrypted SNMP Trap and Email Notifications
- Supports four Intelligent Sensors
- EME160A: Two sensor ports enabled by default. Unlock all four ports with unlock code: EME160A-UC
- Notification Wizards
- Wide range of available sensors
- Optional expansion module connectivity
- Virtual sensors

NOTE: Some of the pictures shown in this manual might not represent the actual Web UI of the unit; this is because we are constantly working on improving the firmware. Contact Black Box Technical Support at 877-877-2269 or techsupport@blackbox.com if you have any issues configuring your unit.

2.3 WHAT'S INCLUDED

Your package should contain the following items. If anything is missing or damaged, contact lack Box Technical Support at 877-877-2269 or techsupport@blackbox.com

- (1) Alertwerks Gateway
- (1) In-line Power Supply (Input: 100-240VAC, 50/60Hz, 2A - Output: 5VDC, 3A – C13 receptacle)
- (1) Power Cord, C14 to NEMA 5-15P
- (1) RJ-45 to RJ-45 crossover cable, 5-foot (1.5-m)
- (1) CD (Manual)

2.4 HARDWARE DESCRIPTION

2.4.1 BACK PANEL: PORTS

Port numbering starts from the power connector on the unit: the closest port to the power connector is Port 1 and closest to the Ethernet interface is Port 4.

You may connect AlertWerks sensors to any available ports.

CAUTION: If you're using analog pins on the sensor ports (with manually on-lined DCV sensors, and pin 7 of the RJ-45 connector), make sure that the voltage doesn't exceed 3 Volts. Otherwise, you might damage the unit!

FIGURE 2-1. BACK PANEL

TABLE 2-1. BACK PANEL COMPONENTS

NUMBER IN FIGURE 2-1	COMPONENT	DESCRIPTION
1	(4) Sensor ports	Connect AlertWerks sensors
2	(1) Barrel connector	Connect for power supply

2.4.2 TOP PANEL: STATUS LEDS

Figure 2-2 shows the LEDs on the top panel of the AlertWerks Gateway . Table 2-2 describes their functions.

FIGURE 2-2. TOP PANEL: STATUS LEDS

TABLE 2-2. TOP PANEL COMPONENTS

NUMBER IN FIGURE 2-2	COMPONENT	DESCRIPTION
1	(1) Power/Ethernet (ETH) LED (red/green)	Turns red if there's no network connection, and blinks green (according to LAN activity) when the connection is normal.
2	(4) Sensor LEDs #1–4 (green)	Off = offline On = online and normal Slow blinking = Warning status Fast blinking = Critical and Error status

2.4.3 SIDE PANEL: RESET BUTTON

There are specific commands you can send to the unit by holding the Reset button for a specified amount of time.

Use a straightened paperclip to press Reset.

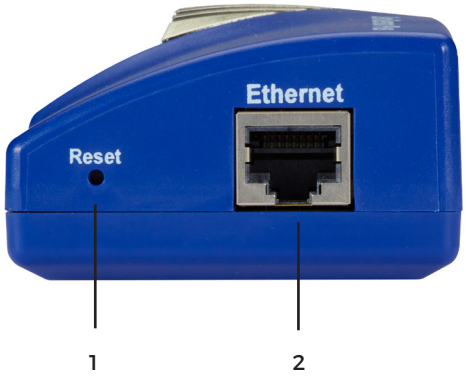

FIGURE 2-3. SIDE PANEL

TABLE 2-3. SIDE PANEL COMPONENTS

NUMBER IN FIGURE 2-3	COMPONENT	DESCRIPTION
1	Reset button	Resets the gateway, see Table 2-4 for functions
2	RJ-45 connector	Links to Ethernet

TABLE 2-4. RESET BUTTON FUNCTIONS

TIME TO HOLD	ACTION
3 to 7 seconds	Reboot
7 to 12 seconds	Web UI password reset
12 to 17 seconds	Serial flash erase (DB erase without factory reset, the system configuration is kept)
17 to 25 seconds	Reset to factory defaults (serial flash erase + config erase)

CHAPTER 3: CONFIGURATION

3.1 SETTING UP THE UNIT'S IP ADDRESS

NOTE: The units ship with the passwords enabled. The default log in for the web interface is:

Username: admin

Password: public

Every unit is shipped with the default IP address of 192.168.0.100

First, we will go through the process of changing this IP address to fit your own network configuration.

NOTE: In some cases, your computer might not be able to connect to this default IP address. In this situation, you either need to:

a) add this IP to your computer's routing table or

b) add a secondary IP address to the LAN card to allow access to the unit.

See below for instructions on how to set these up.

Ensure the following items are available to you before starting:

- RJ-45 CAT5 crossover cable with an RJ-45 male connection
- A PC with Ethernet card or LAN socket, logged in with Administrator rights

Follow these steps:

1. Connect the unit via the Ethernet port of the unit to your computer's LAN or Ethernet port with a CAT5 crossover cable.
2. Open a web browser and type the default IP address, then press enter.
3. You'll be presented with the Summary page.
4. Go to the System/Network page to change the network settings (see Section 4.2.4 in this manual).

Once you have assigned the new IP address use the "ping" command to test the unit's reply.

3.1.1 HOW TO ADD A MANUAL ROUTE TO THE COMPUTER'S ROUTING TABLE

Open an Administrator Command Prompt (CMD) window and type:

route add 192.168.0.100 10.1.1.20

Where 10.1.1.20 is the IP address of the Ethernet interface on the PC that the unit is plugged into with the crossover cable.

NOTE: If you do not receive an OK message. then a parameter was wrong or missing.

The route is not persistent (removed upon rebooting), but you can also delete it with the route delete 192.168.0.100 command.

3.1.2 HOW TO ADD A SECONDARY IP ADDRESS TO THE COMPUTER'S LAN CARD

You can do this via the GUI by opening the LAN connection's properties:

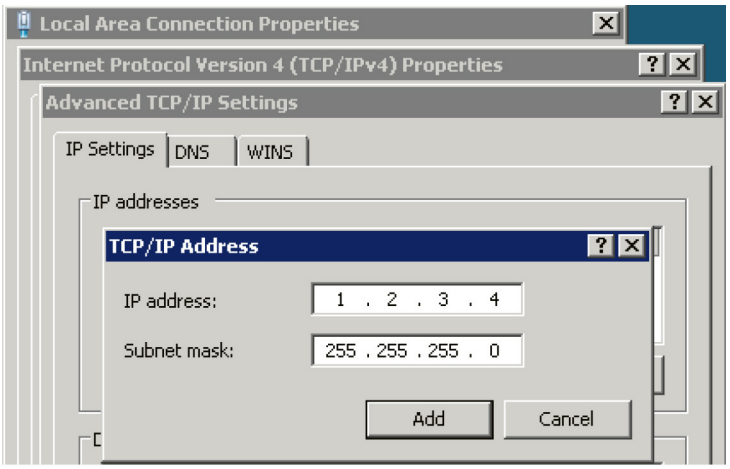

FIGURE 3-1. TCP/IP ADDRESSES SETTING SCREEN

Or open an Administrator Command Prompt (CMD) window and type:

netsh interface ipv4 add address "Local Area Connection" 192.168.0.2 255.255.255.0

The above command adds the IP Address 192.168.0.2 (with Subnet Mask 255.255.255.0) to the connection titled "Local Area Connection."

You will then be able to connect to the unit with its default IP.

NOTE: The secondary IP address is permanent for the LAN connection; don't use it if you only need it once. Instead, use the routing table method above.

4.1 SUMMARY PAGE

Figure 4-1 shows the summary page.

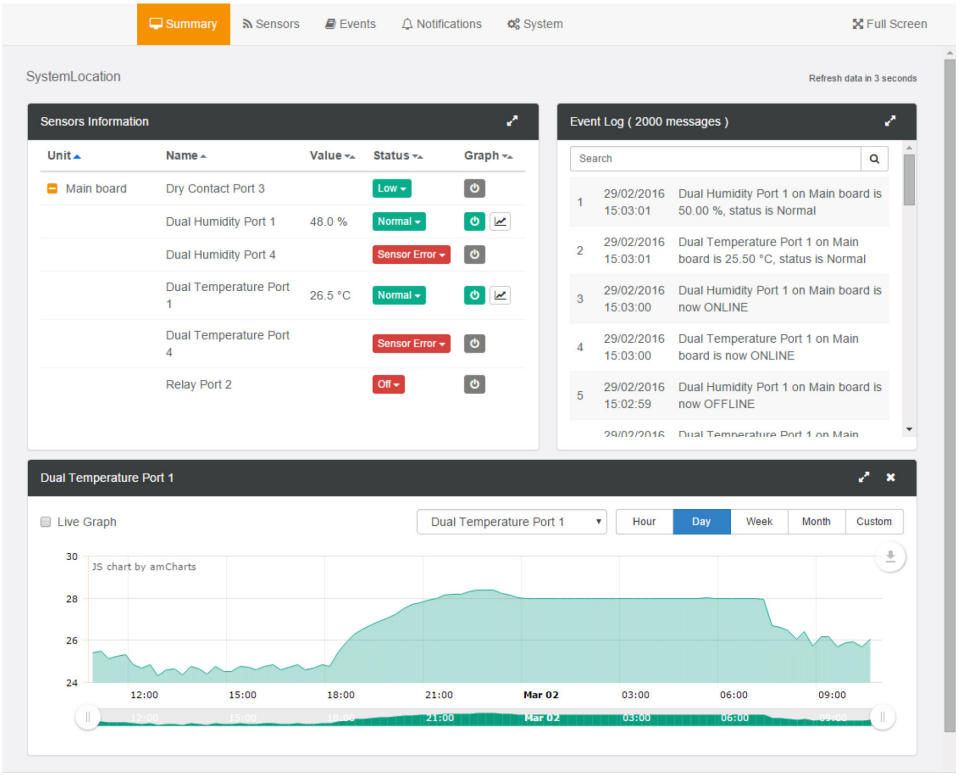

FIGURE 4-1. SUMMARY PAGE

This is the Summary page with Sensor Status and the Event Log, with the Sensor Graph enabled.

The Event Log contains all entries from the “All Events” category.

The last 30 entries are shown, but if you’re scrolling down the list, more events (30 more) will be loaded automatically. You can view the full log if you keep scrolling down.

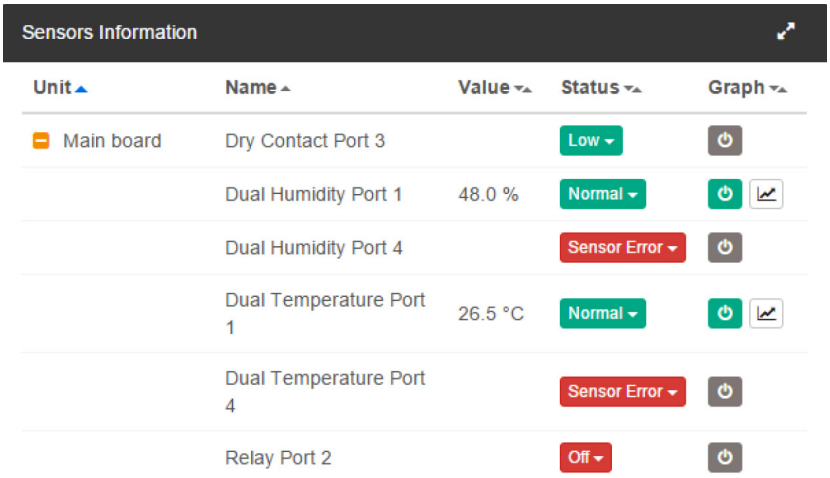

FIGURE 4-2. SENSOR INFORMATION WINDOW

In the Summary page's Sensors Information window you can do the following:

- Directly acknowledge a sensor's status, and put the sensor offline.

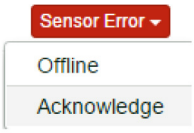

FIGURE 4-3. ACKNOWLEDGE SENSOR OR PUT IT OFFLINE

- Control the relay-type sensors.

FIGURE 4-4. CONTROL THE RELAY TIME SENSORS

- Enable/disable graph data collection per sensor, and display the graph display window for the Summary page.

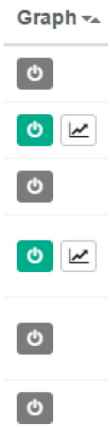

FIGURE 4-5. GRAPH DISPLAY WINDOW

We'll explain the Graph feature in more detail next.

4.1.1 GRAPH FEATURE

After you've enabled the data collection for a sensor, you can choose to display specific time intervals of the stored data: hourly/daily/weekly/monthly and custom display interval.

You can also export the recorded data in multiple formats.

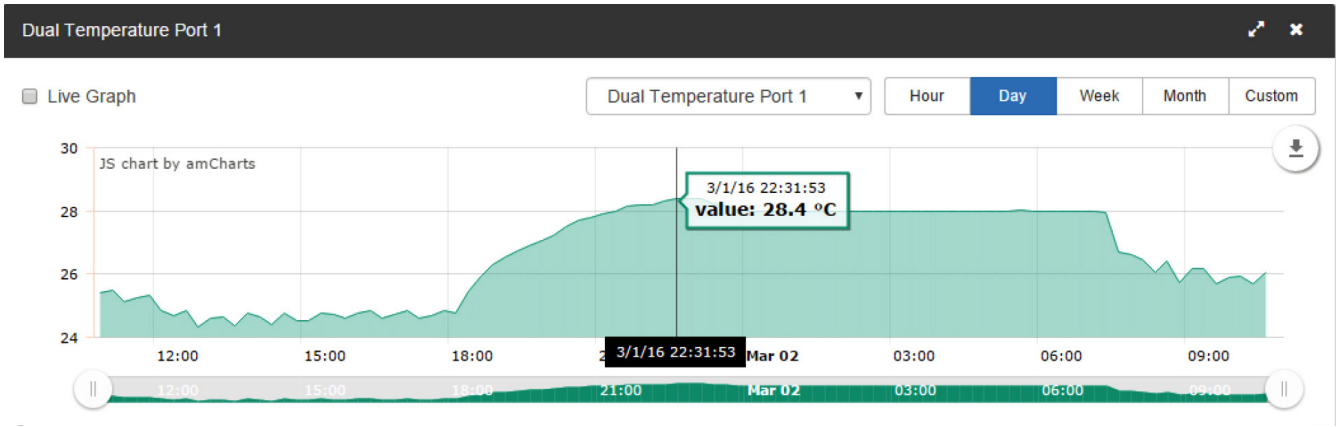

FIGURE 4-6. GRAPH FEATURE EXAMPLE

In this example picture, we've chosen to display the temperature sensor's daily maximum.

You could also resize the graph window (including full screen) and move the scale to display more or less data.

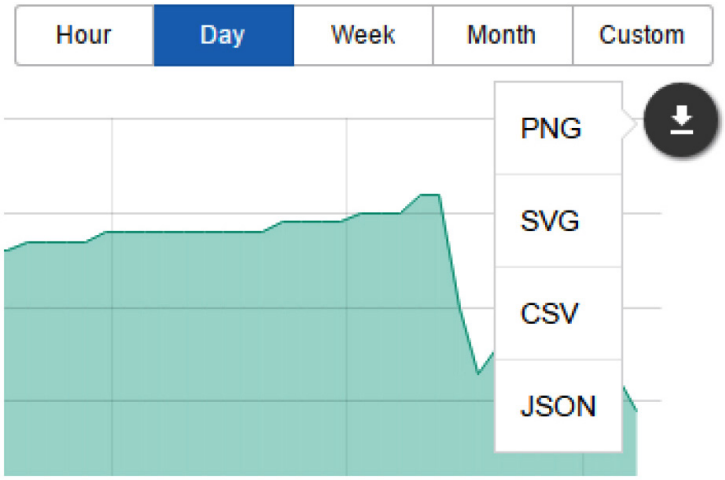

FIGURE 4-7. GRAPH FORMATS DROPDOWN MENU

You can choose to export the graph data in selected formats by clicking on the icon on the right.

The file will be downloaded automatically and assigned a file name that will contain the sensor's name, IP address of the unit, and the date and time.

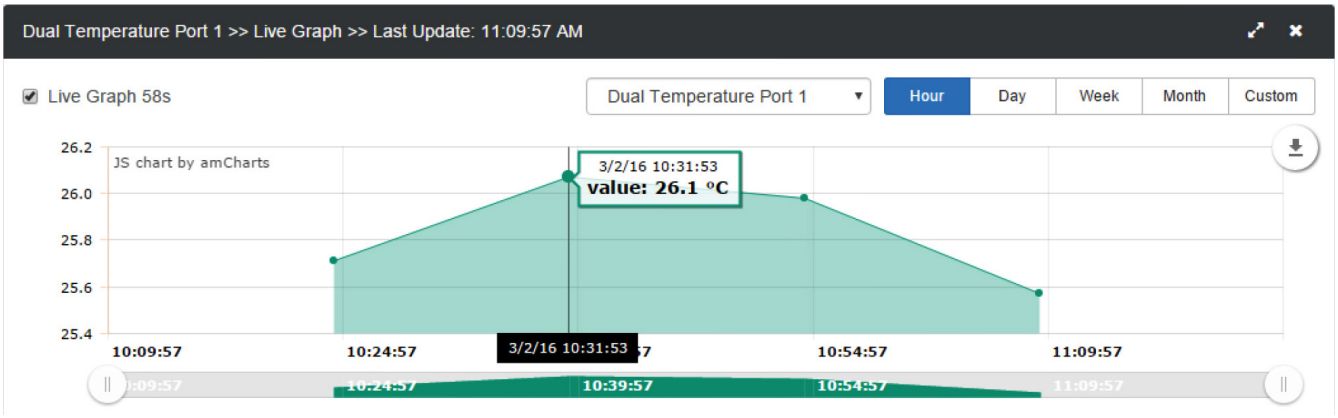

FIGURE 4-8. LIVE GRAPH OPTION

By choosing the Live Graph option, you can get continuous updates of the graph data (by default every 60 seconds). If you don't use this option, the graph data needs to be refreshed manually.

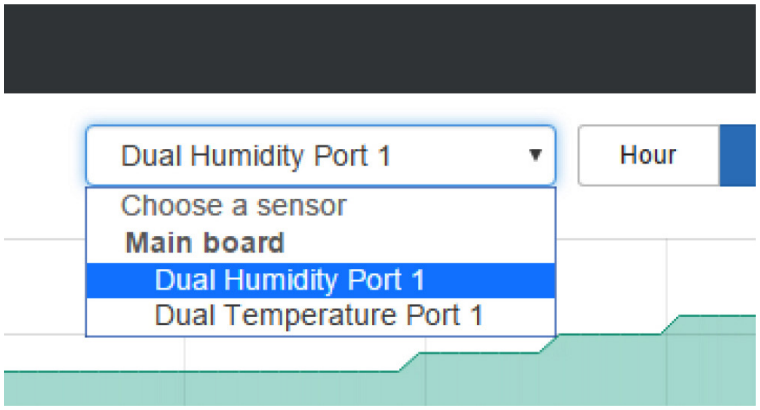

FIGURE 4-9. SENSORS' DROP-DOWN MENU

To change to a different sensor's graph, choose it from the drop-down menu.

NOTE: You can only choose a sensor here that you've already enabled the graph data collection for.

4.2 SYSTEM PAGE

Figure 4-1 shows the summary page.

4.2.1 GENERAL

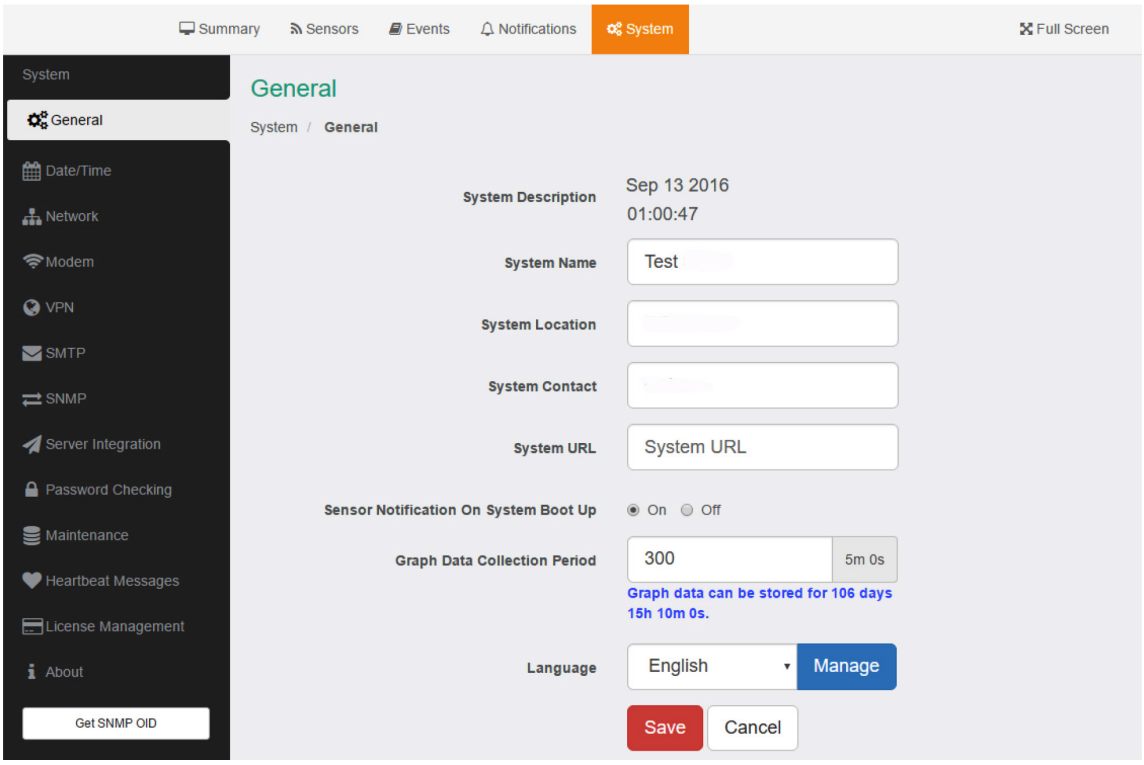

FIGURE 4-10. SYSTEM PAGE, GENERAL SETTINGS

in the previous screen, you can change general settings for the device.

The unit's firmware version is shown in the Description field, and the System Name/Location/Contact options are user configurable.

You can also specify the System URL option for quick access of a custom part of the Web UI for example, but you can specify any URL.

By changing the Graph Data Collection Period, you can choose how frequently the data is sampled.

NOTE: If you had stored graph data previously, changing this setting will clear the data.

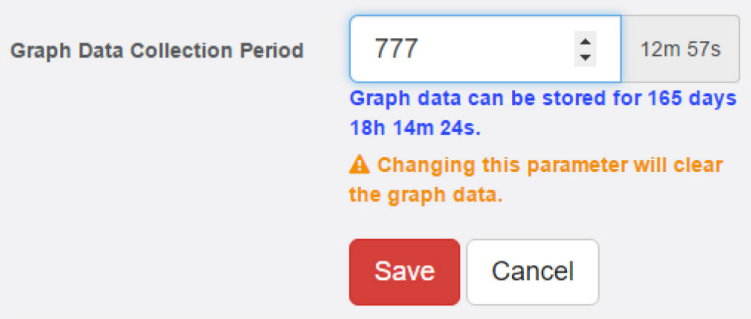

FIGURE 4-11. GRAPH DATA COLLECTION PERIOD SCREEN

NOTE: A Low Power Mode is selectable from EMEMS; on the Web UI this option is not shown.

With the Sensor Notification On System Boot Up option, you can choose to allow/disallow running the notifications with sensor values read at system boot up. In some cases, invalid values are read while the unit is starting up, and you could get false alarm notifications. You can disable the notification processing at startup with this option.

On each System subpage you can see a Get SNMP OID button (where applicable).

FIGURE 4-12. GET SNMP OID BUTTON

This will give you a popup window with all relevant OIDs for the actual page (the General page is shown next).

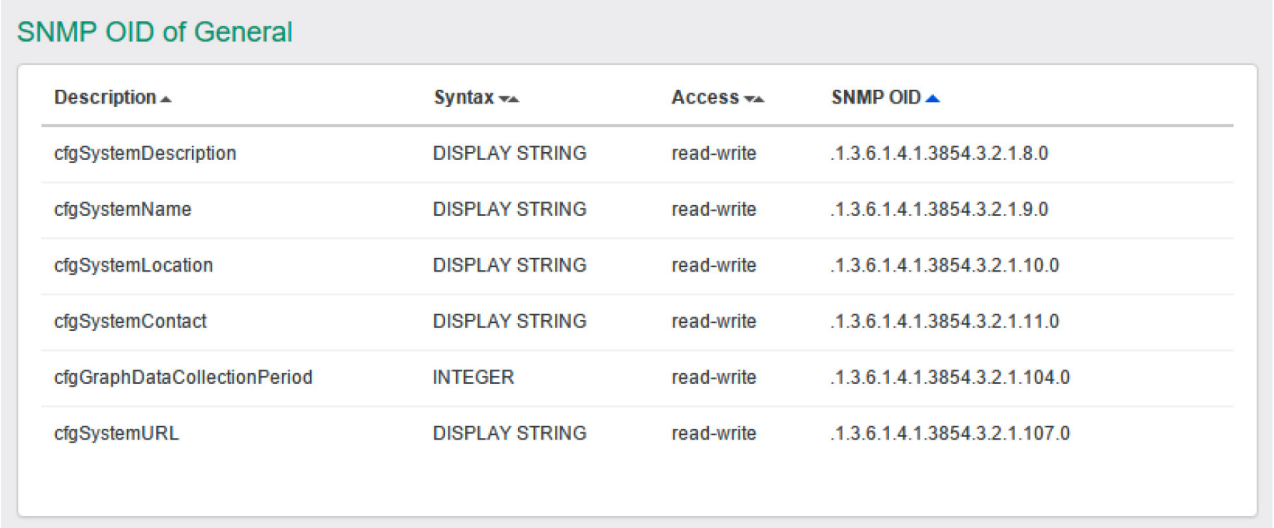

FIGURE 4-13. SNMP OID OF GENERAL PAGE

You can use OIDs for SNMP calls and in custom scripts, or for setting up the unit for monitoring by a third party NMS software such as WhatsUpGold or Paessler.

This button is also accessible on the Sensors page.

4.2.2 LANGUAGE MANAGEMENT

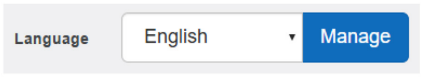

FIGURE 4-14. LANGUAGE MANAGEMENT BUTTON

You can change the display language of the Web UI with this option. Only one additional language is supported, together with the default (and fallback if there's an error) English.

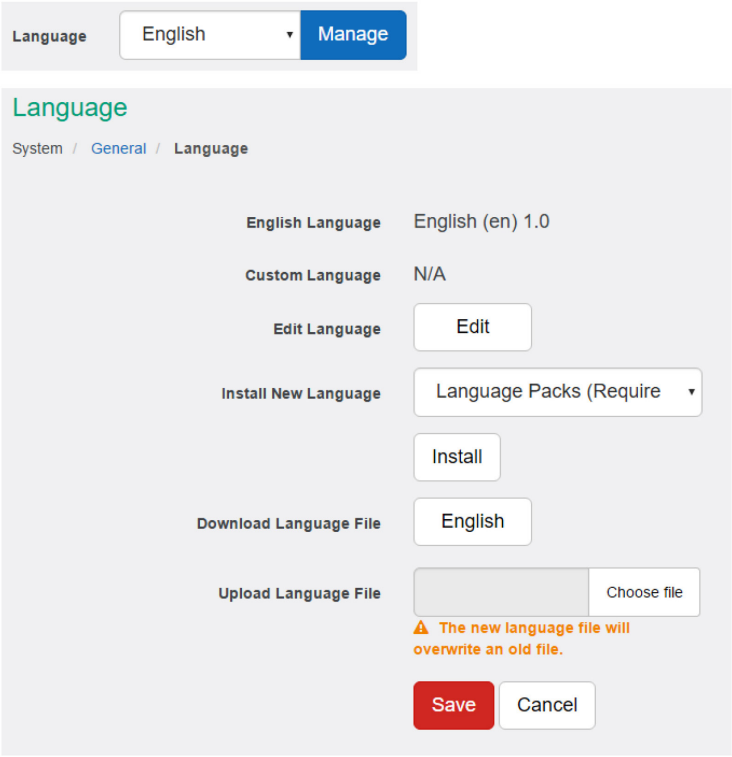

FIGURE 4-15. LANGUAGE SCREEN

In Manage, you can choose to Download Language File if you'd like to edit the language file offline (you can also download the custom language's file if it's already present). Then upload the completed file, and it will be selectable as the Custom Language. For official translation files, the language code and version will show the correct values.

NOTE: Whenever you upload or install a custom language file, it will overwrite the old file. Only one additional language is supported.

For separately downloadable language files, contact Black Box Technical Support.

Select a language from the drop-down menu Install New Language.

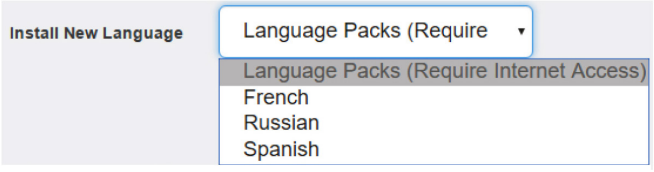

FIGURE 4-16. INSTALL NEW LANGUAGE BUTTON

Then press the Install button. It will ask you to confirm the action in a popup window.

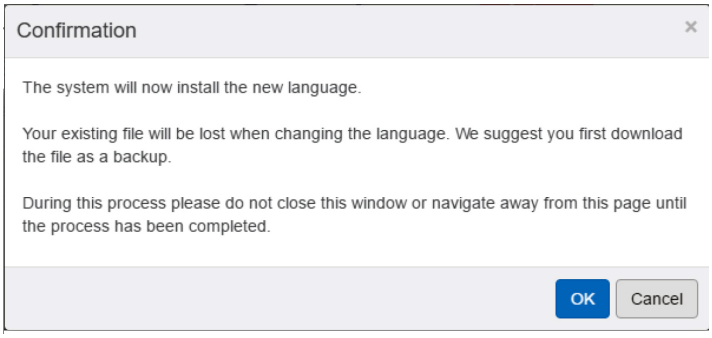

FIGURE 4-17. CONFIRMATION WINDOW

Wait until the language is downloaded and installed.

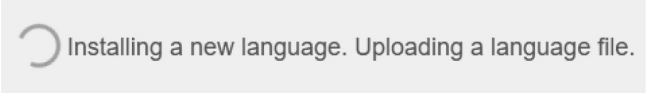

FIGURE 4-18. INSTALLING LANGUAGE MESSAGE

The unit will notify you about the successful language change, and will change the language of the Web UI. You can switch back to English by selecting it from the drop-down list on the General page, then press Save.

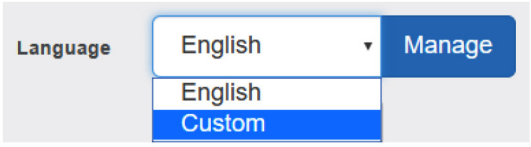

FIGURE 4-19. DROP-DOWN LIST

After you've added the custom language, you can manage it from the same menu.

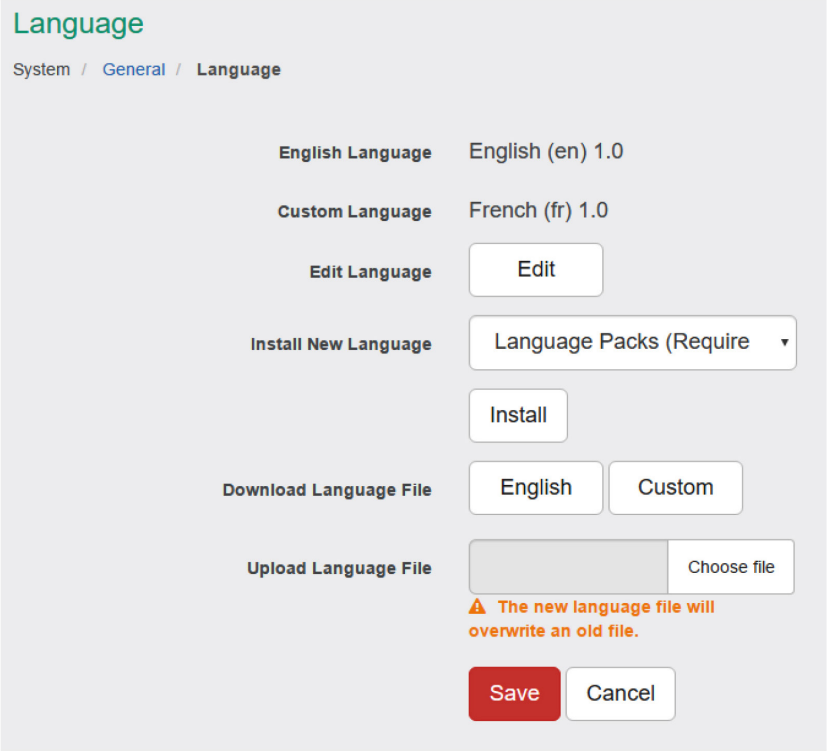

FIGURE 4-20. LANGUAGE SCREEN, CUSTOM LANGUAGE

NOTE: The official language files are also included in the firmware update packages.

You can also edit the chosen language directly in the Web UI, if you choose Edit Language.

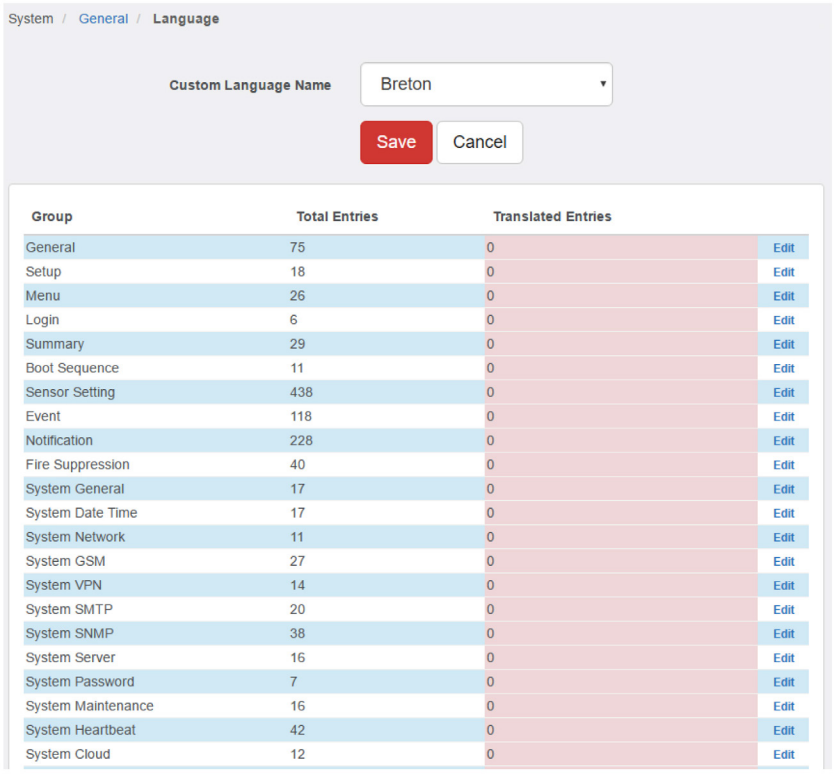

FIGURE 4-21. EDIT LANGUAGE IN WEB UI

If the custom language file is present, you can select it from the drop-down list on the General page.

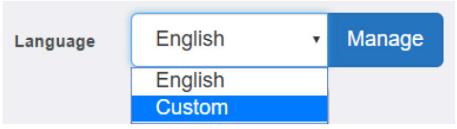

FIGURE 4-22. DROP-DOWN LIST

4.2.3 DATE/TIME

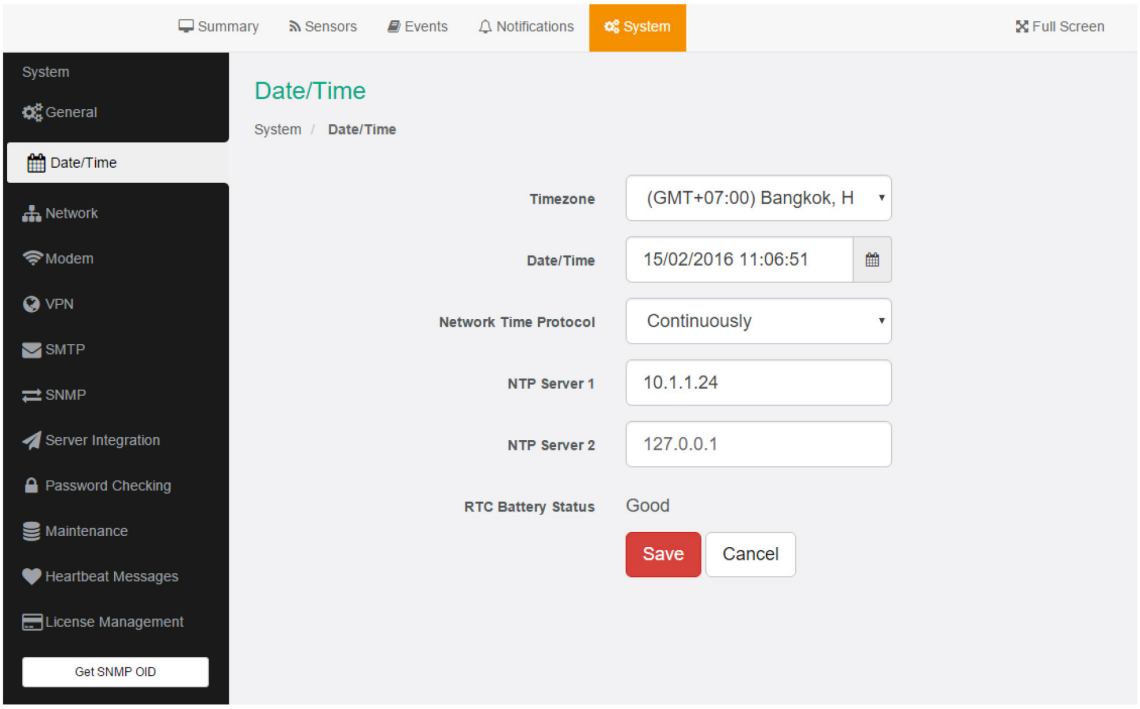

FIGURE 4-23. DATE/TIME OPTION

The system date and time with time zone is user configurable, with NTP server synchronization. If the unit is connected to EMEMS, then it will sync with the NTP service. Also displayed is the status of the battery (good/bad).

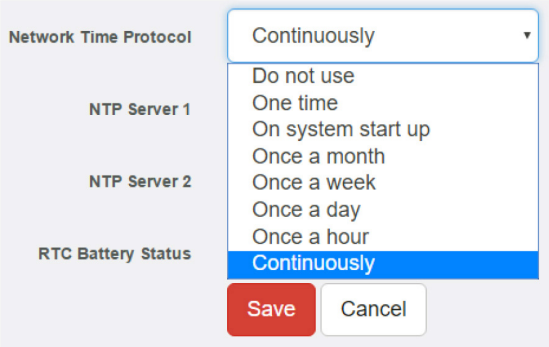

FIGURE 4-24. NTP DROP-DOWN MENU

You can also select the frequency of NTP synchronization with the drop-down menu.

4.2.4 NETWORK

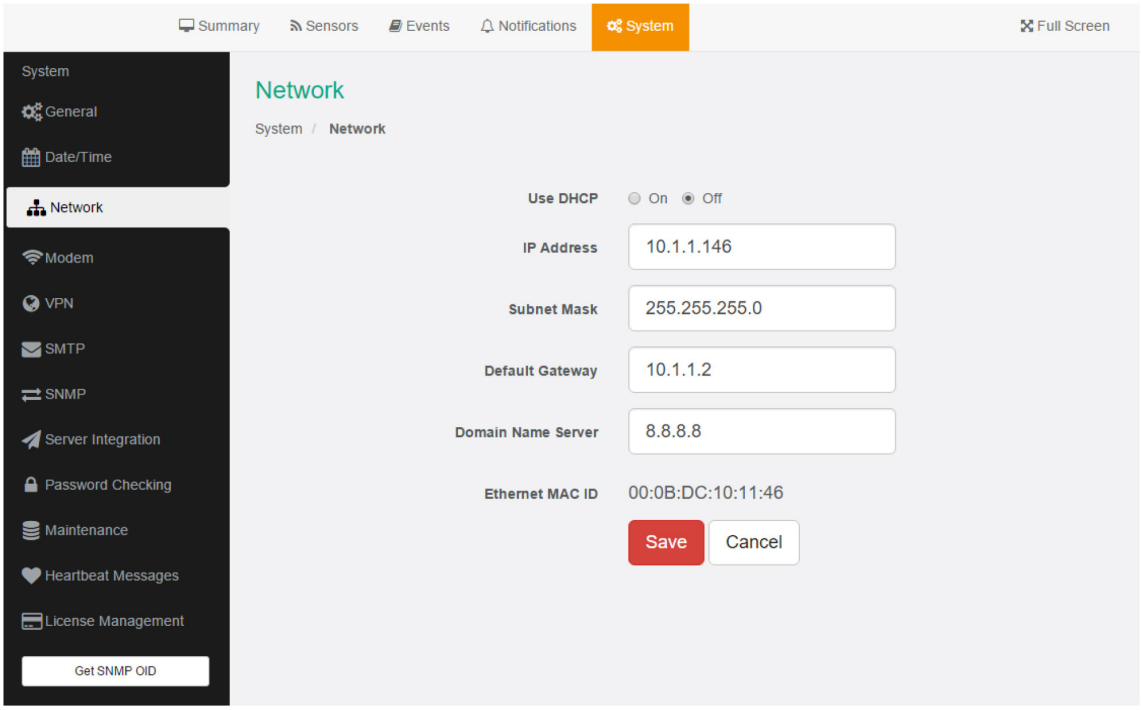

FIGURE 4-25. NETWORK OPTION

The unit's MAC ID is displayed here, and all user configurable options for IPv4 with fixed IP or DHCP client mode.

4.2.5 VPN

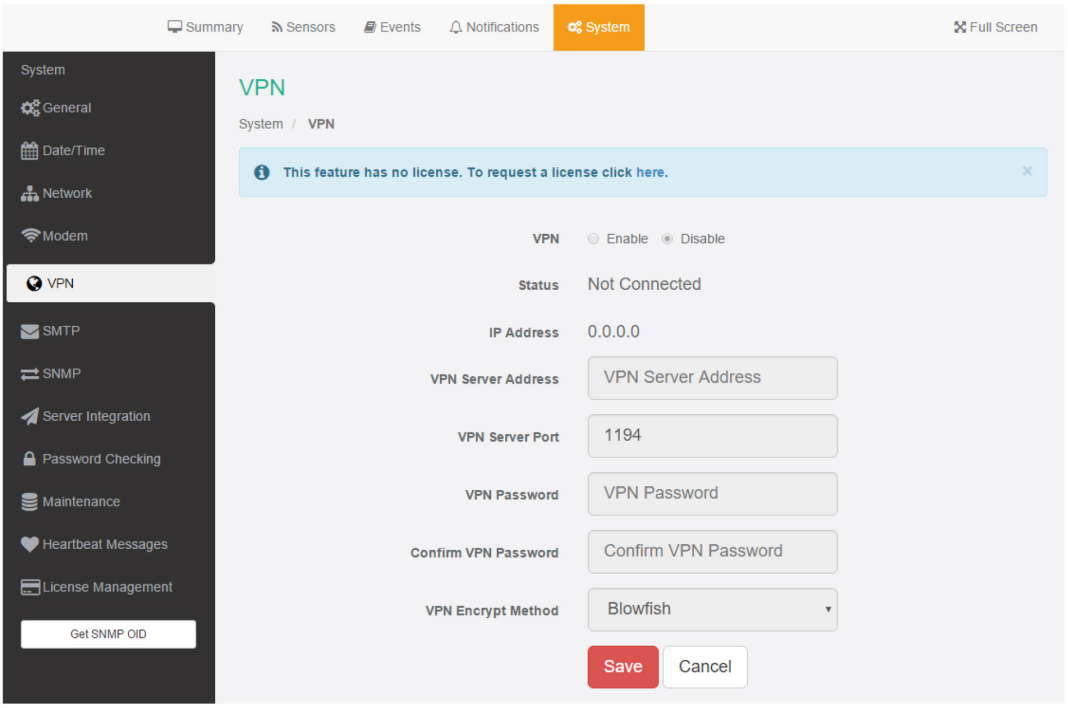

FIGURE 4-26. VPN SCREEN

This feature requires a separate license. You can read more details about the licensing later in this manual.

This feature is used by connecting the AlertWerks Gateway to the VPN server. After the license has been activated and the VPN server is set up, you'll need to fill out the same options here to be able to use the VPN connection.

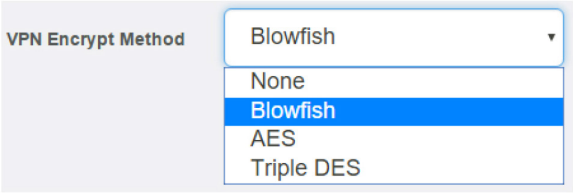

FIGURE 4-27. VPM ENCRYPT METHOD DROP-DOWN MENU

NOTE: You can also configure these settings from the console for the unit.

NOTE: If you use the VPN option, the maximum number of sensors that can be used by the unit will be reduced to 50.

4.2.6 SMTP

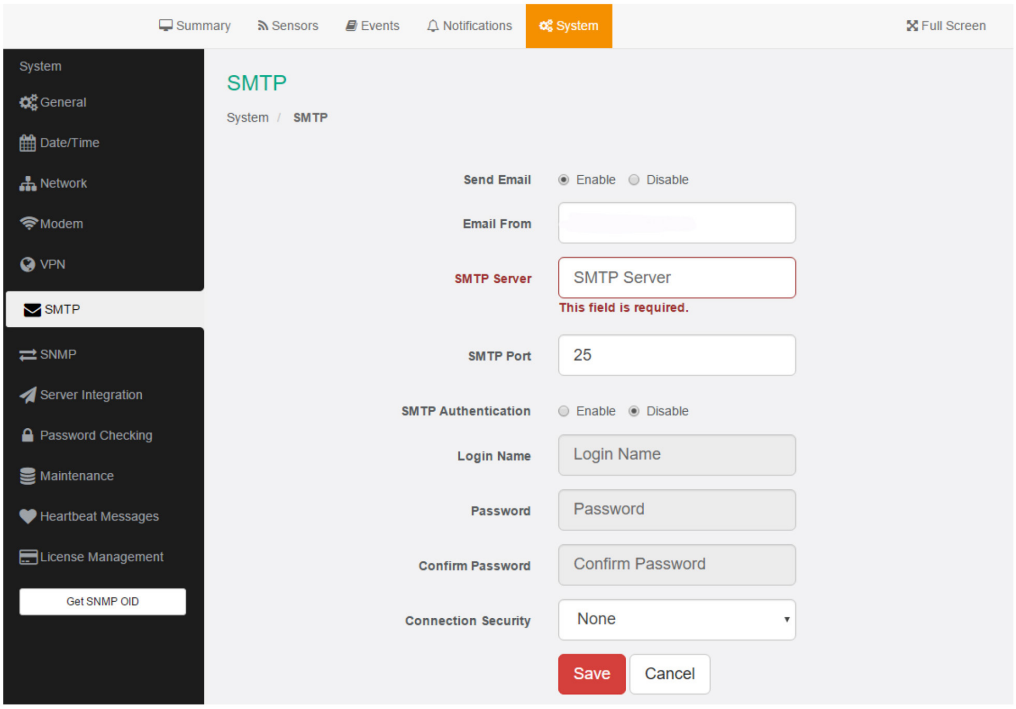

FIGURE 4-28. SMTP SCREEN

The SMTP server configuration options are shown here; it's required to be set up for the Email actions.

Fill out all parameters; the address in the Email From parameter will be used by the Email actions by default, but you could change it if your mail server supports it (when it's not required to match the SMTP user for example).

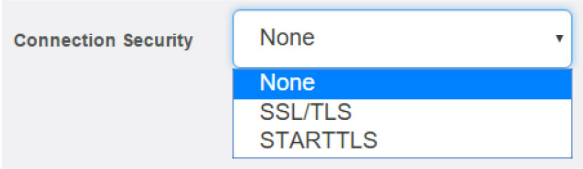

FIGURE 4-29. CONNECTION SECURITY DROP-DOWN MENU

SSL/TLS and STARTTLS are supported for the connection security.

You could also turn off any email sending from the unit by disabling the Send Email option.

4.2.7 SNMP

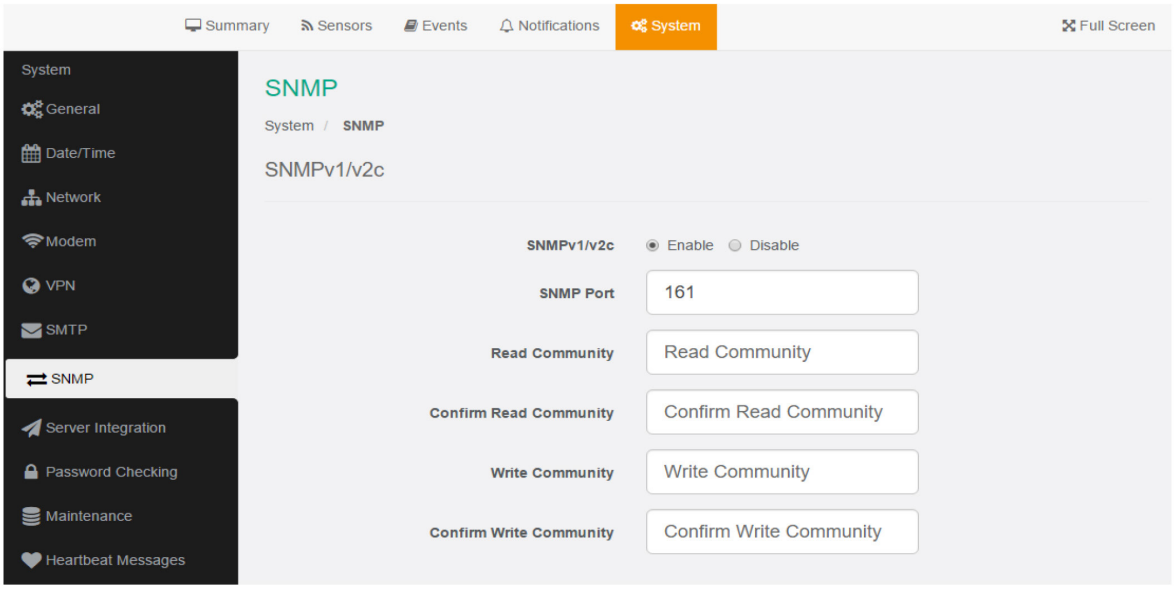

FIGURE 4-30. SNMP PAGE

The SNMP service configuration options are shown here; it is required for SNMP operations.

SNMPv1 is enabled by default, with community password “public”.

Scroll down for SNMPv3 options.

4.2.8 SNMPV3

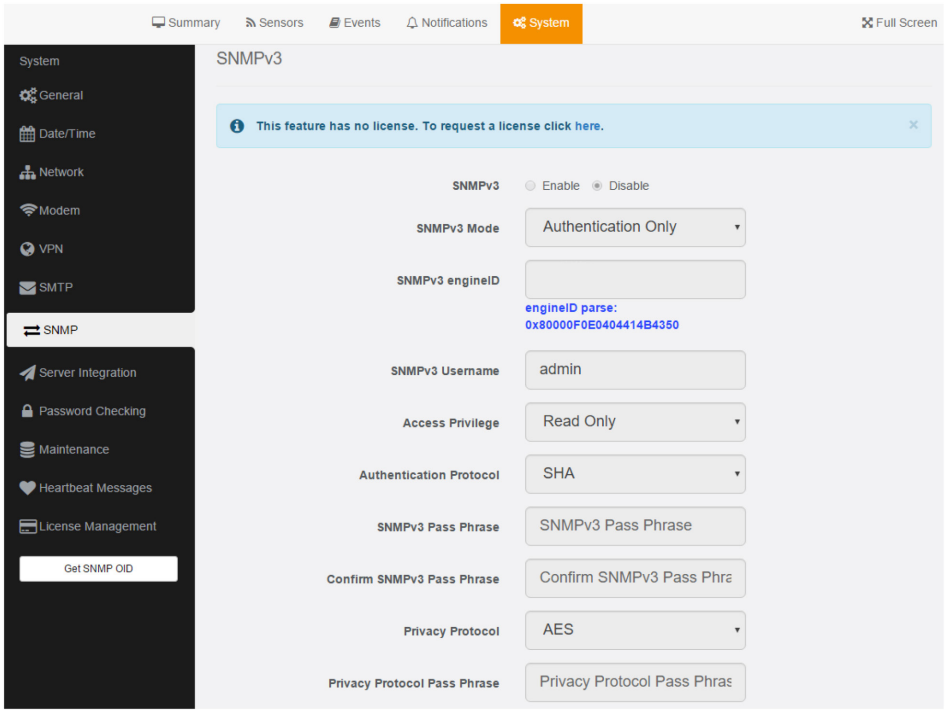

FIGURE 4-31. SNMP PAGE

The SNMPv3 options can be found by scrolling down on the SNMP page.

This feature requires a separate license. You can read more details about the licensing in this manual.

The table below shows a quick description of each setting.

TABLE 4-1. SNMPV3 OPTIONS

LEVEL	AUTHENTICATION	ENCRYPTION	DESCRIPTION
No Authentication (same as SNMP v1/v2c)	Username	No	Match Username
Authentication Only Algorithms (check password)	MD5 or SHA	No	Auth Based on
Auth & Privacy	MD5 or SHA	Yes - DES	Auth Algorithms and Encryption

Basically, if you select No Authentication, then the setup will be the same as with SNMP v1 and v2c versions: authentication is only checked by unencrypted username.

Authentication Only will provide password protection but no encryption.

Authentication & Privacy provides encrypted username and password protection.

4.2.9 SERVER INTEGRATION

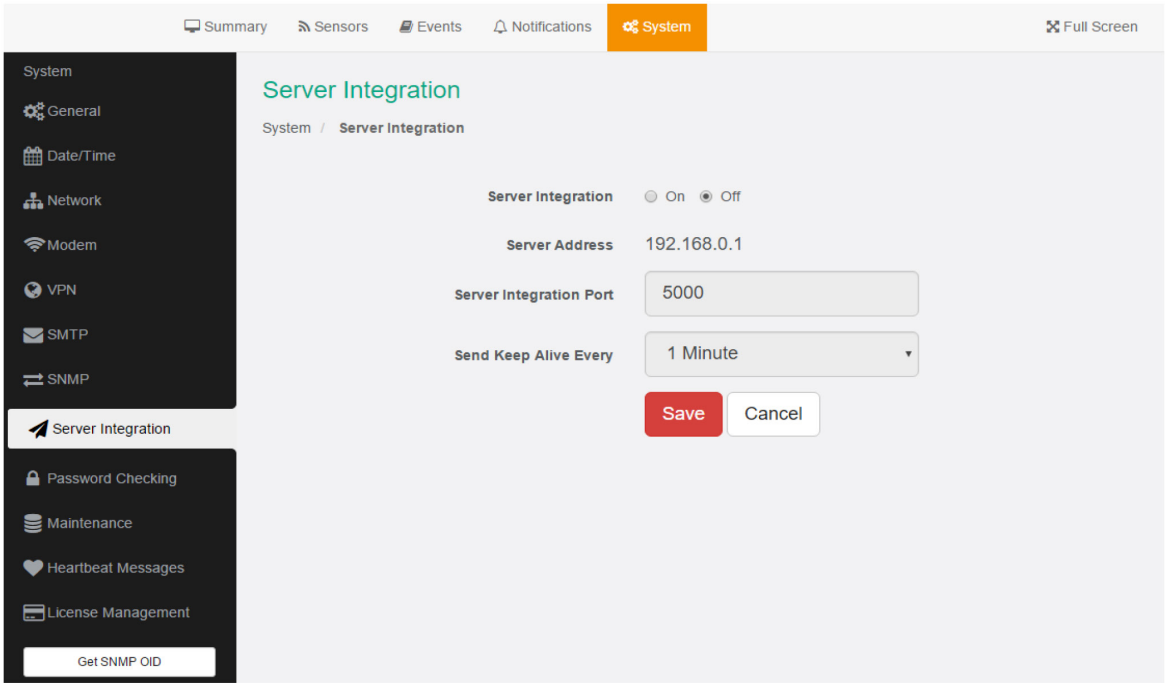

FIGURE 4-32. SERVER INTEGRATION SCREEN

If the unit has been added to the EMEMS console, the server's IP address will be displayed here. User configurable options are the APS port and keep-alive period.

You can change the APS port from the Web UI when the server's port changes.

Alternatively you can re-initialize your unit from the APS console to re-establish communication.

4.2.10 SERVICES

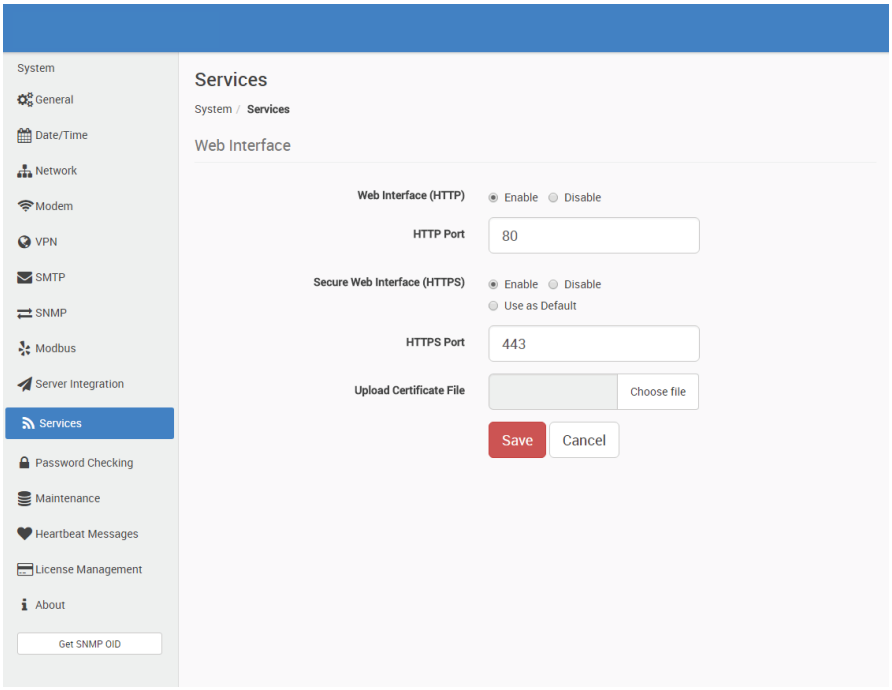

FIGURE 4-33. SERVICES SCREEN

You can close or change the ports used to access the unit's web interface, disable HTTP and enable HTTPS only, which can also be set to be used as default.

On the AlertWerks Gateway, the HTTPS supports TLS v1.1 and v1.2.

The HTTPS cypher suites are not customizable.

Using the "Upload Certificate File" option you can upload an SSL certificate that will be used by the unit's Web UI for HTTPS connection.

SSL Certificate

SSL certificates are generated for DNS host names and not IP addresses. You should set a host name for the AlertWerks Gateway unit in your local DNS server or DHCP server, and then generate the SSL certificate for that host name.

Example: spplus.mycompany.org

The unit's DNS host name is "spplus". Wildcard SSL certificates should also work, but this hasn't been tested.

If the name doesn't match with the one in the certificate, the browser will still show a security warning.

You can purchase a certificate from a trusted, verified Certificate Authority such as GoDaddy or use your company's own CA if you have one.

Please note that only non-password protected certificate files are supported.

When you select the file for uploading, you'll get a warning if the file is not in .PEM format:

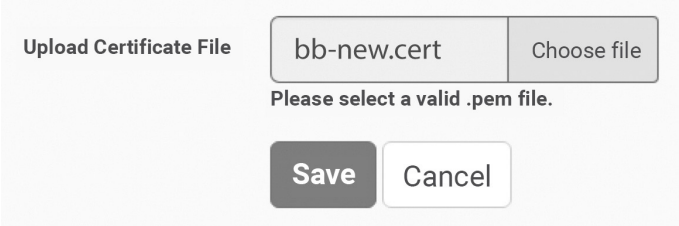

FIGURE 4-34. UPLOAD CERTIFICATE SCREEN

The .PEM file is the private key + certificate combined. You can copy them to one file using Notepad++ if you have 2 separate files, as shown next (it has to be in Unix Line Format and not Windows):

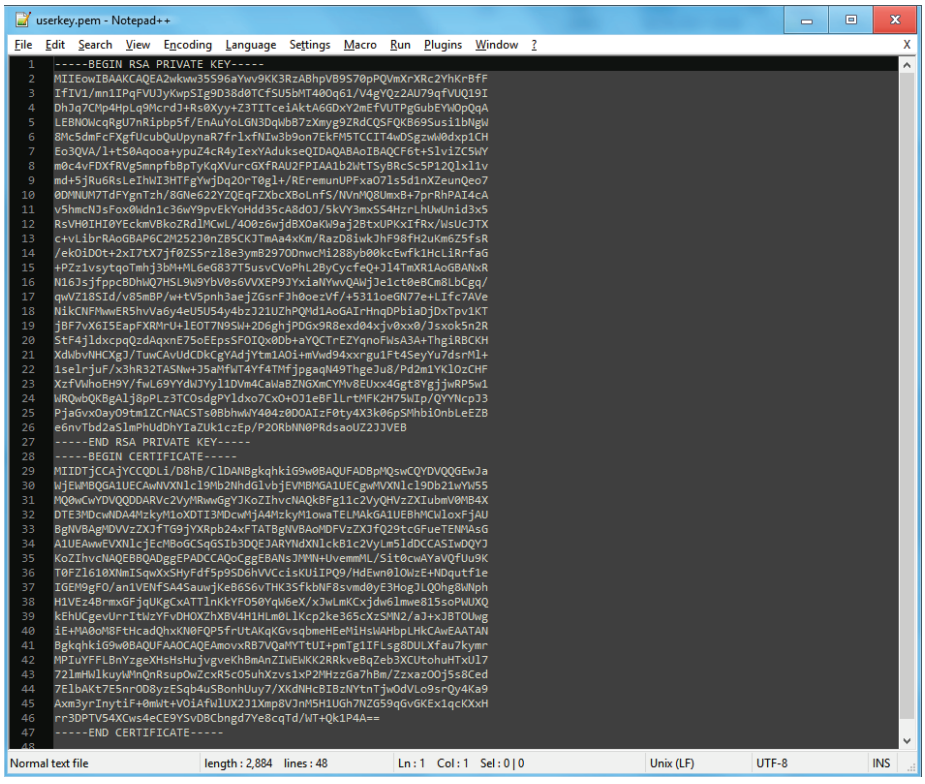

FIGURE 4-35. USERKEY.PEM SCREEN

If you don't upload a certificate but enable HTTPS, a built-in certificate will be used. You'll get a browser warning upon opening the Web UI about an incorrect certificate. This is normal and you should add it as an exception or proceed, depending on your browser:

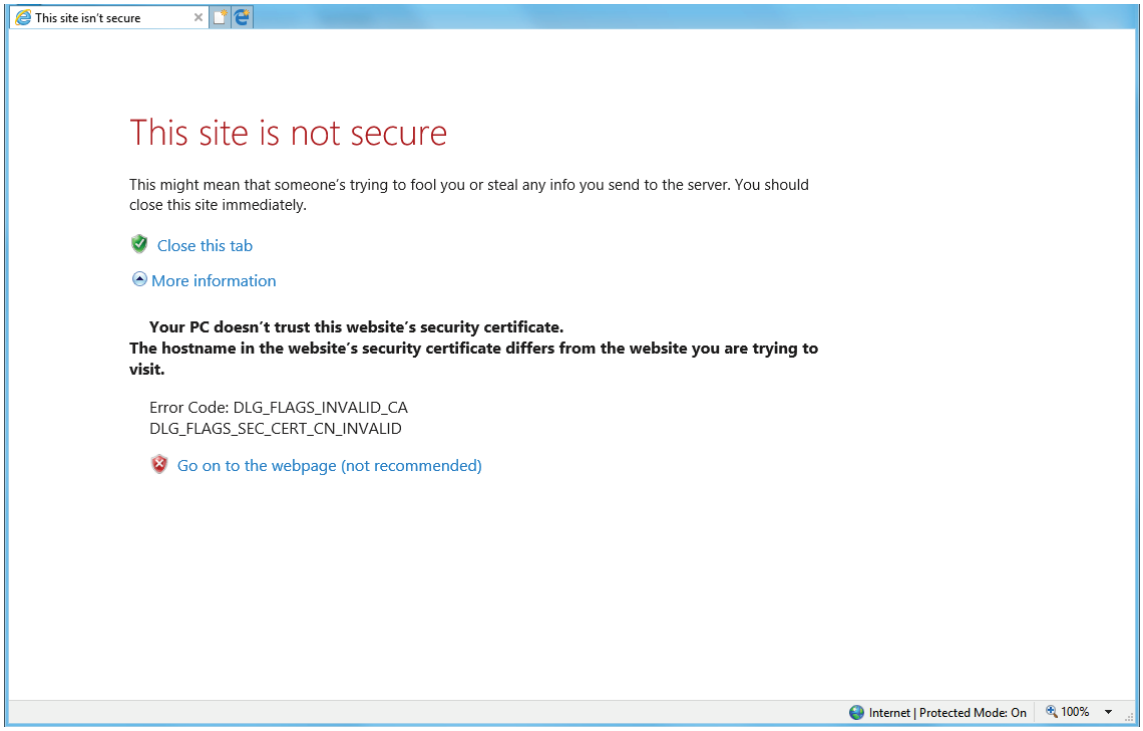

FIGURE 4-36. SITE NOT SECURE SCREEN

4.2.11 MODBUS

MODBUS RTU is a non-proprietary serial communications protocol that is widely used in the process control industry actuation. The AlertWerks Gateway can represent both “master” and “slave” devices and supports both Modbus RTU (RS-485) and Modbus TCP protocols.

The hub currently only supports Modbus with an RJ-45 connector (RTU and TCP) on its expansion port. For just Modbus, only pins 1 and 2 are used (Modbus A/+ and Modbus B/-). You cannot use other sensor ports for Modbus other than the expansion port.

IMPORTANT: When you use Modbus, you can’t connect expansion boards to the unit!

Standard can only use the Modbus Virtual Sensors.

NOTE: Modbus queries are slow (up to 3 seconds). This is per Modbus protocol definition, it’s not an AlertWerks Gateway limitation.
The more sensors you have, the bigger the polling interval must be.

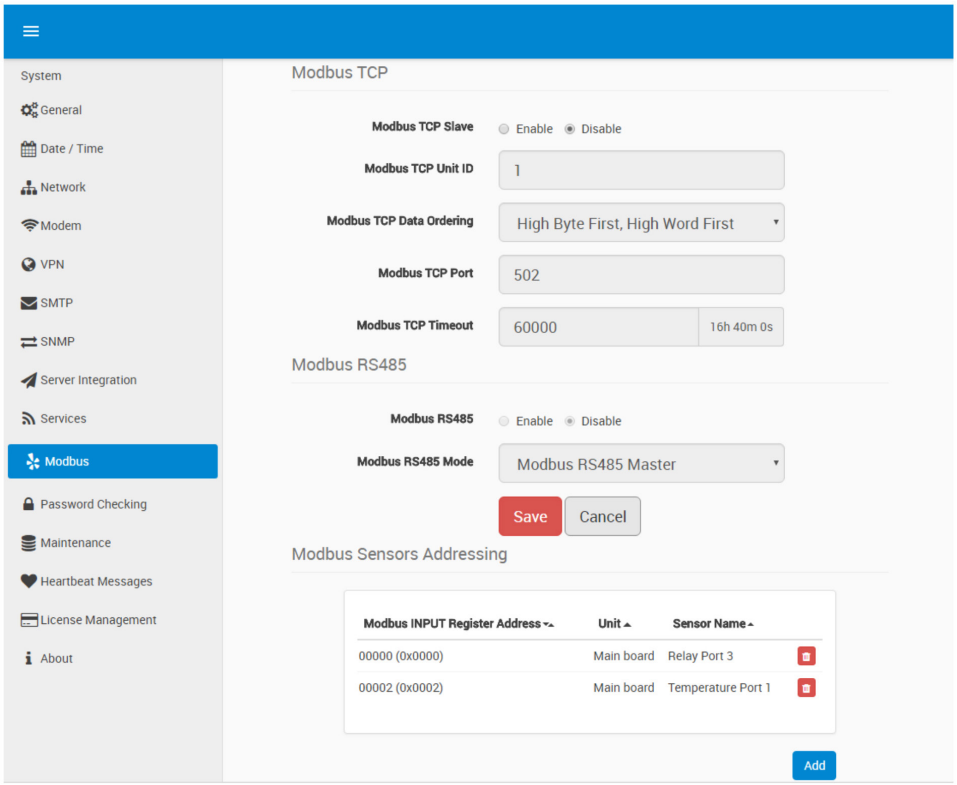

FIGURE 4-37. MODBUS TCP SCREEN

4.2.12 PASSWORD CHECKING

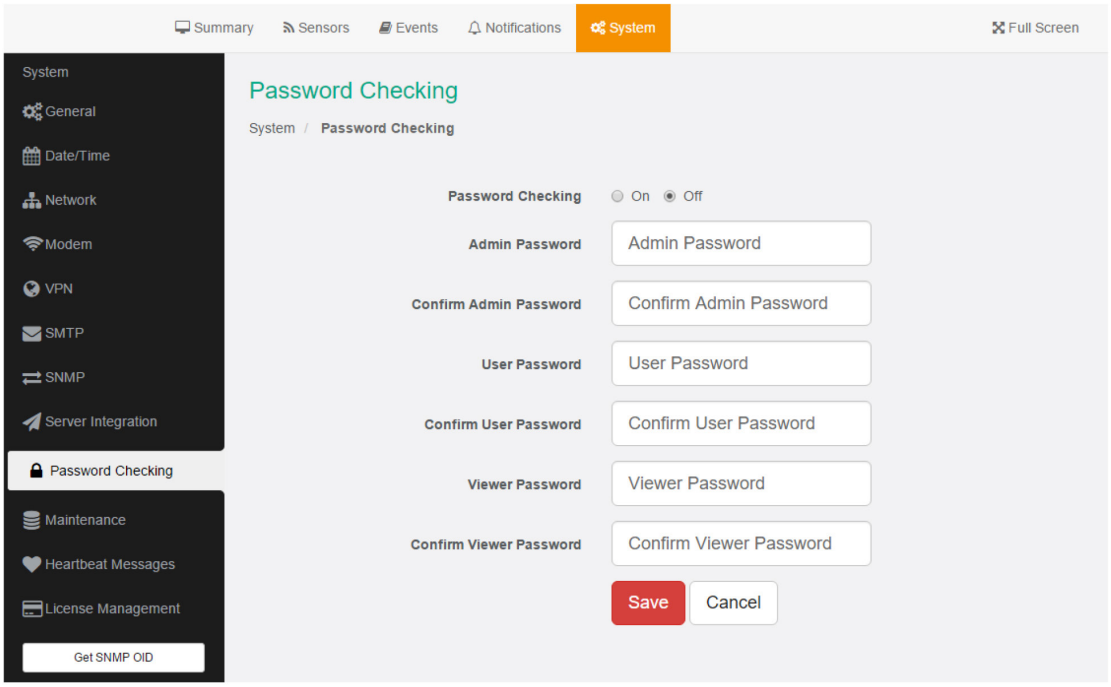

FIGURE 4-38. PASSWORD CHECKING SCREEN

Password checking for the Web UI can be turned on/off here, along with the option for specifying the password for the different user access levels.

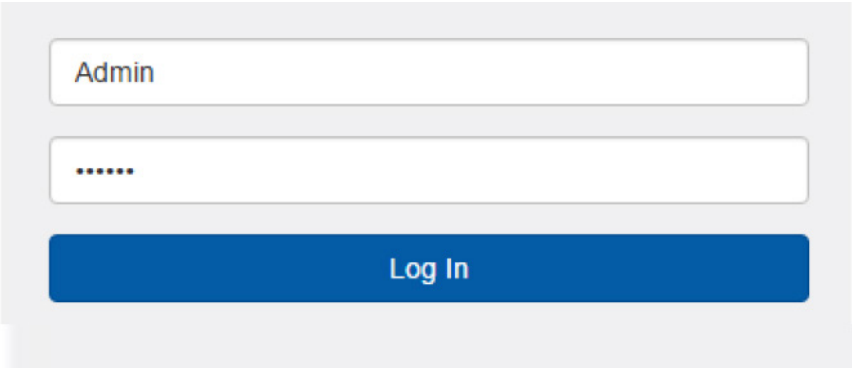

FIGURE 4-39. LOGIN SCREEN

After you enable the password checking, you'll need to re-login.

If you don't remember the admin password, you can hold the unit's reset button for 7-12 seconds to be able to log in to the Web UI without a password.

See below for details about permissions for the different user access levels.

NOTE: The passwords can only be set from the unit's Web UI; this option is not available from EMEMS.

NOTE: The default password is "public" for all access levels.

WEB UI USER ACCESS LEVELS AND PERMISSIONS

Admin - full access to all settings, system and notification configurations

Viewer - read-only guest access for every page

User - full access to most settings except for those which are the system-related such as network

In detail, the User access level provides these permissions in addition to the Viewer level:

- Allow modifying board/sensor settings
- Allow add/modify/remove notifications
- Allow add/modify/remove heartbeats
- Allow send configuration to Support
- Allow change Graph settings
- Allow change the Web UI language

4.2.13 MAINTENANCE

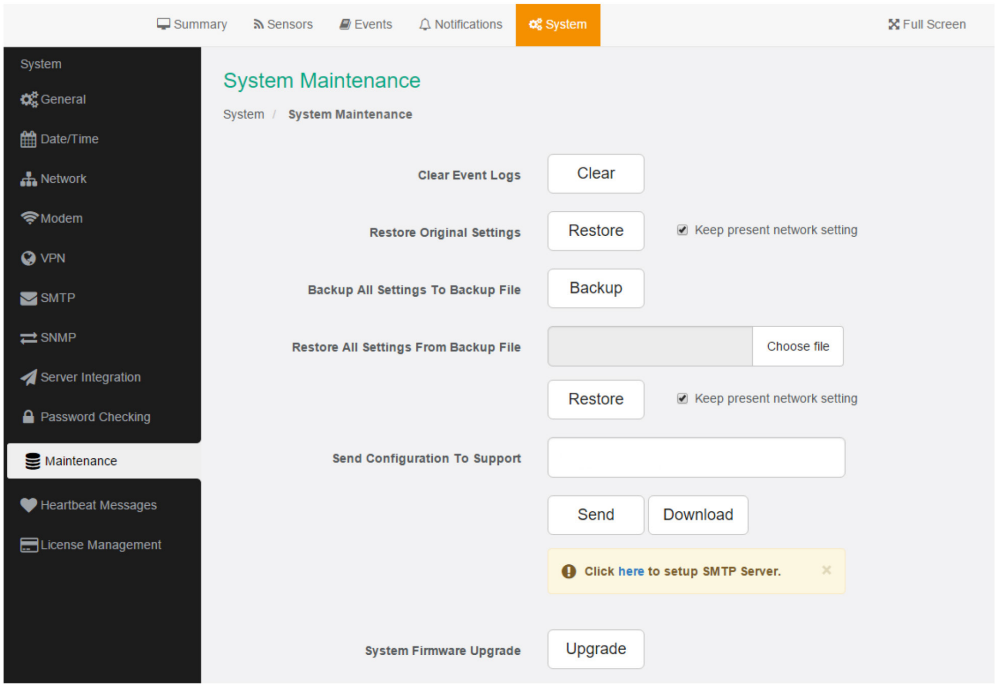

FIGURE 4-40. SERVER INTEGRATION SCREEN

On the System Maintenance page, the following options are available:

- Clear Event Logs: clears all logged events.
- Restore Original Settings: removes all customized settings and returns the unit to factory defaults—you can also choose to keep the network configuration intact.
- Backup/Restore All Settings: the unit's configuration can be backed up to a file and restored quickly and easily. You can choose to keep the present network settings, if the backup file is from another unit. The backup file contains all settings and notifications for the unit.
- Send Configuration To Support: when asked by Support, this sends the unit's backup file to us.
- System Firmware Upgrade: allows you to upgrade to the latest firmware of the unit—alternatively you could upgrade from EMEMS. We'll show you the process of the Web UI firmware upgrade in another section.

4.2.14 HEARTBEAT MESSAGES

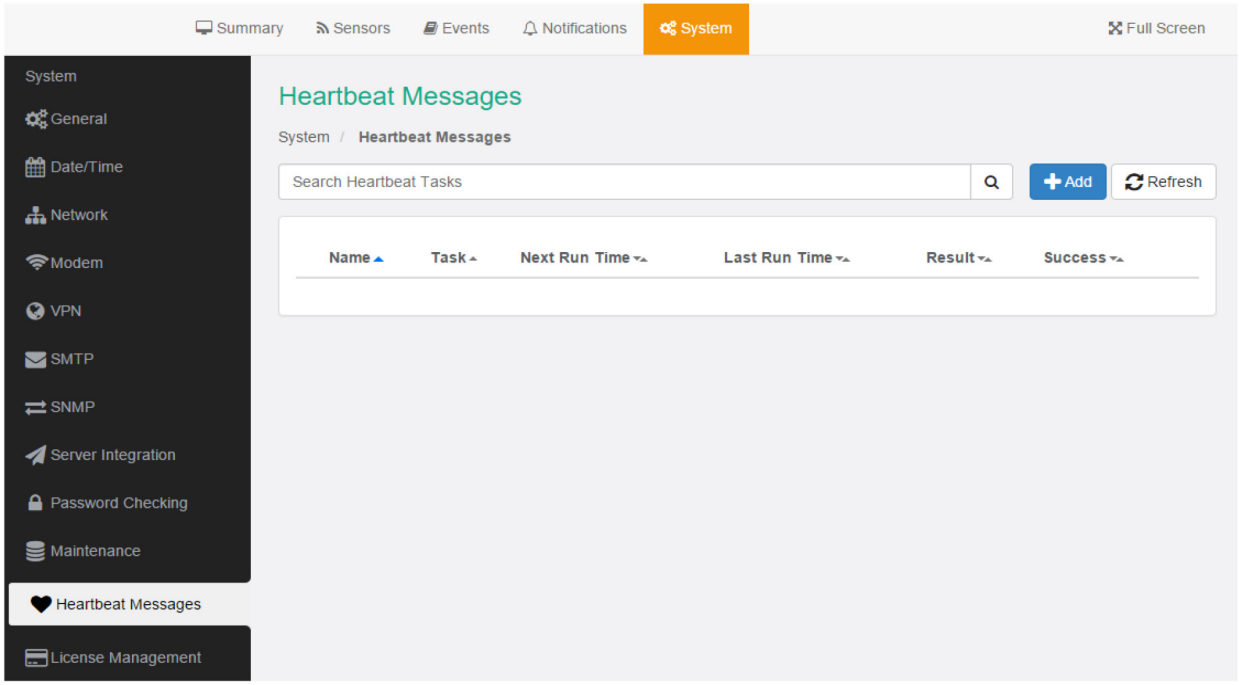

FIGURE 4-41. HEARTBEAT MESSAGES SCREEN

This feature allows you to set up periodical "keep alive" notifications task by email, SMS or SNMP Trap to indicate the unit is still working properly.

4.2.15 LICENSE MANAGEMENT

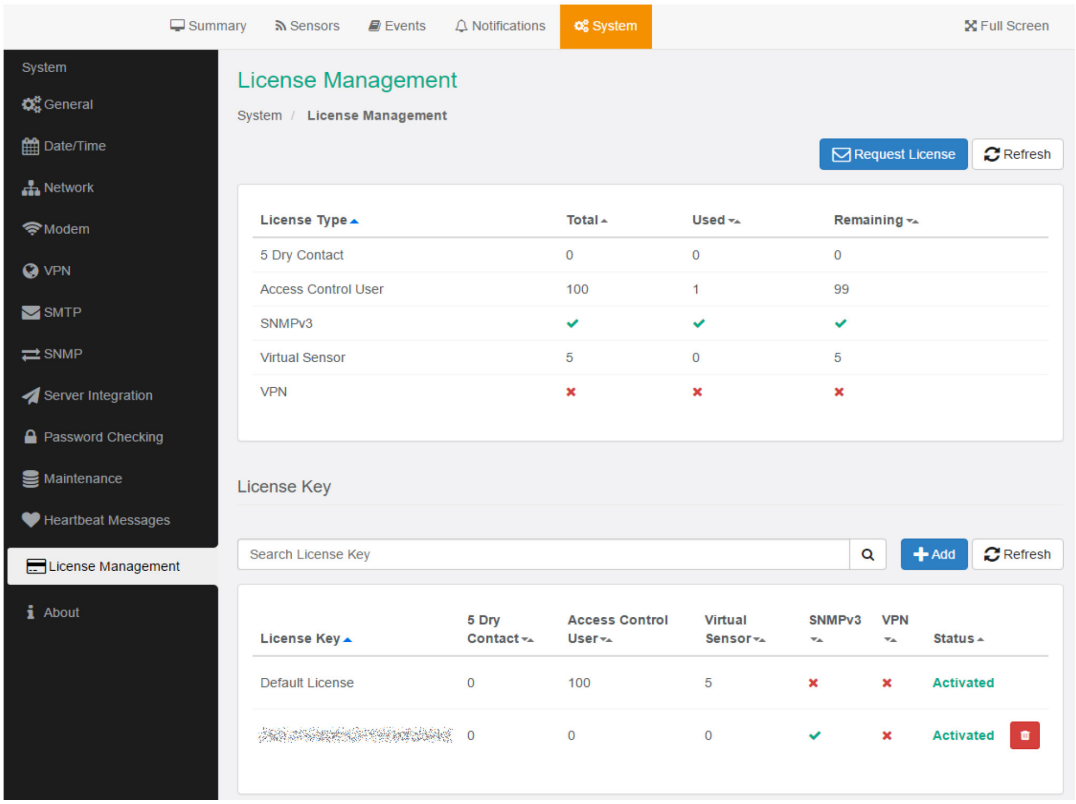

FIGURE 4-42. LICENSE MANAGEMENT SCREEN

Here you can manage the purchased licenses for specific features on the unit.

For example you can request SNMPv3 license by clicking on the Request License button.

This will send an email to our Sales team with your unit's MAC ID. You can then add the purchased license key with the Add button and activate this feature on the unit.

License keys can be backed up/restored with the backup file.

All keys are unique per device and per feature.

Features that needs separate licensing:

- SNMPv3 feature: Allows you to use and configure secure, authenticated SNMP trap messages.
- Virtual Sensors: Allows you to use and configure virtual sensors. The first 5 sensors are free, you can get more licenses in blocks of 5; the limit is 32.
- VPN feature: Currently the VPN integration is supported, to use a secure VPN channel between the unit and EMEMS.

NOTE: When using this option, the number of maximum sensors that can be used by the unit will be reduced to 50.

4.2.16 ABOUT

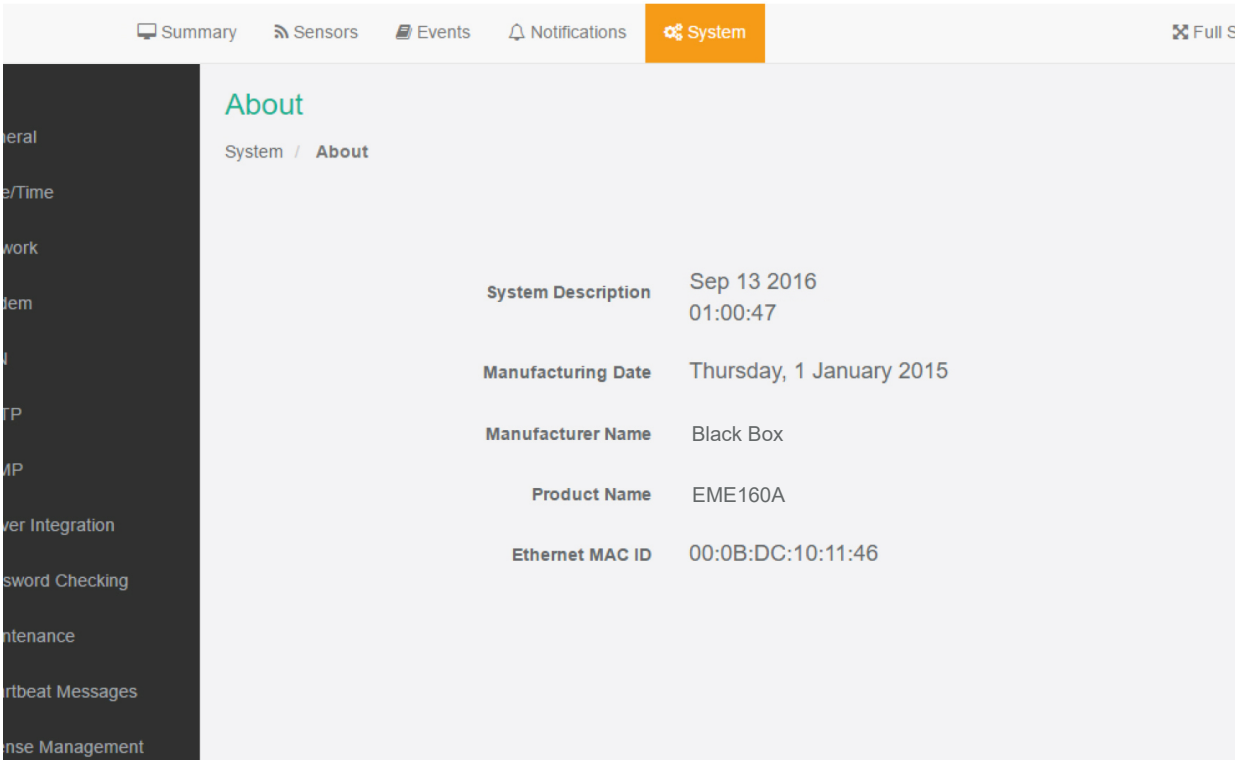

FIGURE 4-43. ABOUT SCREEN

This page shows information about the Manufacturing Date, Ethernet MAC ID, and System Description, which are important when you request support.

You could make a similar screenshot when you need help with your unit, as this information can help us diagnose the problem.

4.3 SENSORS PAGE

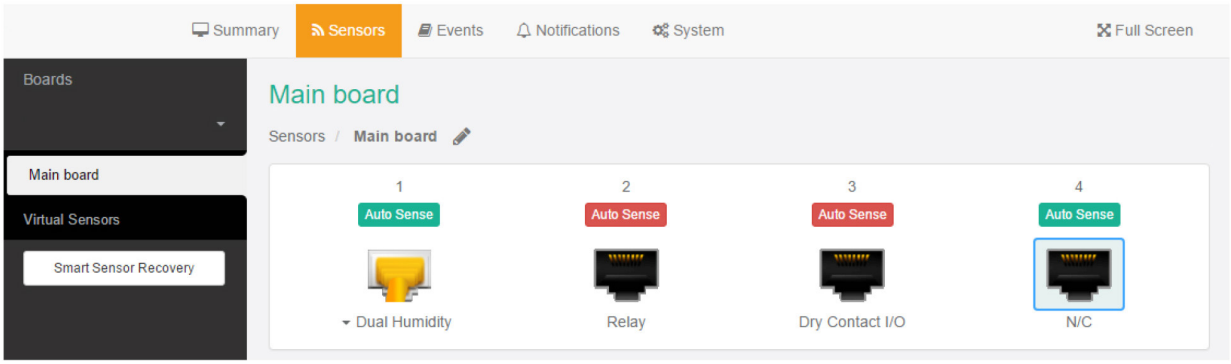

FIGURE 4-44. SENSORS PAGE

On this page, you can view all sensors connected to the unit per port.

Non-connected sensors will be also displayed, until you re-attach or manually remove them from the configuration.

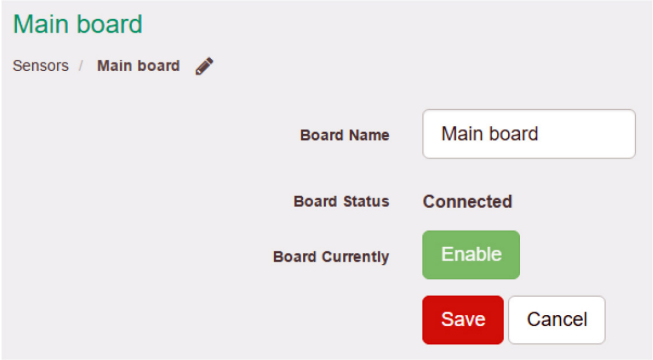

FIGURE 4-45. MAIN BOARD SCREEN

You could also rename the unit's Main board by clicking on the pencil icon.

NOTE: The maximum supported cable length to use with EME1TS/EME1THS:

- Maximum extension cable length from the AlertWerks Gateway sensor port to the EME1TS/EME1THS using CAT5 = 28 Feet
- Maximum extension cable length from the AlertWerks Gateway sensor port to the EME1TS/EME1THS using CAT5e & CAT6 = 60 Feet

CAUTION: If you're using analog pins on the sensor ports (with manually on-lined DCV sensors, and pin 7 of the RJ-45 connector) make sure that the voltage doesn't exceed 3 Volts. Otherwise, you can damage the unit!

4.4 GENERAL OPTIONS FOR ALL SENSORS

You can change the following general options for all sensors: Disable Auto Sense, Choose Sensor Type, Offline a Sensor and Smart Sensor Recovery.

4.4.1 DISABLE AUTO SENSE

FIGURE 4-46. AUTO SENSE BUTTON

Click on the Auto Sense button to turn off the automatic sensor detection for a port.

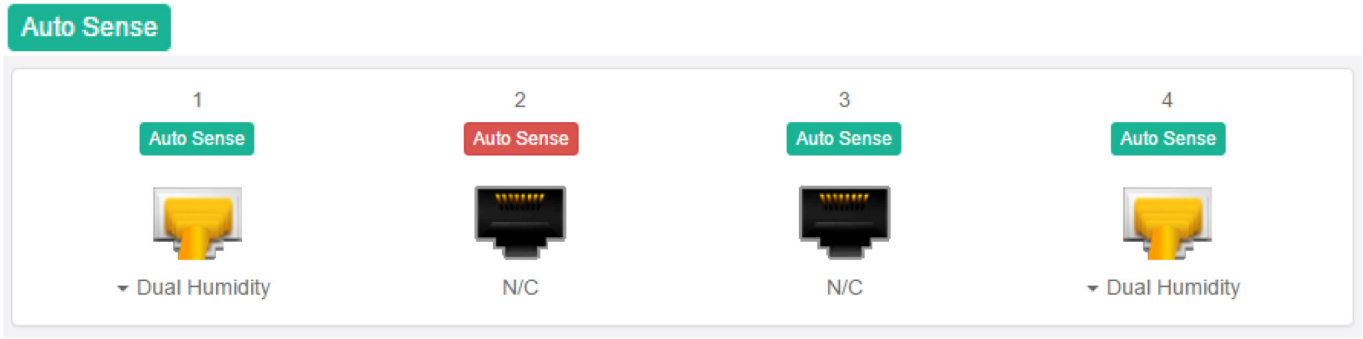

FIGURE 4-47. AUTO SENSE SCREEN

This feature is useful if you want to simulate a sensor (this works for Relay type sensors) or to prevent a sensor from going into offline state.

NOTE: The sensor will be in "sensor error" state if the unit can't get any reading from the sensor.

4.4.2 CHOOSE SENSOR TYPE

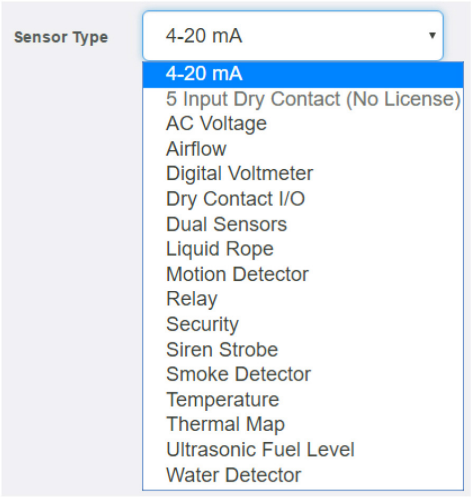

FIGURE 4-48. SENSOR TYPE DROP-DOWN MENU

You can pre-configure a specific sensor type if needed, for example if you put the sensor offline before.

4.4.3 OFFLINE A SENSOR

FIGURE 4-49. GREEN ONLINE BUTTON

You can manually offline any sensor by clicking on the green Online button on the sensor's configuration page.

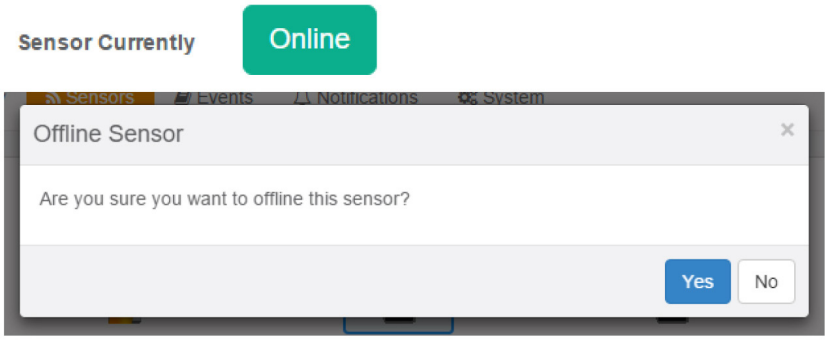

FIGURE 4-50. CONFIRMATION POPUP WINDOW

You'll be asked for confirmation in a popup window.

NOTE: if you change a sensor to offline, it will no longer be displayed on the web interface. To reactivate it, you have to toggle it back to online.

4.4.4 SMART SENSOR RECOVERY

FIGURE 4-51. SMART SENSOR RECOVERY BUTTON

This feature will be used only for the new Smart Sensor type. The firmware can be updated on these sensors automatically, and if the upgrade has failed for some reason and the sensor becomes unresponsive, with this option you can recover them to the default firmware. It's not used by other sensor types.

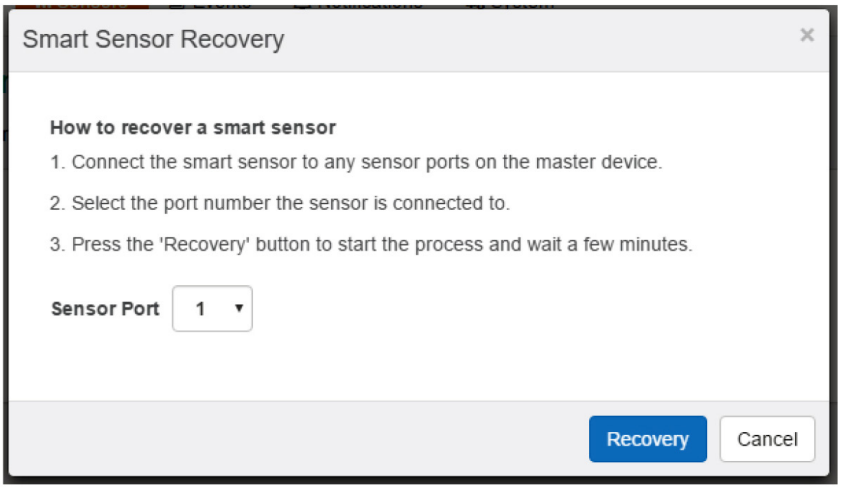

FIGURE 4-52. SMART SENSOR RECOVERY SCREEN

NOTE: If there's a difference between the version stored in the unit's firmware and the sensor's firmware, it will upgrade/downgrade the sensor's firmware upon powering up/reboot of the unit, or on sensor reconnection.

If you need to downgrade the smart sensor firmware, you can only do so together with the unit's firmware.

4.4.5 CHANGE CONTINUOUS TIME

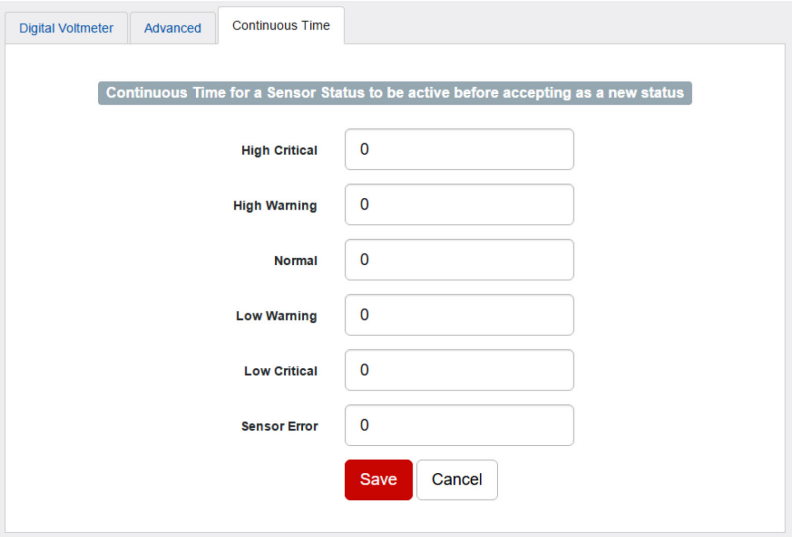

FIGURE 4-53. CONTINUOUS TIME SCREEN

The following advanced functions are for setting the time frame in which the system should delay a notification being triggered when a sensor gives a reading that exceeds the thresholds (high warning, normal, etc).

- Continuous Time to Report High Critical: This helps to eliminate unnecessary messages during minor fluctuations. You can set the amount of time to delay a notification of a status change from high warning to high critical. Enter the time in seconds and press the "Save" button. The amount of time that can be entered is between 0 and 65535 seconds, which equals approximately 18 hours.
- Continuous Time to Report High Warning: As above, but delays notification for "High Warning".
- Continuous Time to Report for Normal: As above, but delays notification for return to "Normal" state.
- Continuous Time to Report for Low Warning: As above, but delays notification for "Low Warning" state.
- Continuous Time to Report for Low Critical: As above, but delays notification for "Low Critical" state.
- Continuous Time to Report for Sensor Error: As above, but delays notification being sent for sensor going into an error state.

Example: An airflow sensor or humidity sensor may have temporary drops in readings that are normal operating characteristics; a logical time limit is set to show abnormal conditions.

4.5 VIRTUAL SENSORS

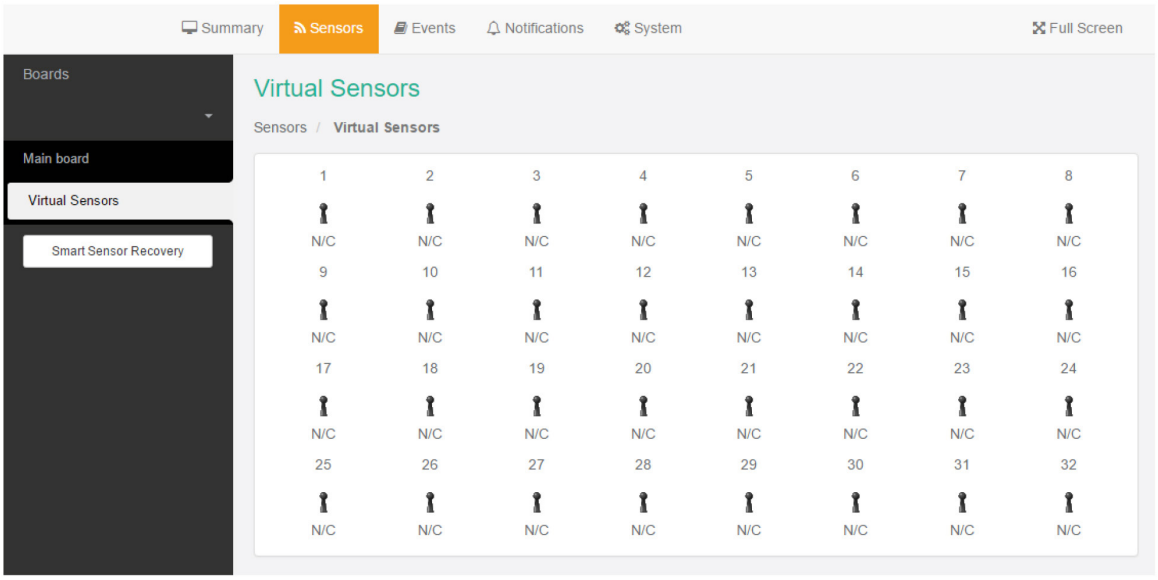

FIGURE 4-54. VIRTUAL SENSORS SCREEN

On this page, you can configure the Virtual Sensors. The first 5 sensors are free, if you need to use more you can purchase additional licenses (see the Licensing section in this manual).

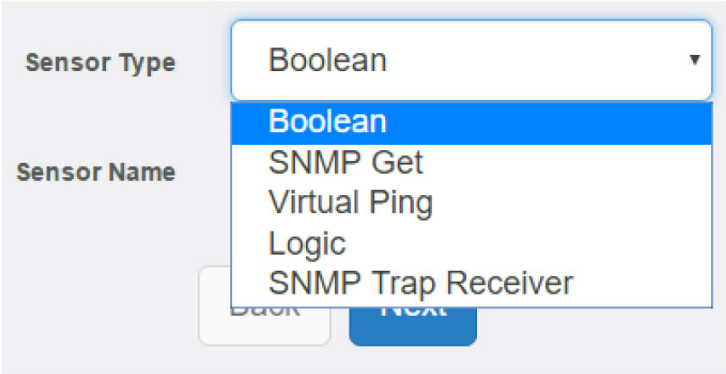

FIGURE 4-55. SENSOR TYPE DROP-DOWN MENU

Virtual Sensors can be a very powerful tool in your monitoring system. On the AlertWerks Gateway, you can have up to 32 of these virtual sensors and they allow for a multitude of applications.

SNMP Get, sensor logic evaluation and ping commands among others are all possible from the virtual sensors. An example use of this could be to perform a SNMP Get command on a server to monitor memory, CPU load, or temperature. You can also ping network enabled devices and be alerted if they go offline.

4.6 EXAMPLE SENSOR CONFIGURATION

Below we'll show the configuration of 2 sensor types: the Temperature/Humidity and a Relay sensor.

The configuration of these 2 types of sensors covers most settings that can be configured for other sensor types.

4.6.1 TEMPERATURE/HUMIDITY SENSOR

Click on the sensor port where the sensor is connected to open the sensor's configuration.

NOTE: Another way of accessing this page is to click on the sensor from the Summary page.

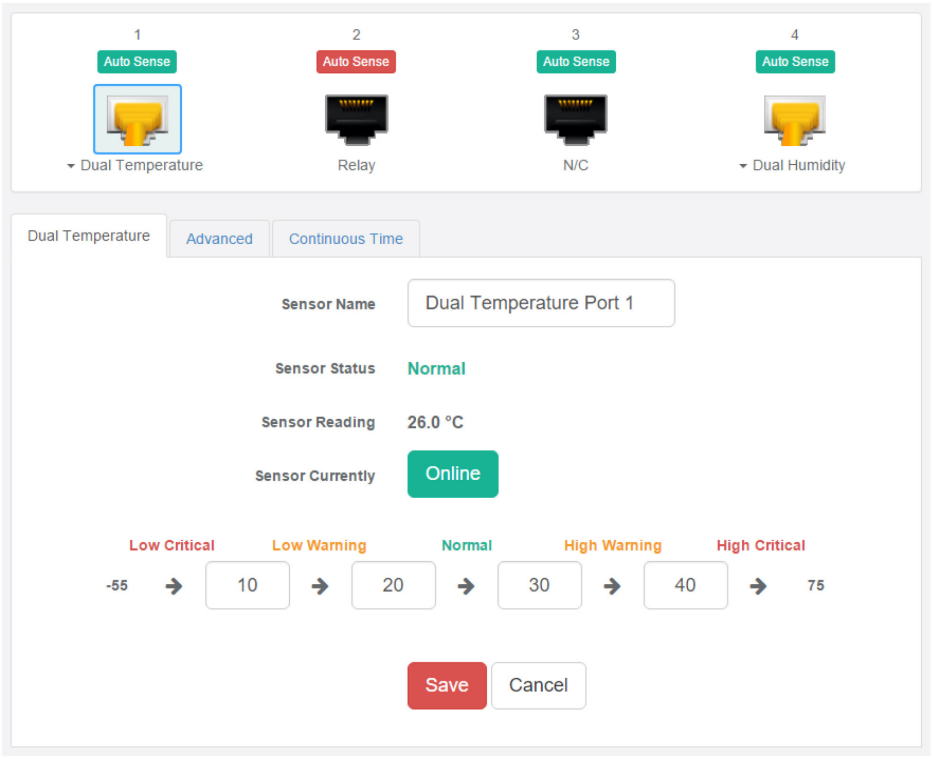

FIGURE 4-56. SENSOR'S CONFIGURATION SCREEN

From this page you can carry out various operations. You can view the current status (normal, low critical, high critical etc), rename the sensor, put it offline and change the thresholds. In the screen shot above you can see the sensor is indicating a temperature of 26 degrees ˚C, and a status of Normal.

You can re-configure the thresholds for each sensor state. After changing a threshold value, click Save. In the next screen shot, you can see that a threshold has been changed to 27 make a new "low warning" state, and along with it the sensor status has changed.

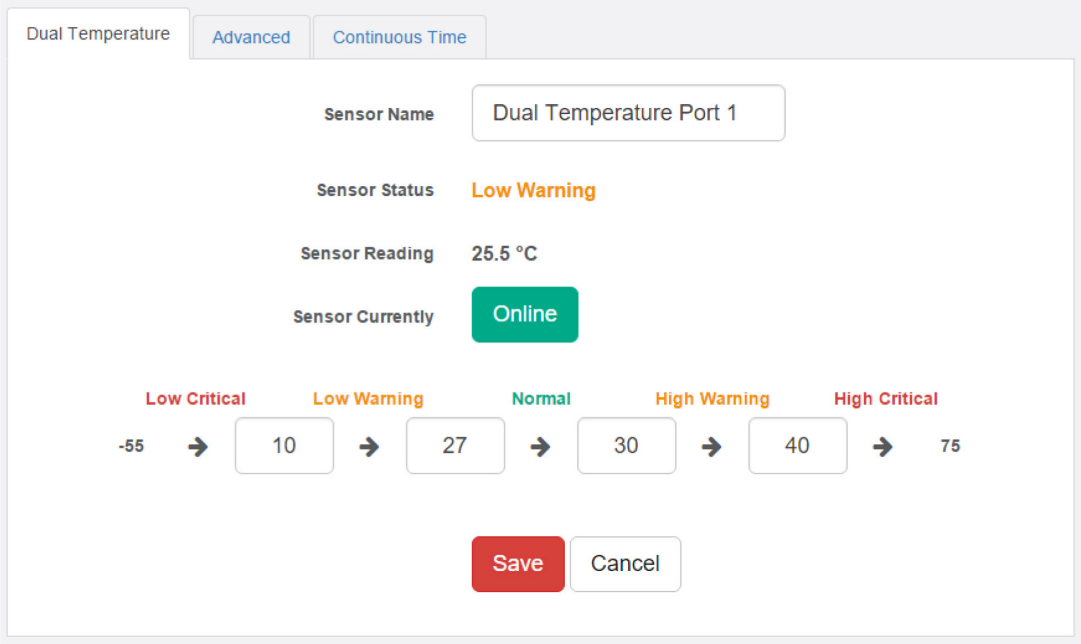

FIGURE 4-57. SENSOR STATE CHANGED SCREEN

NOTE: the Humidity sensor has the same configuration options as the Temperature sensor.

ADVANCED SENSOR CONFIGURATION FOR TEMPERATURE/HUMIDITY SENSORS

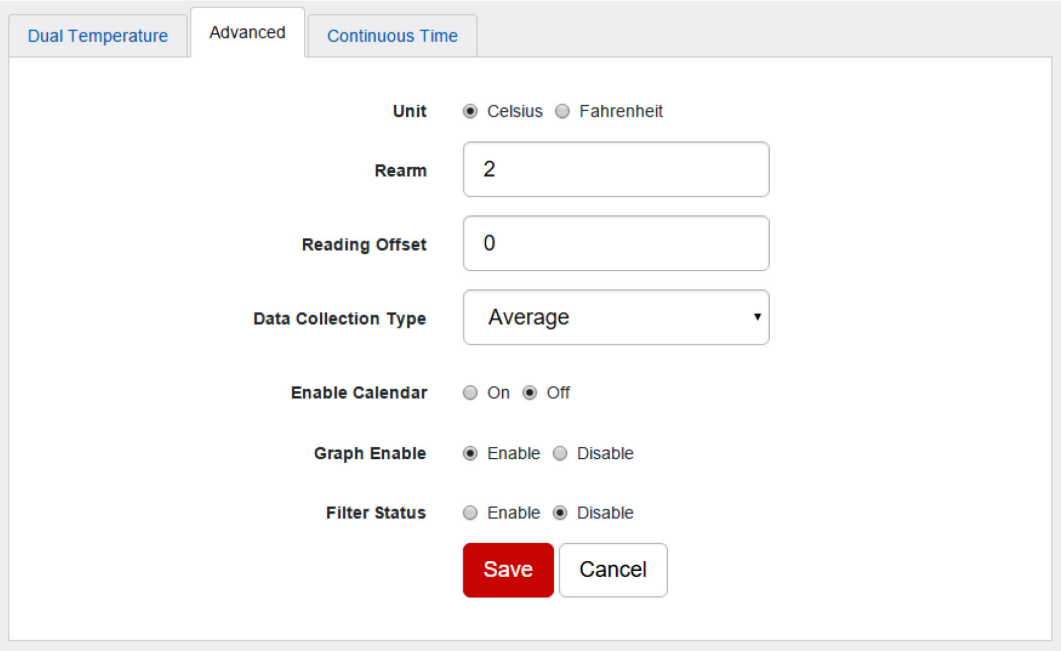

FIGURE 4-58. ADVANCED SENSOR CONFIGURATION SCREEN

Fields in above screen:

- Units: Changes units from ˚C to ˚F or vice versa.
- Rearm: The Rearm parameter is useful for sensors whose values can vary, such as the temperature and humidity sensors.

  It is used to prevent the sensor from rapidly changing between two states. For example if the Warning High threshold for the temperature sensor is set to 80 degrees and the sensor were to vary between 79 and 80 you could be faced with a very large number of emails, traps, and events logged. The Rearm parameter prevents this by forcing the temperature to drop by the Rearm value before changing the state back to normal. In this example, if Rearm is set to 2, then the sensor would have to drop from 80 down to 77 before the status would change from Warning High back to normal.

- Reading Offset: The Reading Offset feature is a calibration tool. If you wish to calibrate the temperature sensor, for example, you could enter an offset value of 5. This would mean if the sensor reads 20 degrees then it would record as 25 degrees. This figure can also be a minus figure (e.g. -5 would show 15 degrees instead of 20).

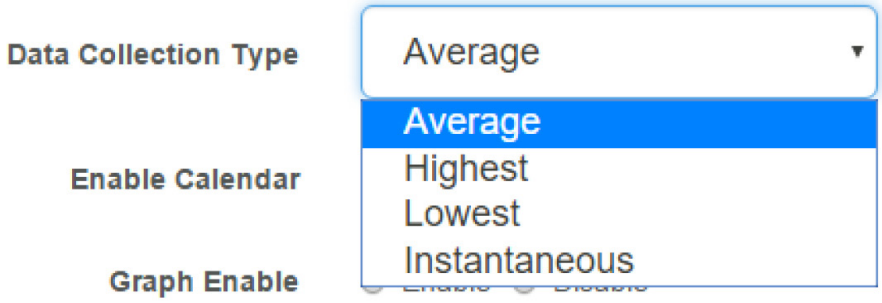

FIGURE 4-59. DATA COLLECTION TYPE DROP-DOWN MENU

Data Collection Type: This refers to the data collection from the sensor and how the data is then displayed on the graphs.

There are four options for the collection of data: Average, Highest, Lowest and Instantaneous. The default setting is Average.

- When the data collection type is set to Average, the averaged value between 2 graph intervals is stored and output graphs for the daily, monthly, and yearly all have the same size on the screen. For the daily graph, each data point on the graph is one data point collected from the sensor. But for the monthly and yearly graph, to display more data into the same size as the daily graph, some consolidation on the data is needed. One data point on the monthly and yearly graph is an average of the sensor data in a range.

  The maximum and minimum values showing on the monthly and yearly graphs are the value of this consolidated data and not the raw data over that period of that time.

- When the Data Collection Type is set to the Highest setting, then you will get the graphing output displaying the sensors highest average readings during sampling. This is the same for the Lowest setting (lowest average).
- With the Instantaneous setting, you can store the actual value of the sensor at the sampling interval without averaging.
- Graph Enable: To save the data from the sensors on the unit, you will need to enable the Graphing feature on the unit. You need to change the Enable Graph to the On position and click on the Save button to enable the graphing.

NOTE: You can also enable the graphing from the Summary page.

- Filter Status: The Sensor Filter Status is a feature that you can Enable or Disable and when enabled will check the sensor status. If the status of the sensor changes very rapidly, then it will report how many times the sensor status changed, instead of having multiple separate entries in the syslog.

  When enabled, this will report the changes and status of a sensor only once.

4.6.2 RELAY SENSOR

Click on the sensor port where the sensor is connected to open the sensor's configuration.

NOTE: Another way of accessing this page is to click on the sensor from the Summary page.

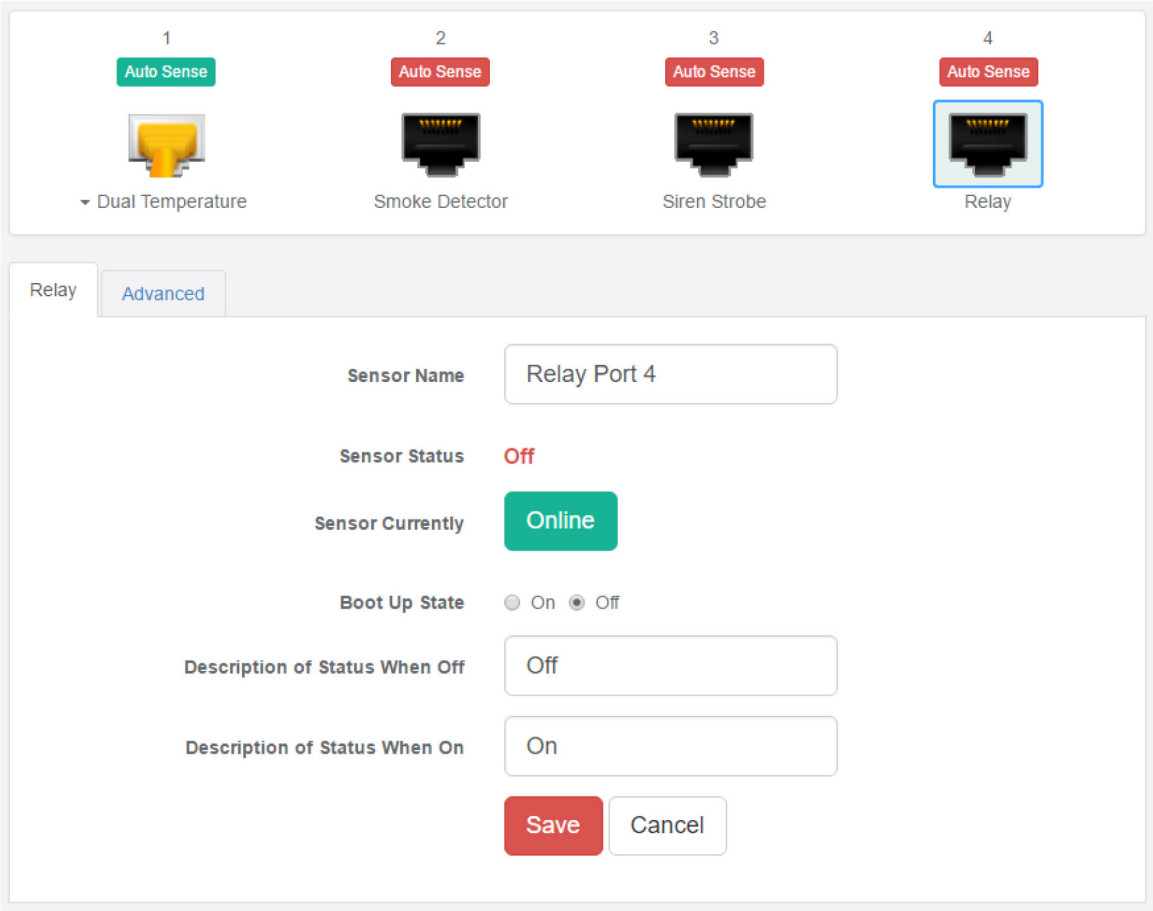

FIGURE 4-60. RELAY SENSOR SCREEN

- Boot Up State: You can change the state of the relay when the unit starts. The default is Off.
- Description of Status When Relay Off: This field is the custom description, which will be displayed in the Relay Status field when the relay state is off. The same text is listed as one of the relay actions used to turn off the relay. Examples for this field are Close Door, Turn Pump Off, Turn Light Off, etc.
- Description of Status When Relay On: This field is the custom description, which will be displayed in the Relay Status field when the relay state is on. The same text is listed as one of the relay actions used to turn on the relay. Examples for this field are Open Door, Turn Pump On, Turn Light On, etc.

ADVANCED SENSOR CONFIGURATION FOR RELAY SENSORS

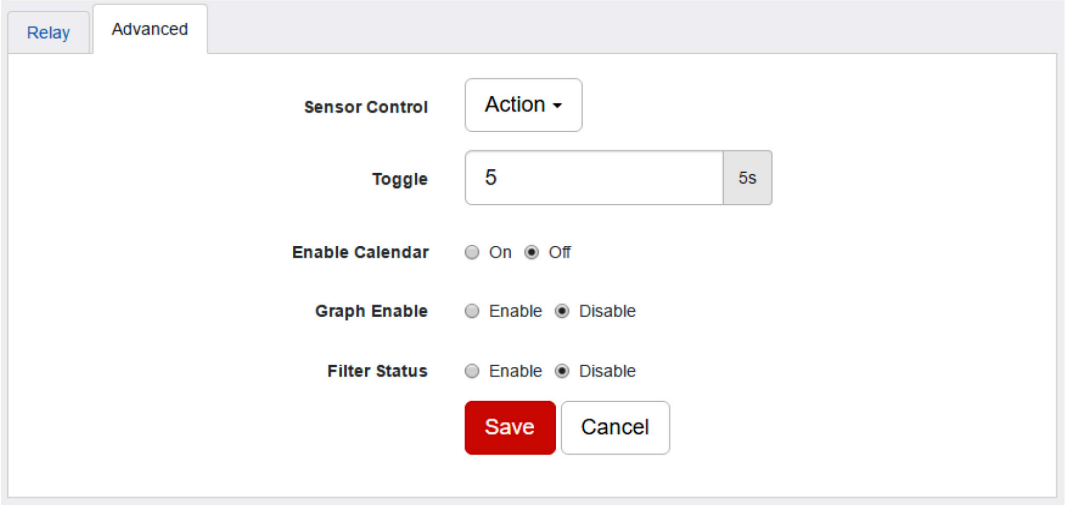

FIGURE 4-61. ADVANCED SENSOR CONFIGURATION SCREEN

- Sensor Control:

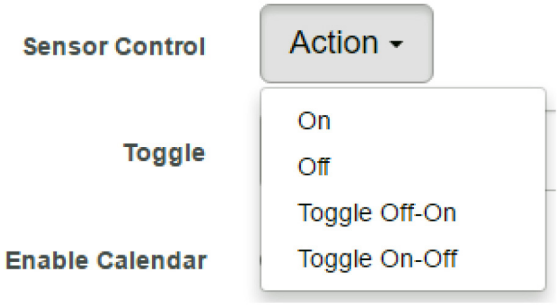

FIGURE 4-62. SENSOR CONTROL ACTION DROP-DOWN MENU

This button allows you to manually control the relay by controlling the cycle of the relay in an on-off-on or an off-on-off cycle. You can also set the "Toggle" (Cycle Time) here in seconds.

You don't need to change an option to be able to link the relay to an action.

The following actions can be chosen in an action: Turn on until sensor normal, turn off until sensor normal, cycle the relay, turn on until acknowledged, and turn off until acknowledged.

- Enable Calendar: Allows you to setup a Calendar Profile for what days and times you want or do not want the relay to be active.

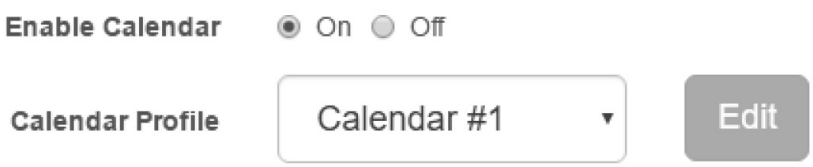

FIGURE 4-63. CALENDAR PROFILE EDIT BUTTON

Click on the Edit button next to a selected calendar to modify it.

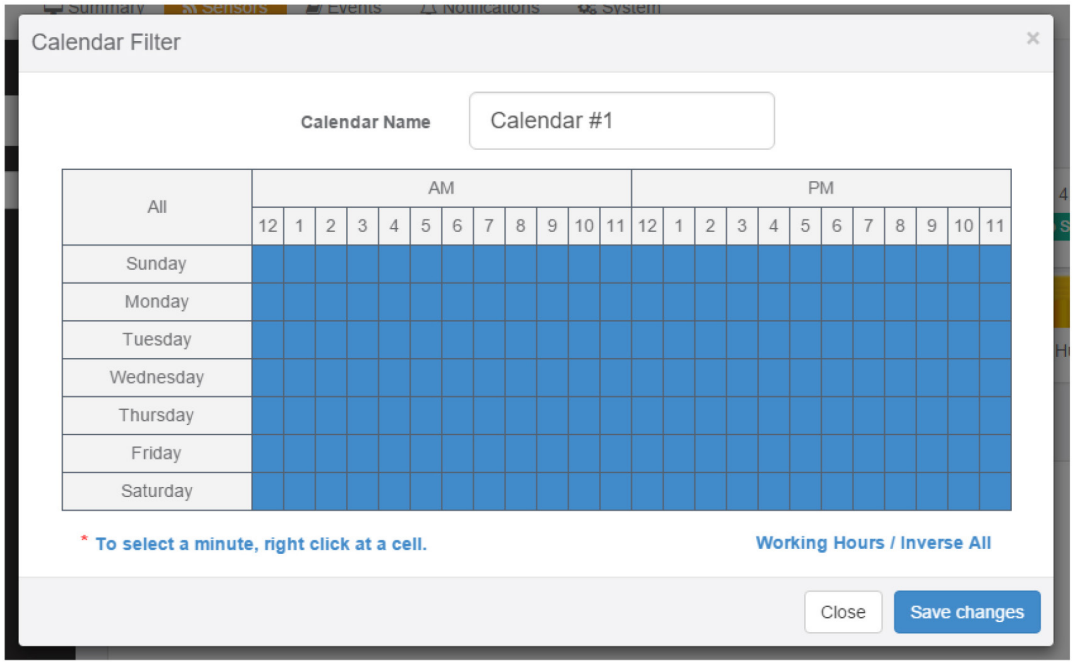

FIGURE 4-64. CALENDAR FILTER SCREEN

Blue cells means that the notification is on, white cells means it's off.

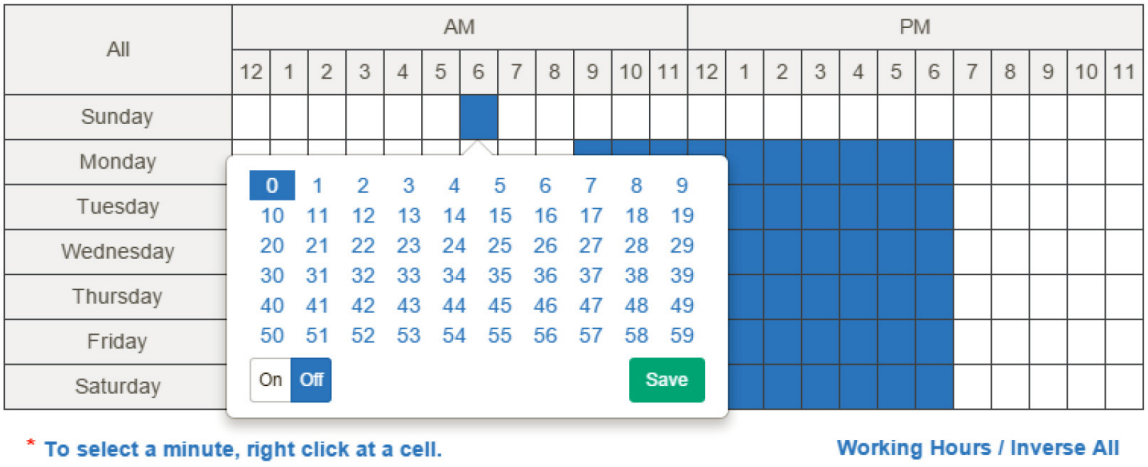

FIGURE 4-65. CALENDAR SCREEN

You can quickly select the Working Hours only, and specify a custom schedule down to minutes by right clicking on a cell.

4.7 MANAGING RACK MAPS

You can add a Rack Map as a graphical representation of your server rack, and to display and record the temperature of the airflow within your server cabinets.

NOTE: On the Web UI only limited options are available for the Rack Map; for example you cannot add devices or assets. Full functionality is available in the EMEMS Management software.

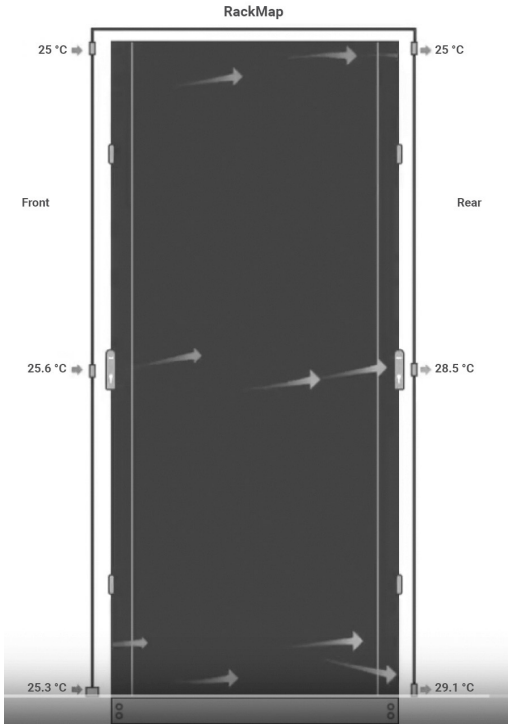

FIGURE 4-66. RACK MAP

Click on the Maps tab and Add Rack Map link to add a Rack Map:

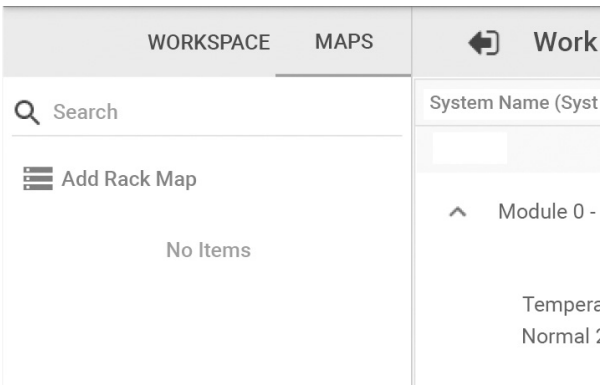

FIGURE 4-67. ADD RACK MAP LINK

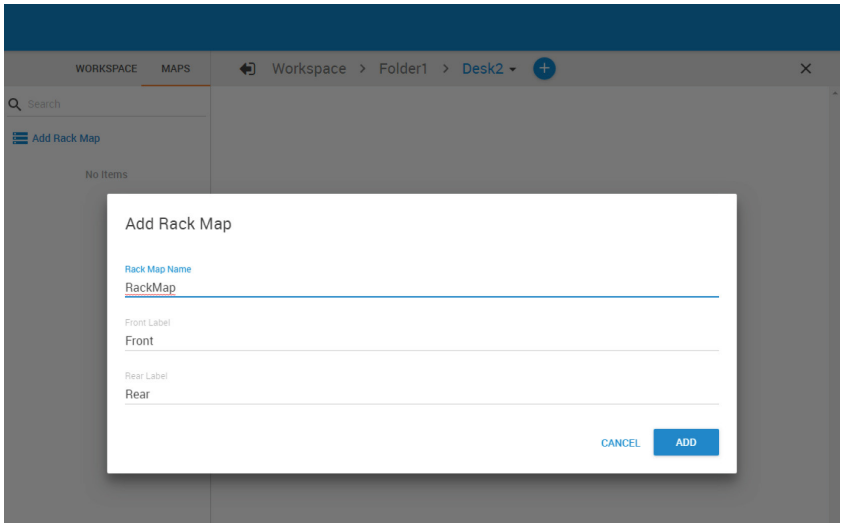

FIGURE 4-68. ADD RACK MAP SCREEN

After created, you can drag and drop the Rack Map to a desktop.

You can add Temperature sensors on a Rack Map. Simply drag and drop the desired sensor from your unit's sensor list, as shown below.

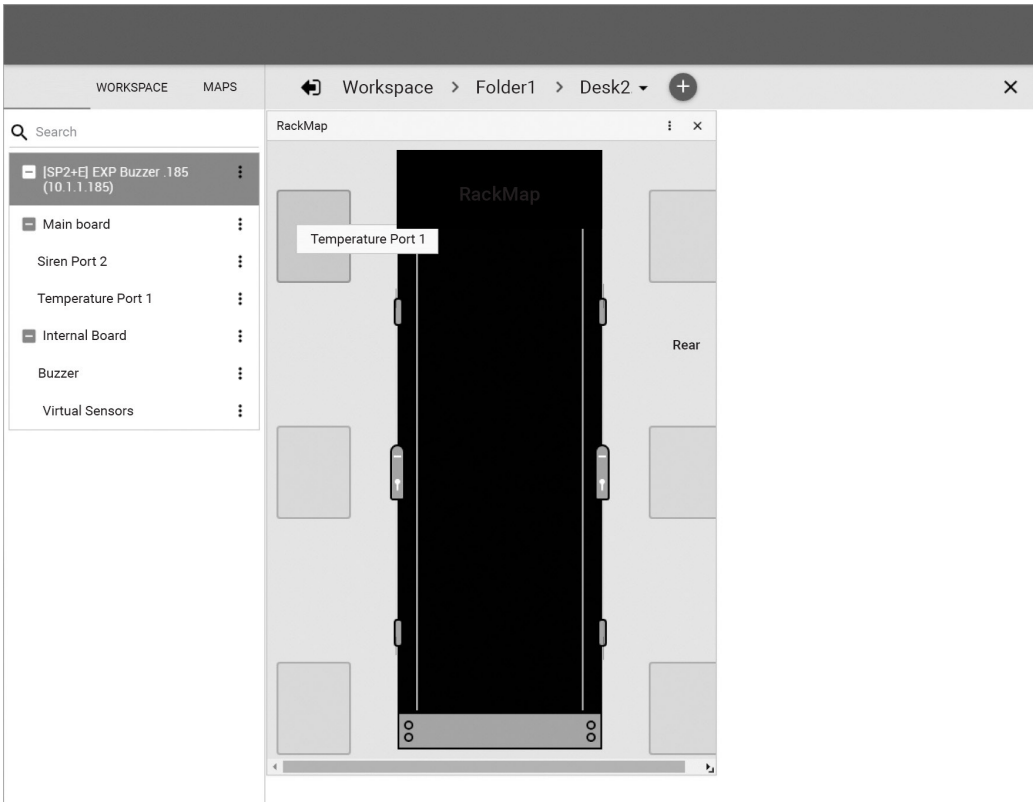

FIGURE 4-69 RACK MAP

4.8 FIRMWARE UPGRADE THROUGH THE WEB UI

The firmware upgrade process is very simple and straight-forward.

FIGURE 4-70. SYSTEM/MAINTENANCE PAGE

Open the System/Maintenance page and click on the Upgrade button at the System Firmware Upgrade section.

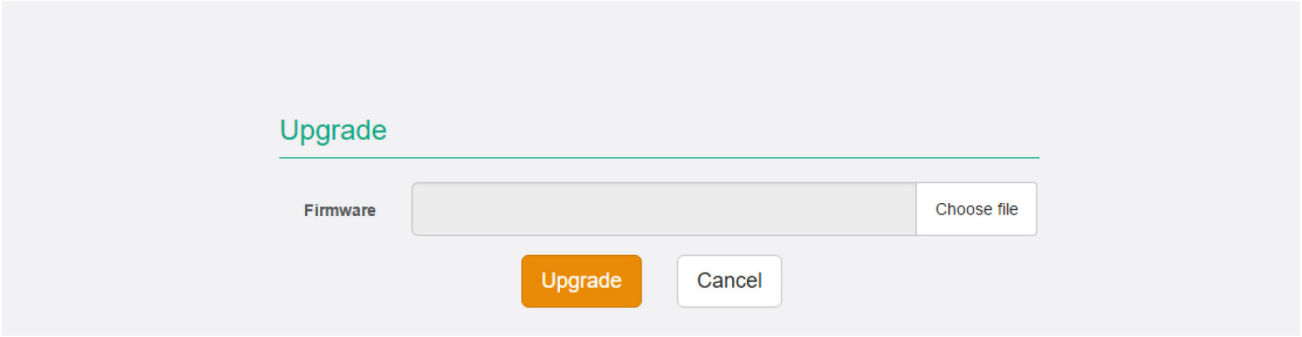

FIGURE 4-71. UPGRADE PAGE

This will start the Upgrade page. Choose the firmware file from your PC and click on Upgrade to start the process.

The firmware file for the AlertWerks Gateway has the following format:

spplus-1.0.1804.bin

- where 1.0.1804 is the build version.

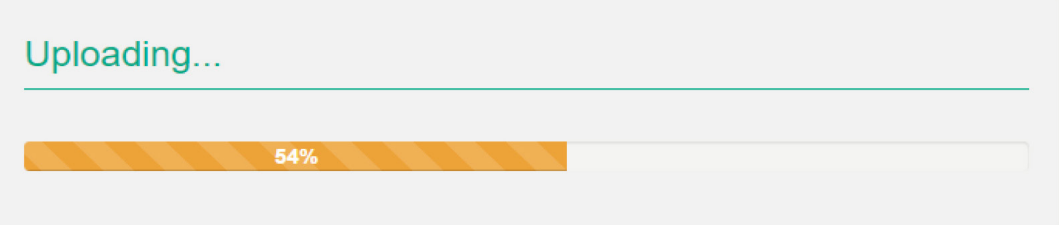

FIGURE 4-72. UPLOADING... SCREEN

First the file will be uploaded to the unit.

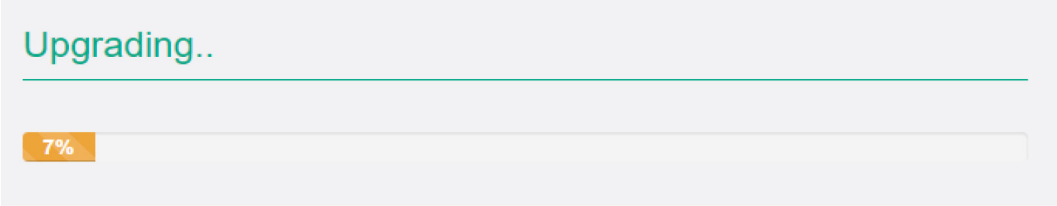

FIGURE 4-73. UPLOADING... SCREEN

Then the upgrade process will run. The whole process can be done in a few minutes.

The Power/Ethernet LED will be red during the upgrade.

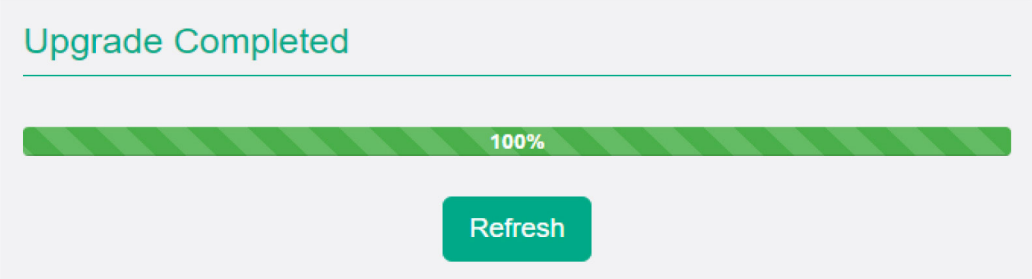

FIGURE 4-74. UPGRADE COMPLETED SCREEN

The unit will reboot at the end of the upgrade. Click on the Refresh button to reload the Web UI.

CHAPTER 5: CONFIGURING THE BUILT-IN NOTIFICATIONS

This chapter covers all of the built-in notifications on the AlertWerks Gateway and how to configure them.

5.1 EVENTS

The Events page contains all logged events that the unit stores. It's functioning like a categorized syslog, where you can search for a specific event, and also export the logged entries to a file.

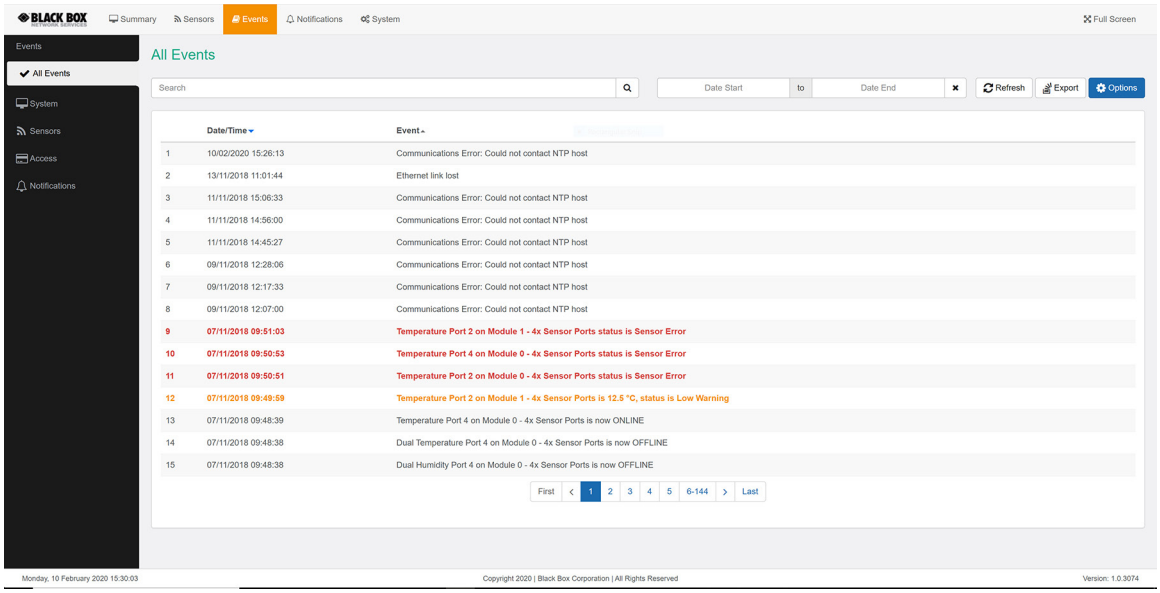

FIGURE 5-1. EVENTS PAGE

The default view is All Events, which contains all logs in one view. We'll explain all of the categories next.

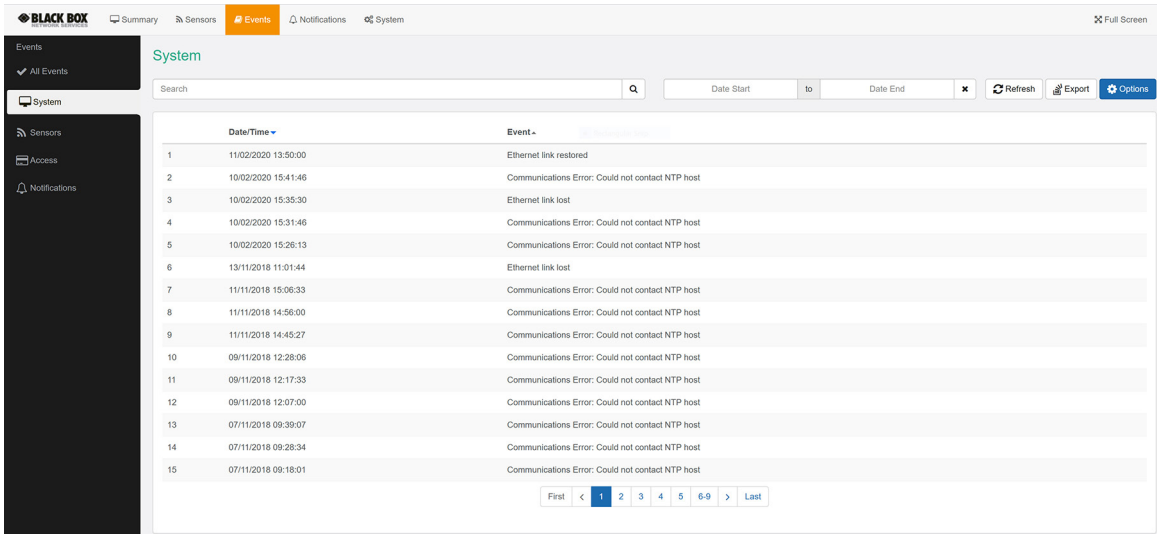

FIGURE 5-2. SYSTEM SCREEN

You can filter the events by type, by clicking on the tabs.

In this picture we've chosen to display only the System events.

EVENTS BY CATEGORY

- **All Events** — Contains all logs from the device, sorted by date and time; you can specify the start and end dates to narrow the list, or choose a specific log category.
- **System** — Contains the logs for the device's system events, such as reboot, firmware update etc.
- **Sensors** — Contains logs for all sensor related events, such as status changes, online/offline etc. and the port number where the sensor is attached.
- **Access** — Contains logs for all user authentication-related events, such as access granted/denied.
- **Notifications** — Contains logs for the active notifications on the device, for example the result of an email notification, heartbeat message or an SNMP Trap.

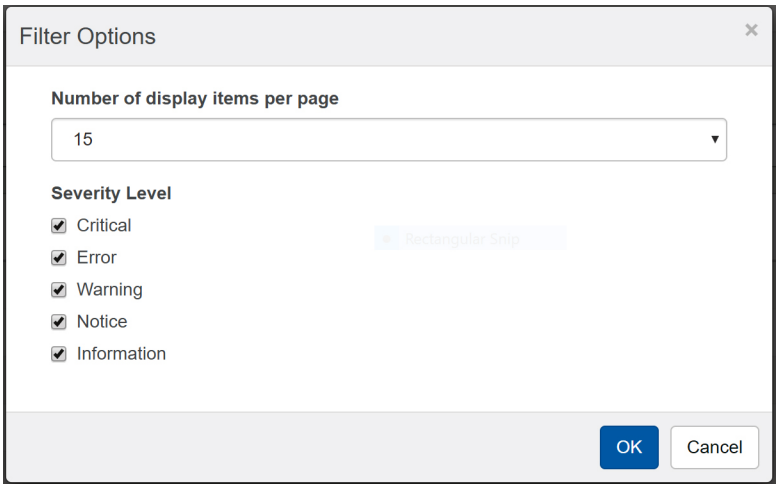

FIGURE 5-3. FILTER OPTIONS

In the Options, you can change the number of log entries displayed per page. The default is 15; it's possible to specify up to 100. Also, you can filter by Severity Level.

If you click on the Export button, a confirmation popup window will appear, asking if you'd like to export the log entries.

If you answer yes, then the full event log will be downloaded as a text file.

The file name will contain the IP address of the unit, for example: log_10.1.1.146.txt

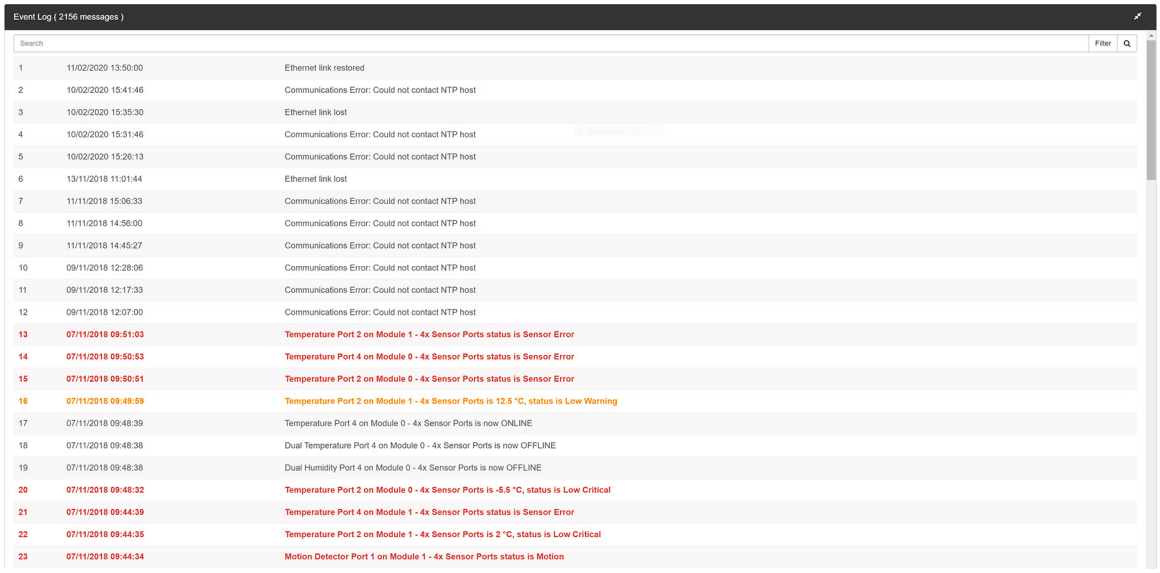

FIGURE 5-4. EVENT LOG

The unit's Summary page also shows the Event Log, which contains all entries from the "All Events" category. The last 30 entries are shown, but if you're scrolling down the list, more events (30 more) will be loaded automatically. You can view the full log if you keep scrolling down.

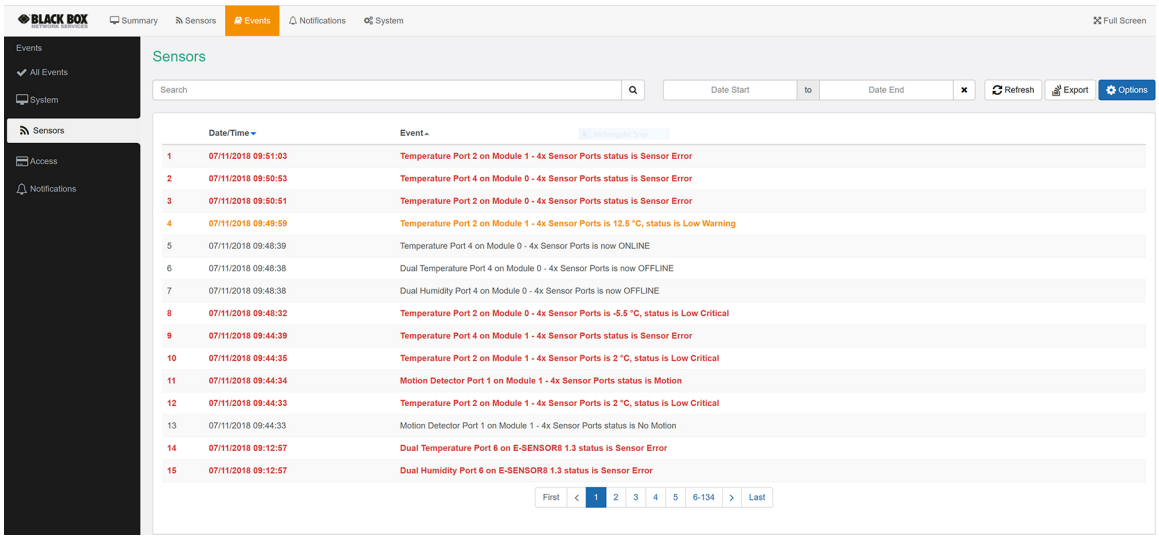

FIGURE 5-5. SENSORS SCREEN

In this picture, you can see the difference between logs generated by sensors connected to the base unit (Module 0) or the expansion board (Module 1).

5.2 NOTIFICATIONS

If you set up a notification, you can define the action to take when a sensor gives a reading beyond your previously set thresholds. This allows you to determine how you will be notified that a sensor's reading has reached the specified thresholds (high warning, critical etc).

What function do the different types of notifications provide?

The notifications are used to notify you when a sensor reading has hit a certain preset "critical" threshold. There are many ways you can be notified. They are as follows:

- **SNMP Trap:** This form of notification sends out a signal to your SNMP trap receiver server.
- **email:** This sends a notification via e-mail.
- **SMS:** This sends an SMS message to your mobile phone.
- **Relay:** The relay is used as a switch, for example, it could switch on an air conditioner unit if the temperature reading of a temperature sensor reaches a certain threshold.
- **Telephone call:** Will call you and play a customizable text to speech message.
- **Dry Contact:** You can control the Dry Contact ports with the notification, similar to the Relay action.

5.2.1 NOTIFICATIONS PAGE

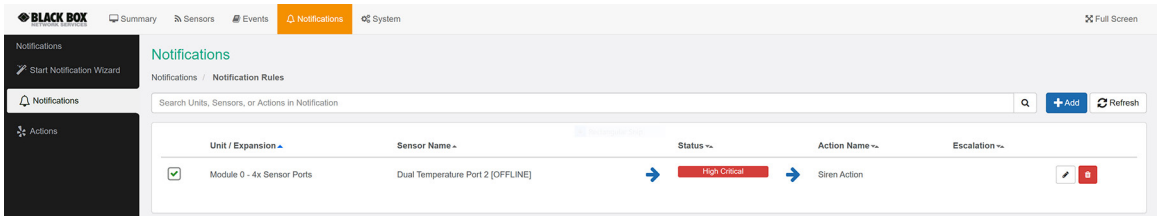

FIGURE 5-6. NOTIFICATIONS PAGE

This is the Notifications page. If you have notifications set up, they will appear in the list and you can edit or remove them.

If you don't have any actions set up, you'll need to create them first before making notifications. The notice to run the Action Wizard is displayed on the top for easy action setup. Click on the Start Now button or the Start Notification Wizard tab to start the wizard.

In the next section, we'll show you how to set up the actions.

After you have actions set up, you can link the actions to a sensor with the Add button.

All notifications are following the same setup steps with the Link Notification Wizard. We'll show you how to use this wizard with an example notification below in the manual with an SMS action, you'll then be able to configure other notifications similarly.

5.2.2 CREATE AN ACTION WITH THE ACTION WIZARD

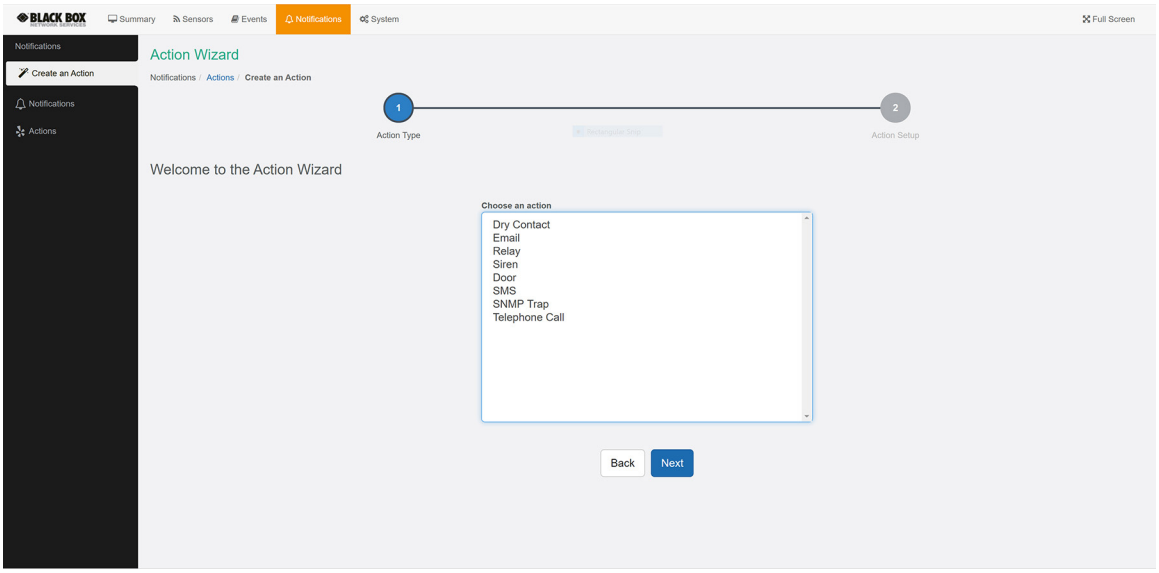

FIGURE 5-7. ACTION WIZARD SCREEN

This is the Action Wizard's welcome page; the supported Web UI configurable actions are shown. Select one to configure and click Next. We'll show you each action's configuration in the following sections.

NOTE: EMEMS Management Software allows more types of actions to be set up.

5.2.3 DRY CONTACT ACTION SETUP

You can use the Dry Contact Action to control a dry contact when a sensor reaches a certain threshold.

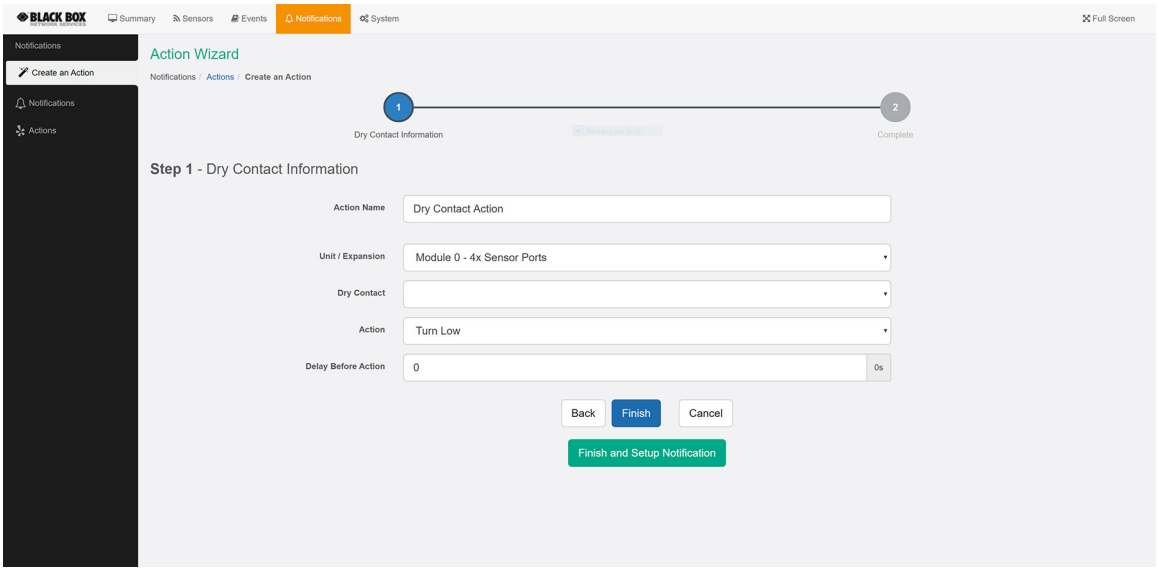

FIGURE 5-8. DRY CONTACT ACTION SETUP OPTION

NOTE: When using the RJ-45 I/O Dry Contacts, they need to be connected to the unit before they can be configured, and have to be in the Output direction.

If you click on the Finish and Setup Notification button, this will launch the Link Notification Wizard where you can use the new action for making a notification.

NOTE: If you've connected an expansion board, you can choose it from the Unit/Expansion selection menu as shown next.

You'll have the following options for controlling the Dry Contact with the action.

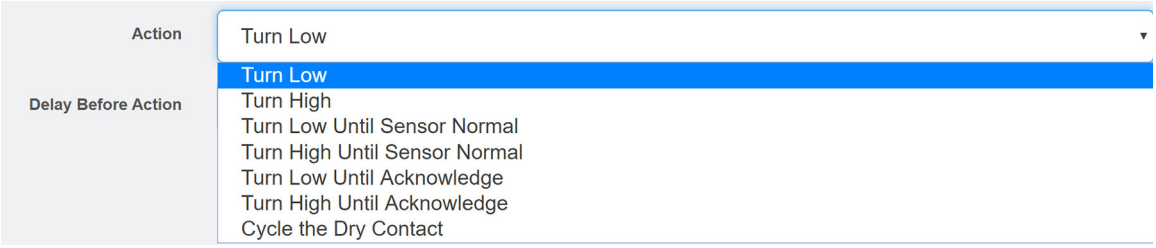

FIGURE 5-9. OPTIONS

If you choose to cycle the dry contact, you can specify the cycle time.

You'll need to change the RJ-45 I/O Dry Contact sensor to Output direction mode from the Sensors page as shown next.

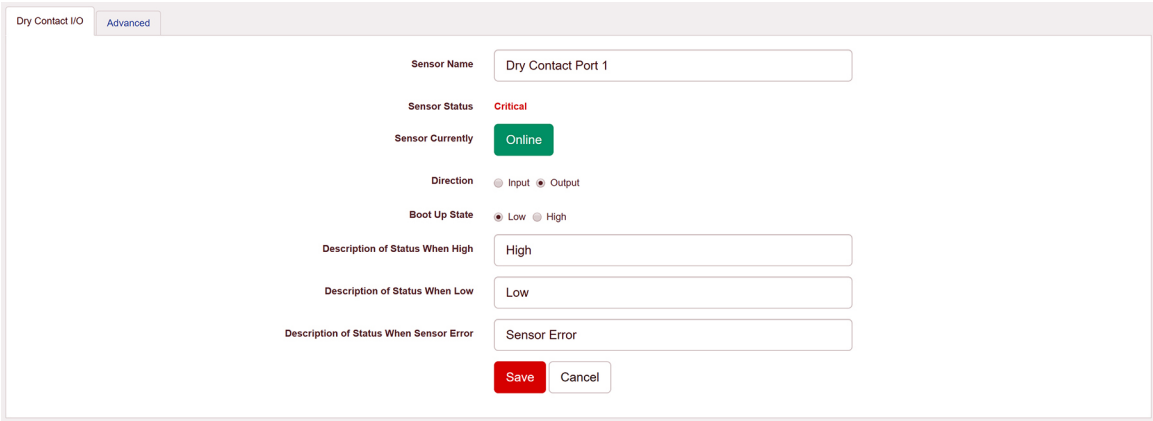

FIGURE 5-10. SELECT THE DIRECTION

Change the Direction from Input to Output and click Save.

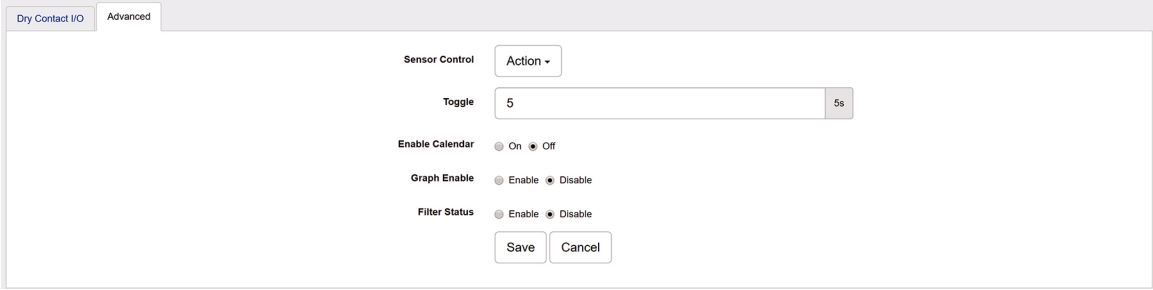

FIGURE 5-11. ADVANCED TAB

For the I/O Dry Contacts, you can choose to manually control the sensor from the Advanced tab using the Sensor Control button.

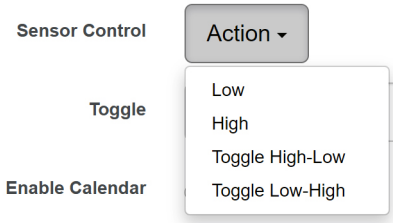

FIGURE 5-12. SENSOR CONTROL BUTTON

For the input-only Dry Contacts, the configuration doesn't need to be changed.

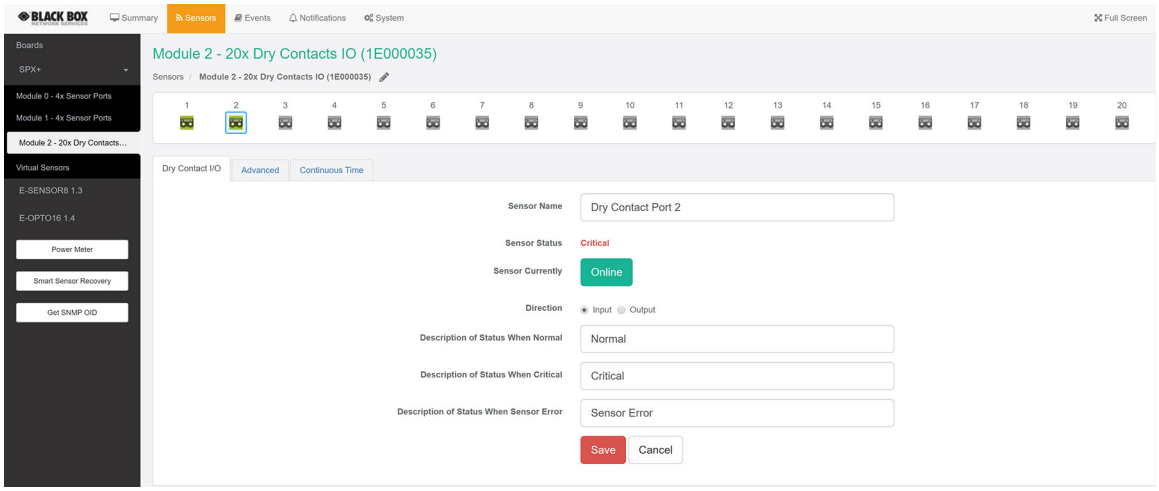

FIGURE 5-13. DRY CONTACTS SCREEN

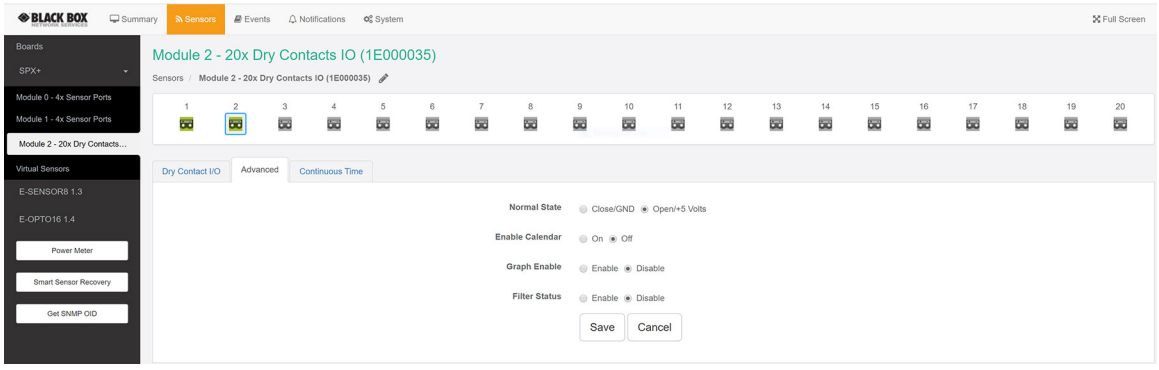

FIGURE 5-14. ADVANCED TAB

You can select the Normal State for a given Dry Contact from the Advanced tab, as well as enabling the Calendar, Graphing, and Filter Status options.

5.2.4 EMAIL ACTION SETUP

You can use the Email Action to send a notification by email when a sensor reaches a certain threshold.

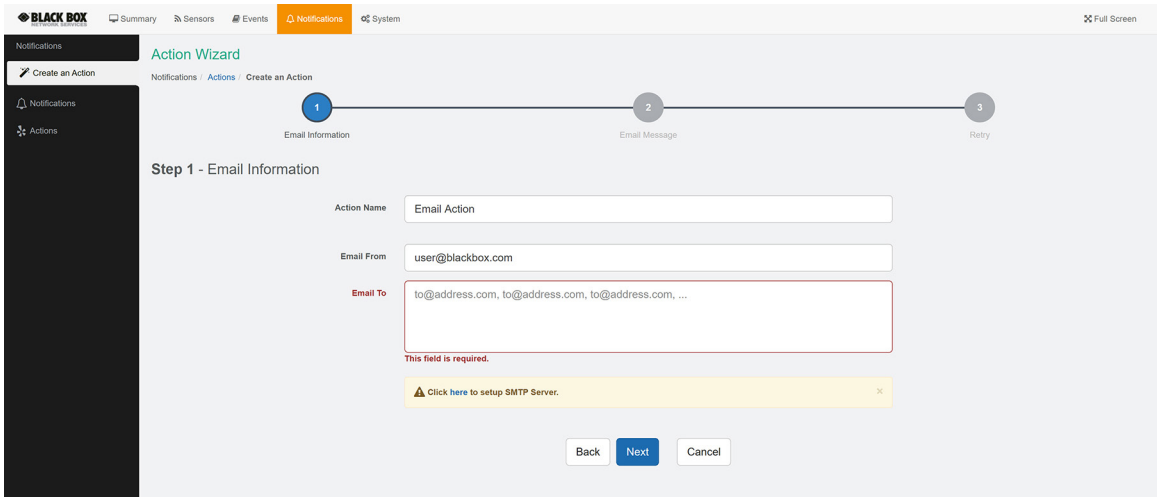

FIGURE 5-15. EMAIL INFORMATION

NOTE: The SMTP server settings needed to be configured on the unit before this action will work.

All email actions will use this SMTP server for sending emails.

Either click on the link on the notice, or go to the System/SMTP page for the configuration.

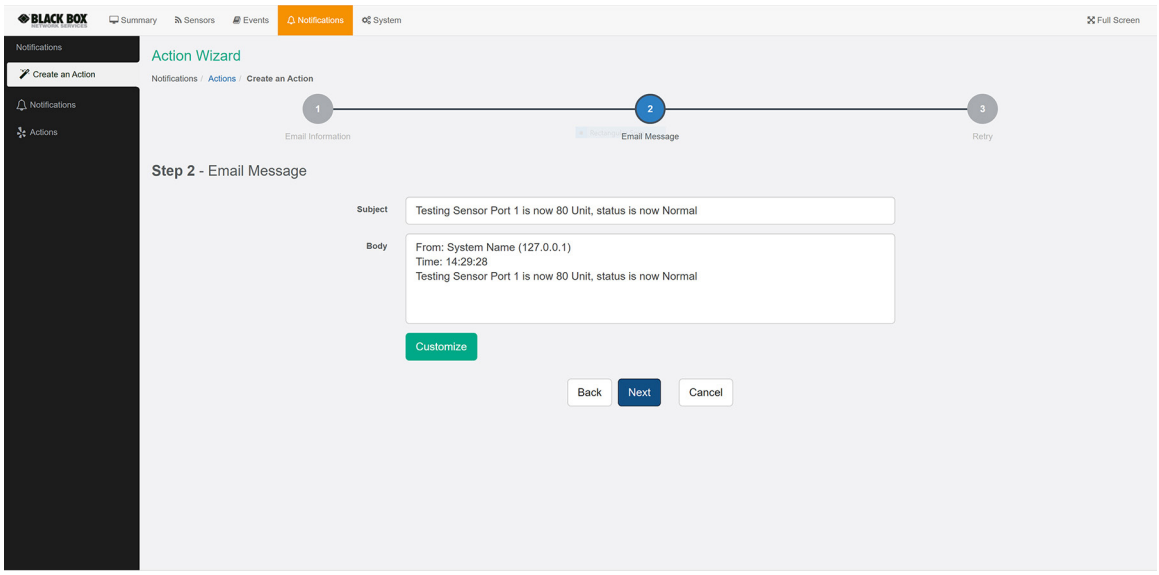

FIGURE 5-16. EMAIL MESSAGE

After clicking “Next,” you will get a page where you can input the email name and message. Press the “Customize” button and the fields will re-write in a format that will allow for an automated email that will display the sensor information.

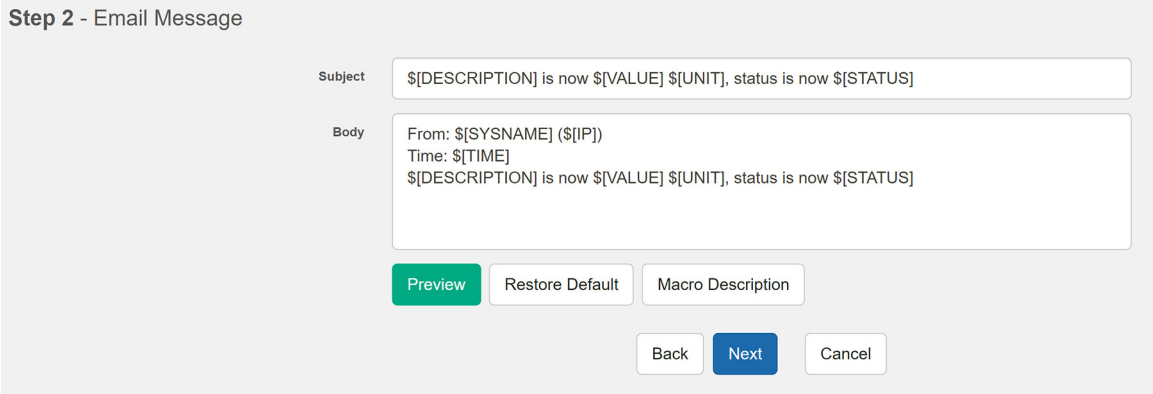

FIGURE 5-17. ENTER EMAIL NAME AND MESSAGE

For all possible macro values (dynamic text values starting with $), you can see a detailed list at the end of this chapter.

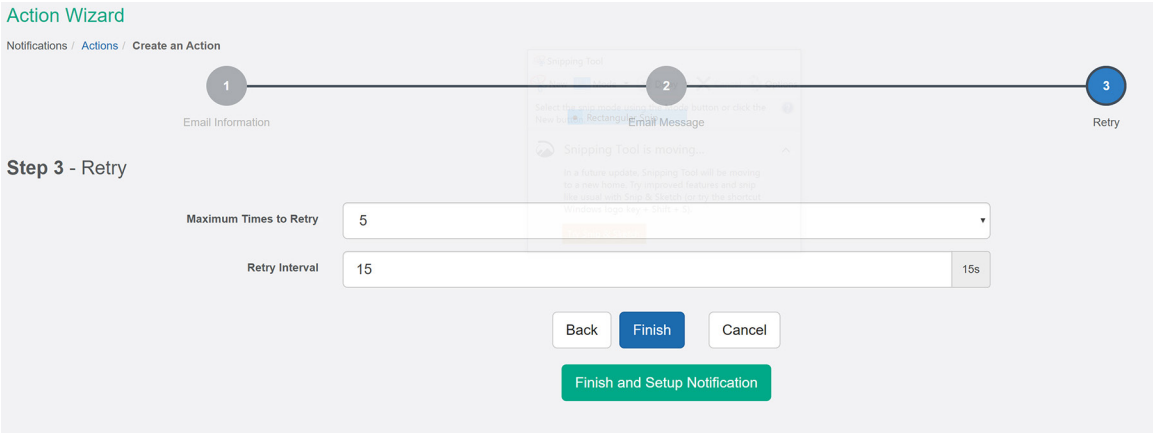

FIGURE 5-18. RETRY

These parameters set the maximum number of times to send the email notification and the time interval between each notification.

If you click on the Finish and Setup Notification button, this will launch the Link Notification Wizard where you can use the new action for making a notification.

5.2.5 RELAY ACTION SETUP

You can use the Relay Action to control a relay when a sensor reaches a certain threshold.

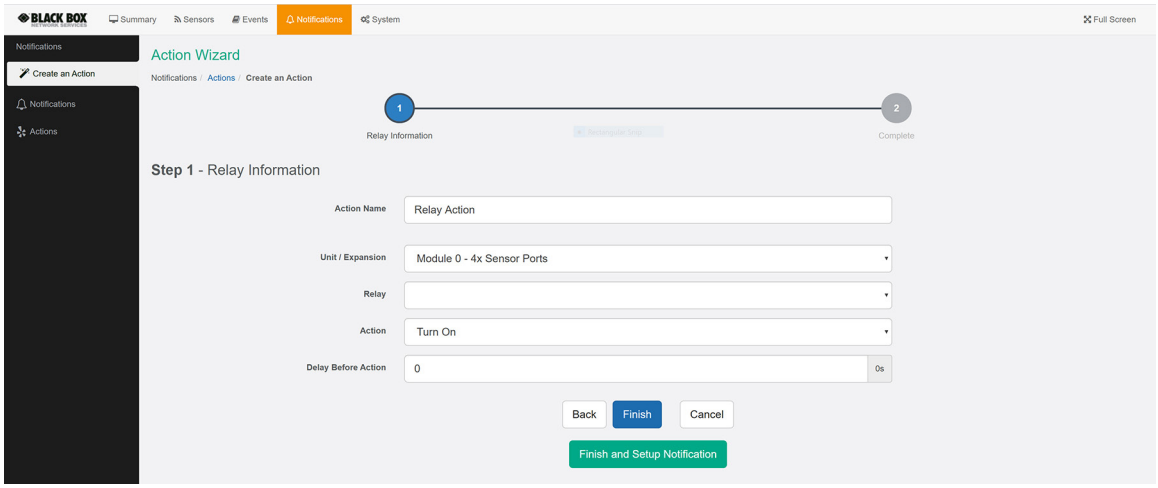

FIGURE 5-19. RELAY INFORMATION

NOTE: The relay needs to be connected to the unit before it can be configured.

If you click on the Finish and Setup Notification button, this will launch the Link Notification Wizard where you can use the new action for making a notification.

NOTE: If you've connected an expansion board, you can choose it from the Unit/Expansion selection menu as shown next.

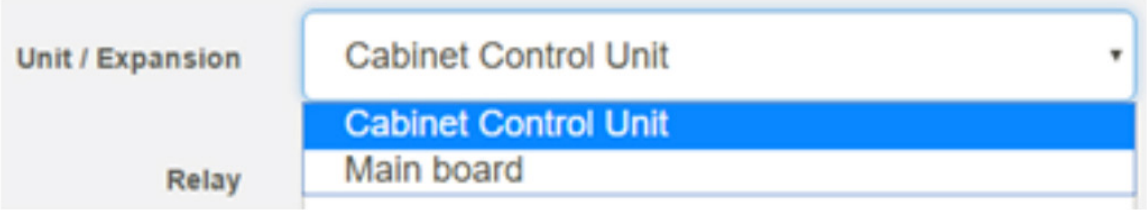

FIGURE 5-20. UNIT/EXPANSION SELECTION MENU

You'll have the following options for controlling the relay with the action.

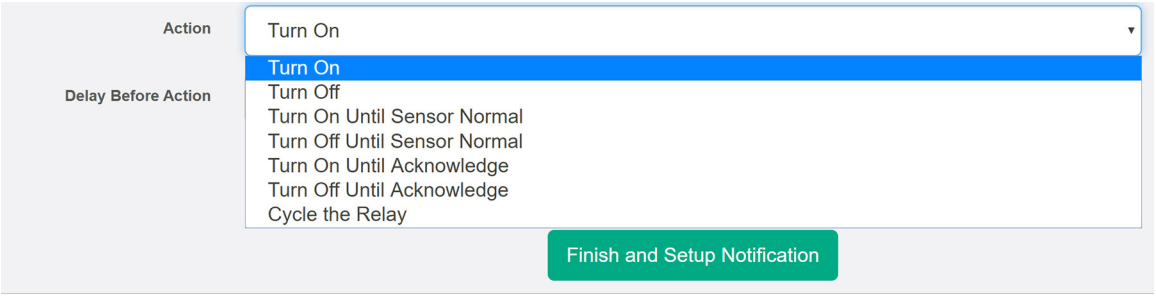

FIGURE 5-21. RELAY CONTROL OPTIONS

If you click on the Finish and Setup Notification button, this will launch the Link Notification Wizard where you can use the new action for making a notification.

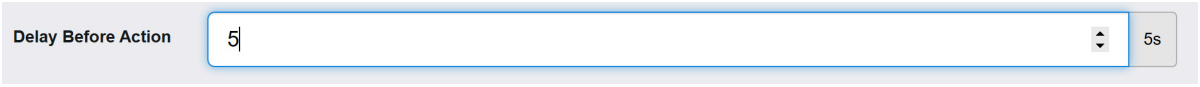

FIGURE 5-22. CYCLE TIME SCREEN

If you choose to cycle the relay, you can specify the cycle time.

On the Sensors page, you can specify additional settings for the relay as shown next.

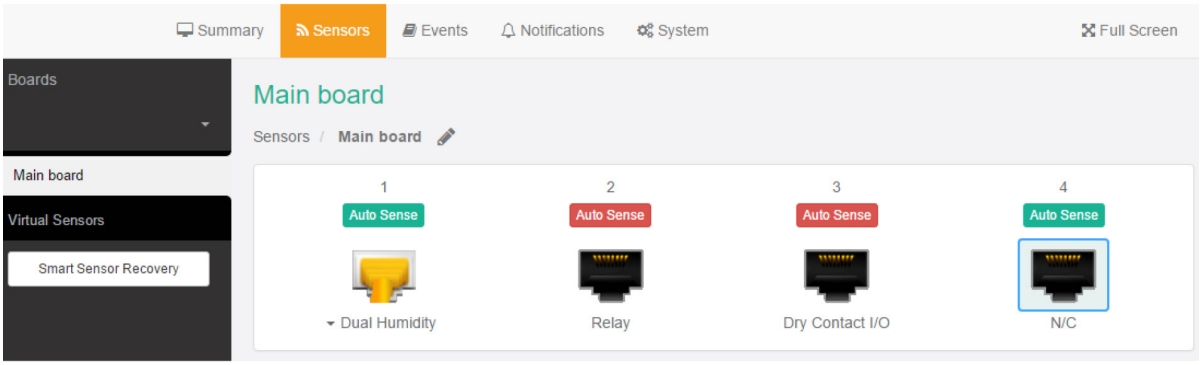

FIGURE 5-23. SENSORS PAGE

You can choose to manually control the sensor from the Advanced tab using the Sensor Control button.

5.2.6 SIREN ACTION SETUP

You can use the Siren Action to turn on the siren and strobe light when a sensor reaches a certain threshold.

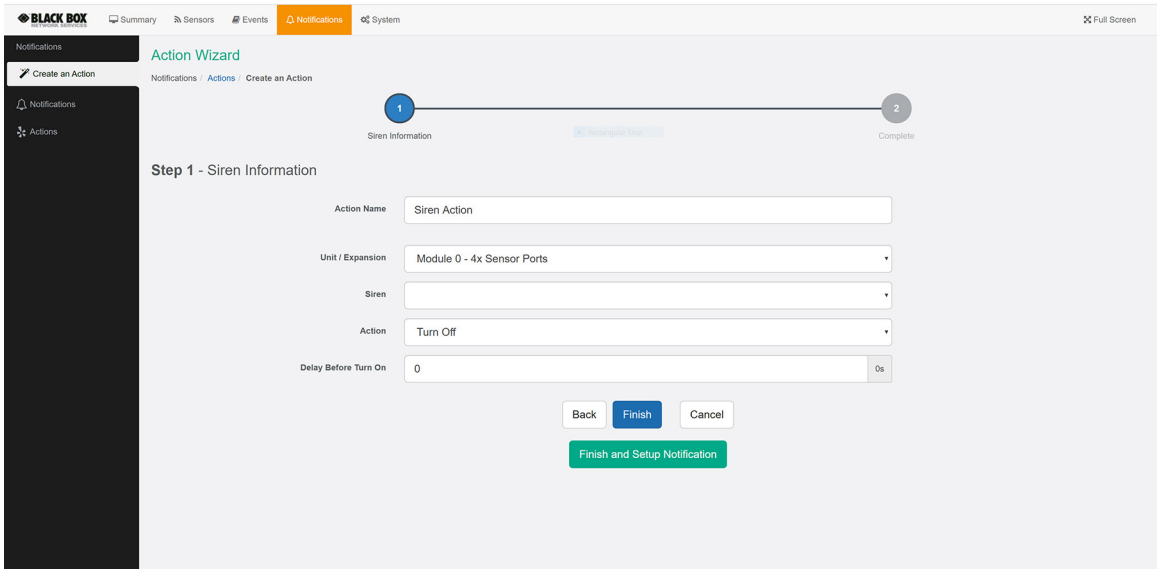

FIGURE 5-24. SIREN INFORMATION SCREEN

NOTE: The siren needs to be connected to the unit before it can be configured.

You'll have the following options for controlling the siren with the action.

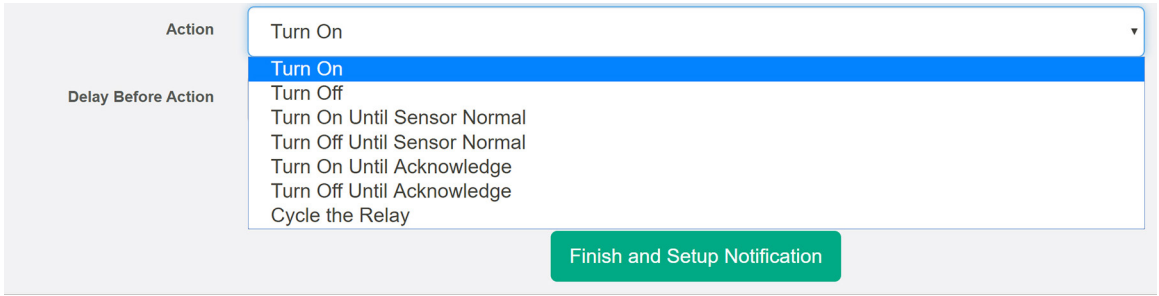

FIGURE 5-25. SIREN ACTION OPTIONS

If you choose Defined Time, you can specify the time in seconds for how long the siren should be turned on.

On the Sensors page, you can specify additional settings for the siren as shown next.

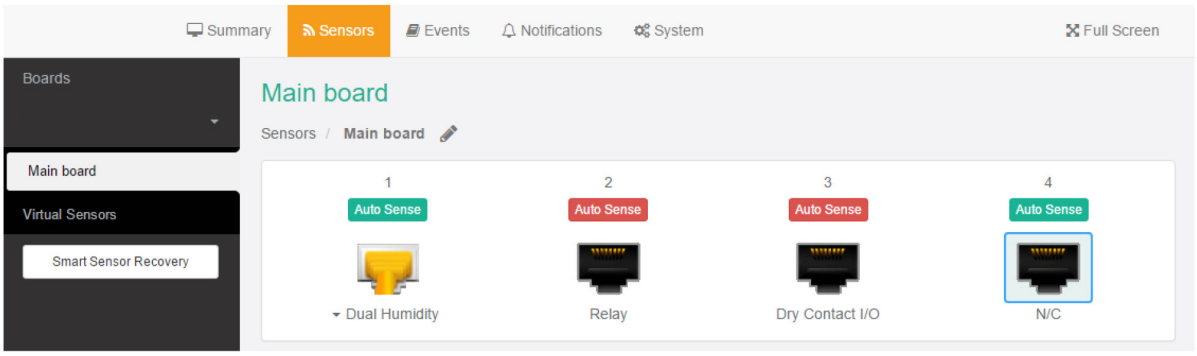

FIGURE 5-26. SENSORS PAGE, SIREN SETTINGS

You can choose to manually control the sensor from the Advanced tab using the Sensor Control button.

5.2.7 SMS ACTION SETUP

You can use the SMS Action to send a notification by SMS when a sensor reaches a certain threshold.

The unit can send an SMS, or voice alert to many different phone numbers, but you can specify only one phone number per action when setting it up. However, please keep in mind that both the SMS and the dial up actions such as Voice will call to the first number, then after sending to this number, it will call to the second number and so on. So, if you have many numbers in the call list, it will take that much more time to finish sending the SMS or dial up Voice call alerts.

NOTE: The modem module is needed and must be configured for this action.

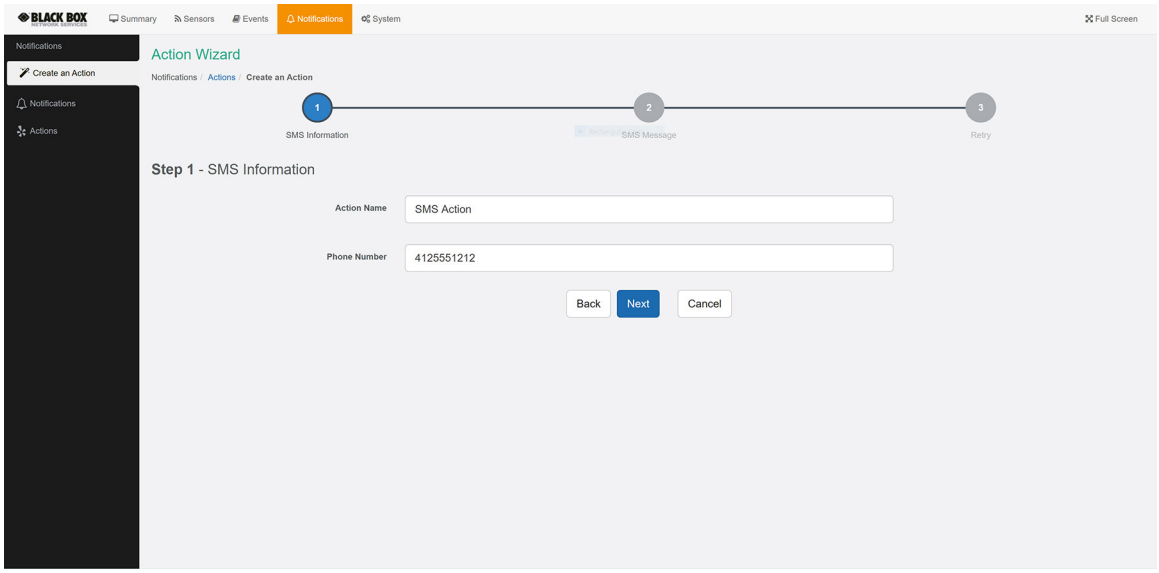

FIGURE 5-27. SMS ACTION SCREEN

After typing in your phone number, click Next.

You can specify only one phone number per action.

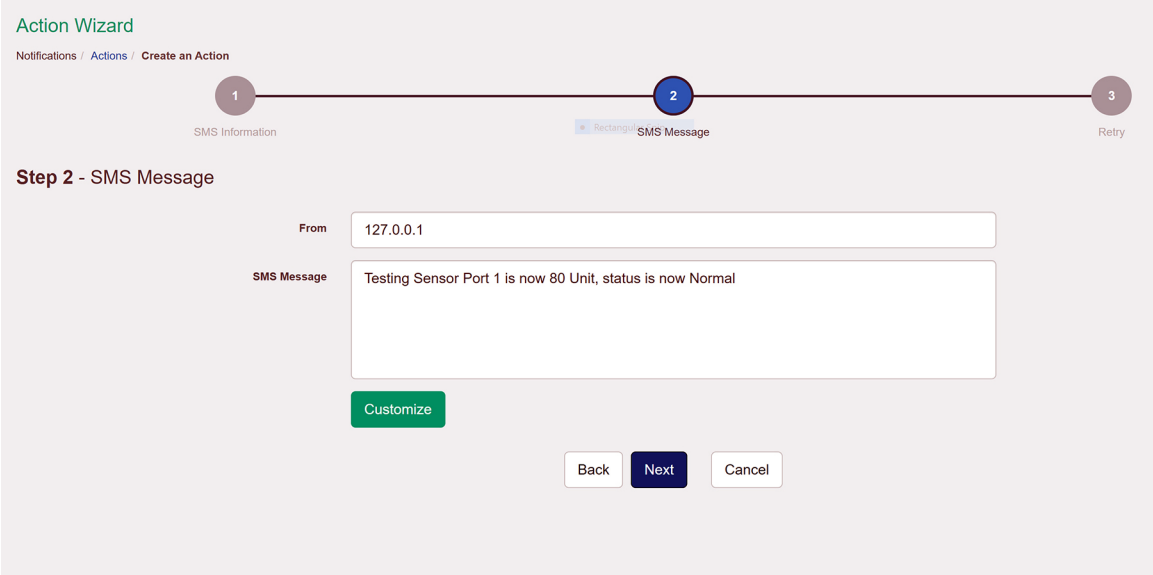

FIGURE 5-28. SMS MESSAGE SCREEN

After clicking "Next," you will get a page where you can input the SMS message. Press the "Customize" button and the fields will re-write in a format that will allow for an automated SMS that will display the sensor information.

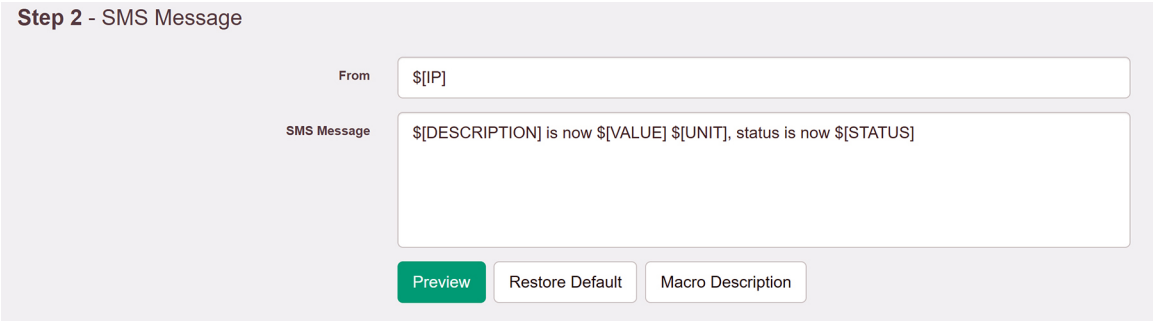

FIGURE 5-29. SMS MESSAGE

For all possible macro values (dynamic text values starting with $), you can see a detailed list at the end of this manual.

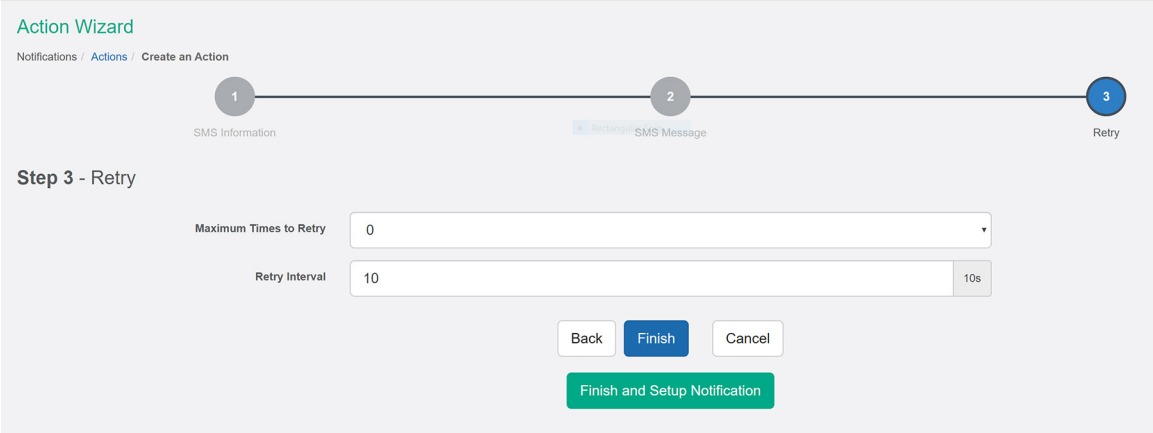

FIGURE 5-30. RETRY SCREEN

These parameters set the maximum number of times to send the SMS notification and the time interval between each notification.

If you click on the Finish and Setup Notification button, this will launch the Link Notification Wizard where you can use the new action for making a notification.

Troubleshooting the SMS Action

If you are having trouble sending the SMS alerts, go through the check list below. Also, try moving the modem's antenna to a slightly different location.

1. Test the SIM card on mobile phone: verity the account is active, has adequate credit for making phone calls, and that the PIN code is disabled.
2. Make sure that the SIM card is properly inserted in the modem's slot. Inserting and removing the SIM is only possible while the unit is powered off; otherwise, you can damage the SIM or the unit.

5.2.8 SNMP TRAP ACTION SETUP

You can use the SNMP Trap Action to send a notification (Trap message) to your SNMP Trap Receiver server when a sensor reaches a certain threshold.

SNMP v1 Action

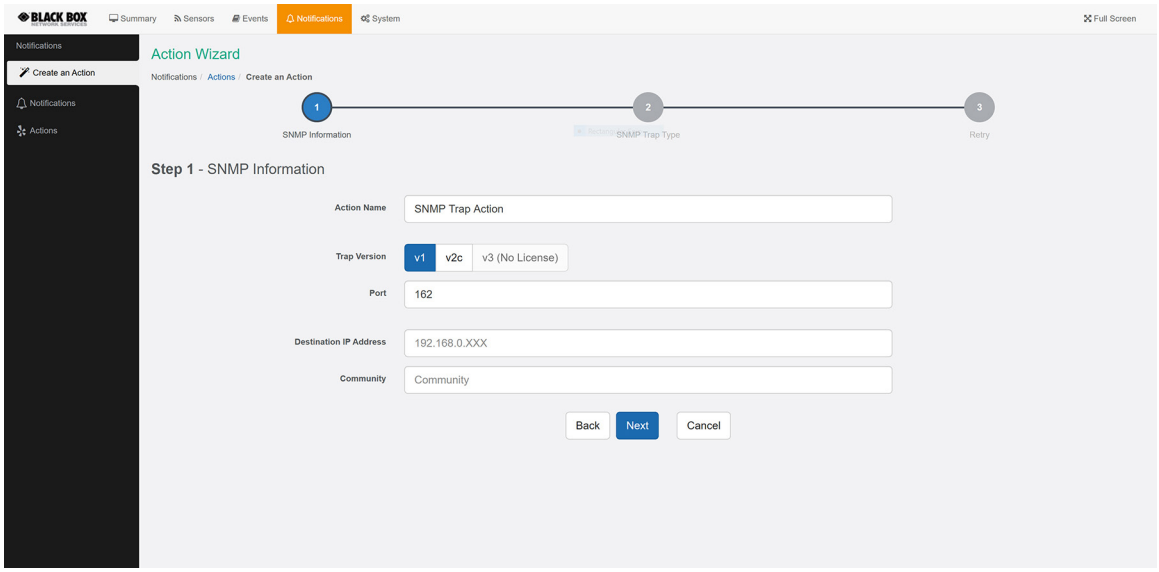

FIGURE 5-31. SNMP INFORMATION SCREEN

Enter your Destination IP Address and Community; the default SNMP port is automatically selected.

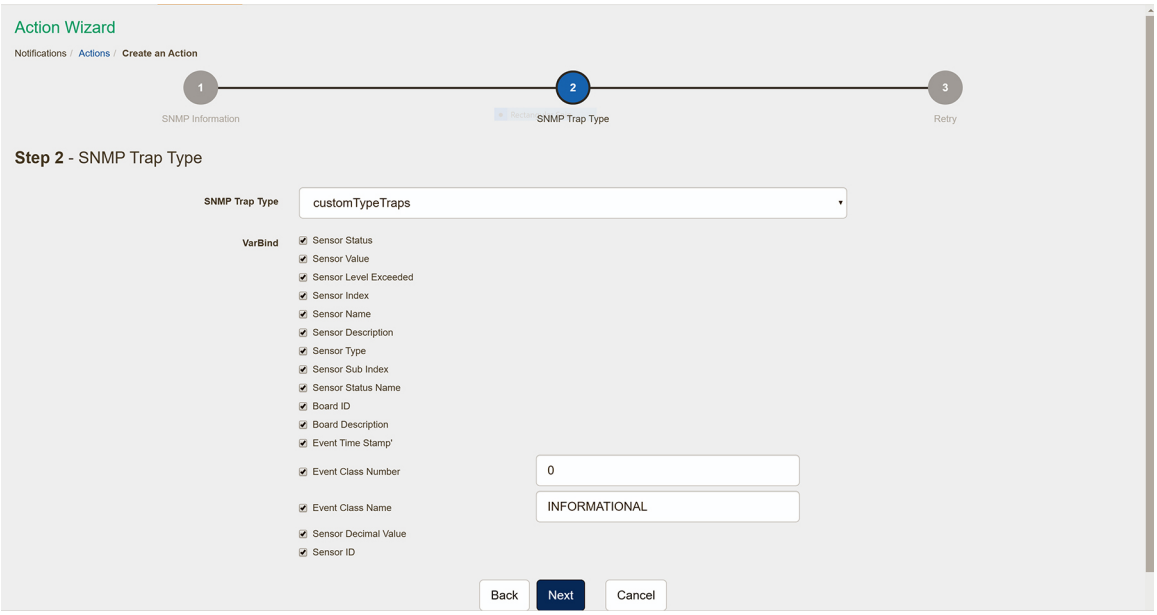

FIGURE 5-32. SNMP TRAP TYPE SCREEN

A different trap message is sent for each sensor type, such as temperature, humidity, and switch.

The trap messages include VarBind fields that include the current sensor status (Normal, Critical High, Warning High, Critical Low, Warning Low, and sensorError), the current sensor value, the level exceeded, the sensor index, the sensor name, and the sensor description.

You can enable or disable specific fields if you choose the customTypeTraps from the drop-down list.

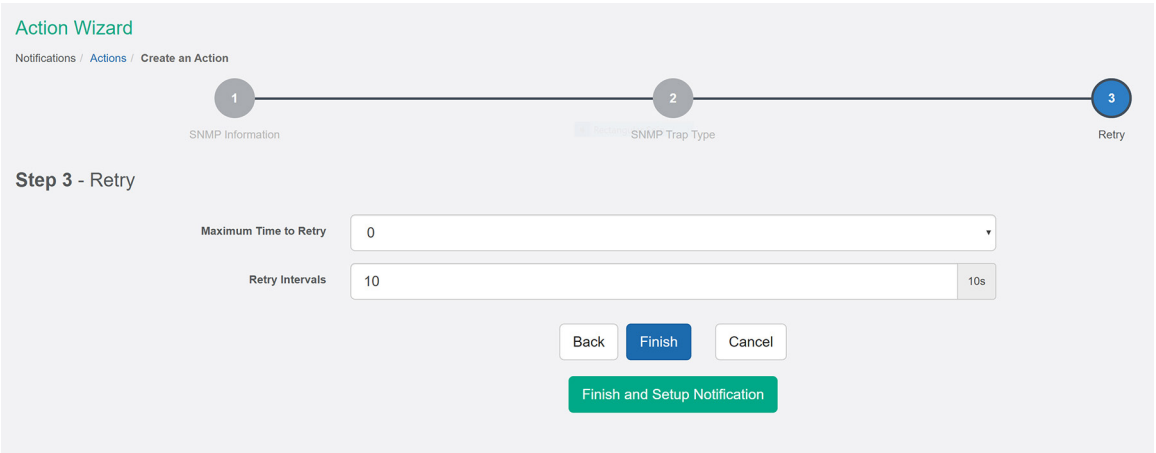

FIGURE 5-33. RETRY SCREEN

These parameters set the maximum number of times to send the trap notification and the time interval between each notification.

If you click on the Finish and Setup Notification button, this will launch the Link Notification Wizard where you can use the new action for making a notification.

SNMP v2c Action

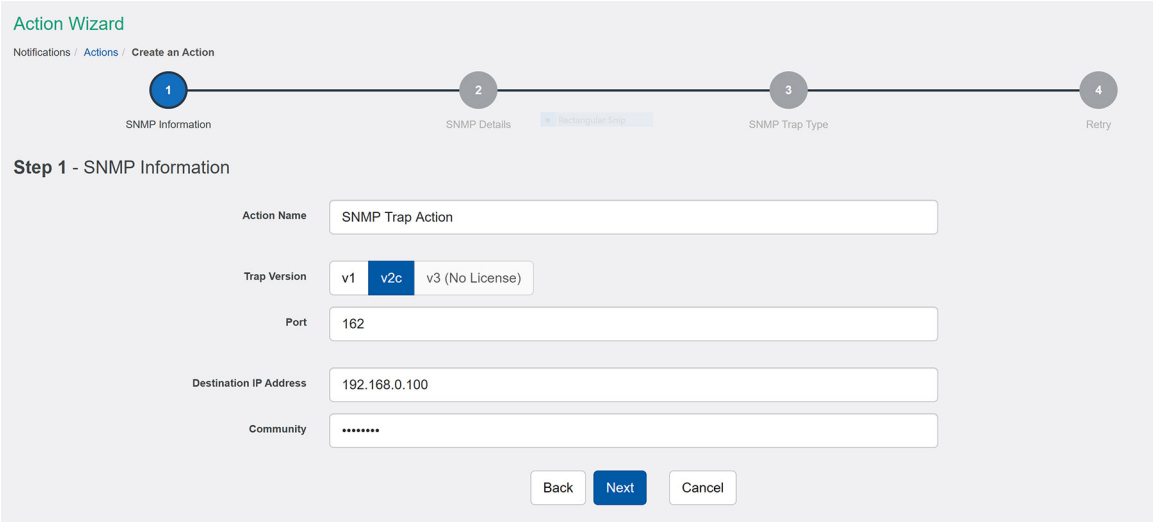

FIGURE 5-34. SNMP INFORMATION SCREEN

Enter your Destination IP Address and Community; the default SNMP port is automatically selected.

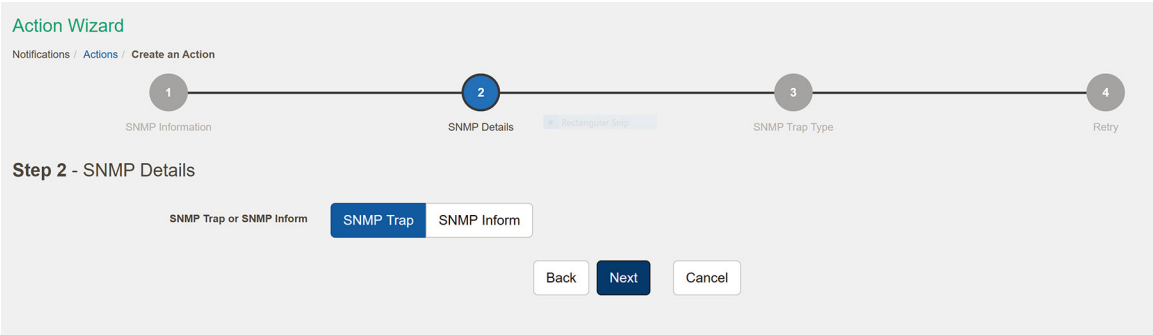

FIGURE 5-35. SNMP DETAILS SCREEN

You can choose the packet to be sent between SNMP Trap or Inform packet.

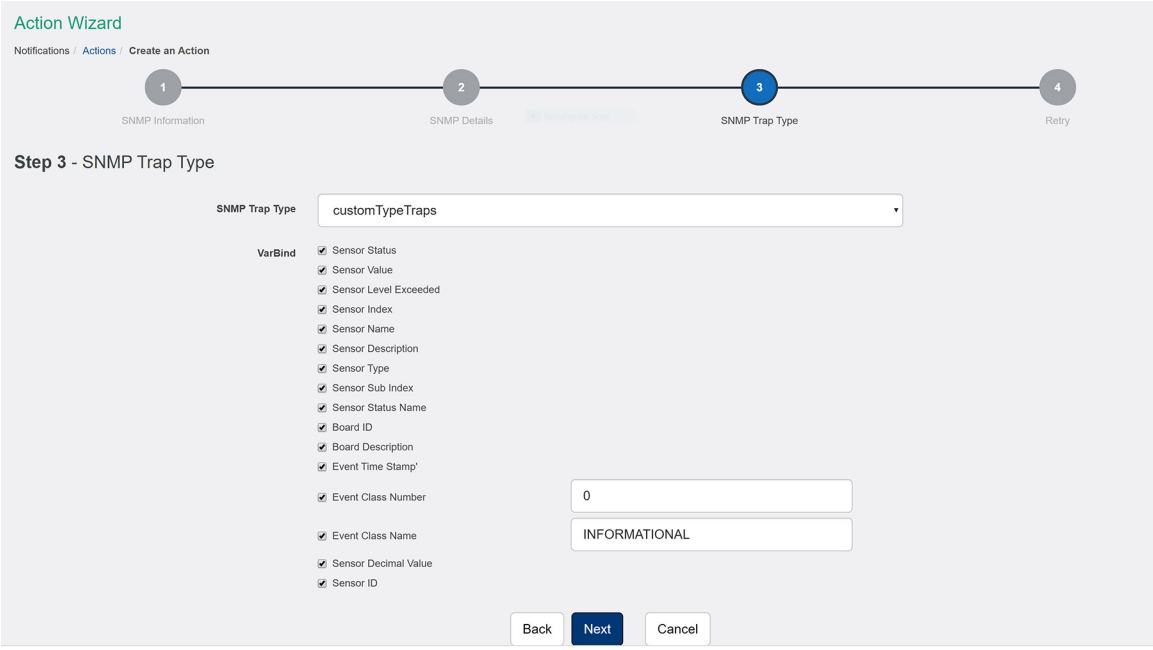

FIGURE 5-36. SNMP TRAP TYPE SCREEN

A different trap message is sent for each sensor type such as temperature, humidity, and switch. The trap messages include VarBind fields that include the current sensor status (Normal, Critical High, Warning High, Critical Low, Warning Low, and sensorError), the current sensor value, the level exceeded, the sensor index, the sensor name, and the sensor description.

You can enable or disable specific fields if you choose the customTypeTraps from the drop-down list.

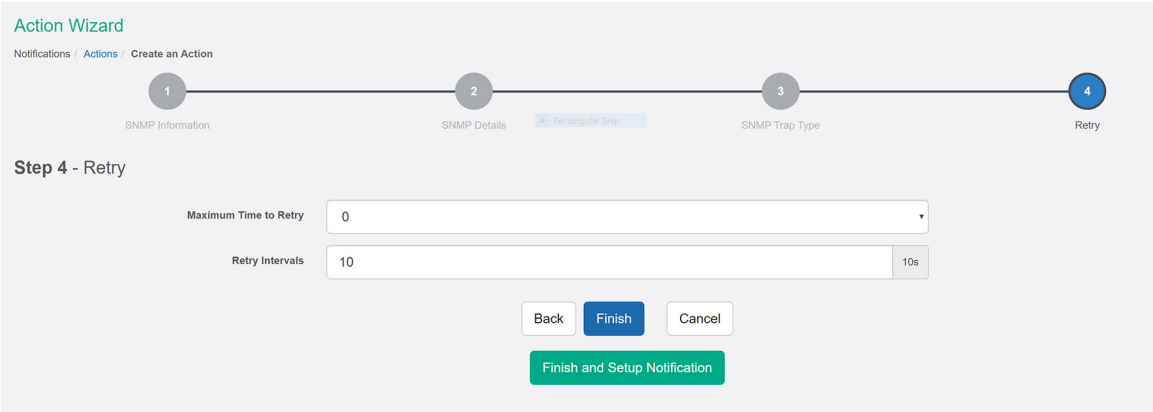

FIGURE 5-37. RETRY SCREEN

These parameters set the maximum number of times to send the trap notification and the time interval between each notification.

If you click on the Finish and Setup Notification button, this will launch the Link Notification Wizard where you can use the new action for making a notification.

SNMP v3 action

Only SNMPv3 provides secure SNMP communication. The previous versions are considered unsecure and unencrypted.

This feature requires a separate license.

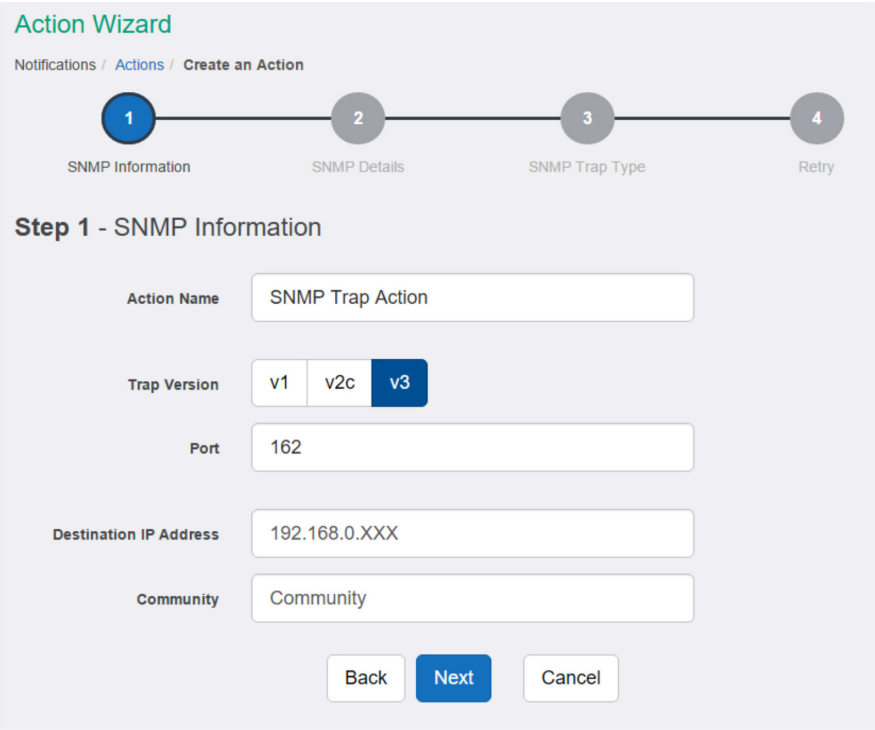

FIGURE 5-38. SNMP INFORMATION SCREEN

Enter your Destination IP Address and Community; the default SNMP port is automatically selected.

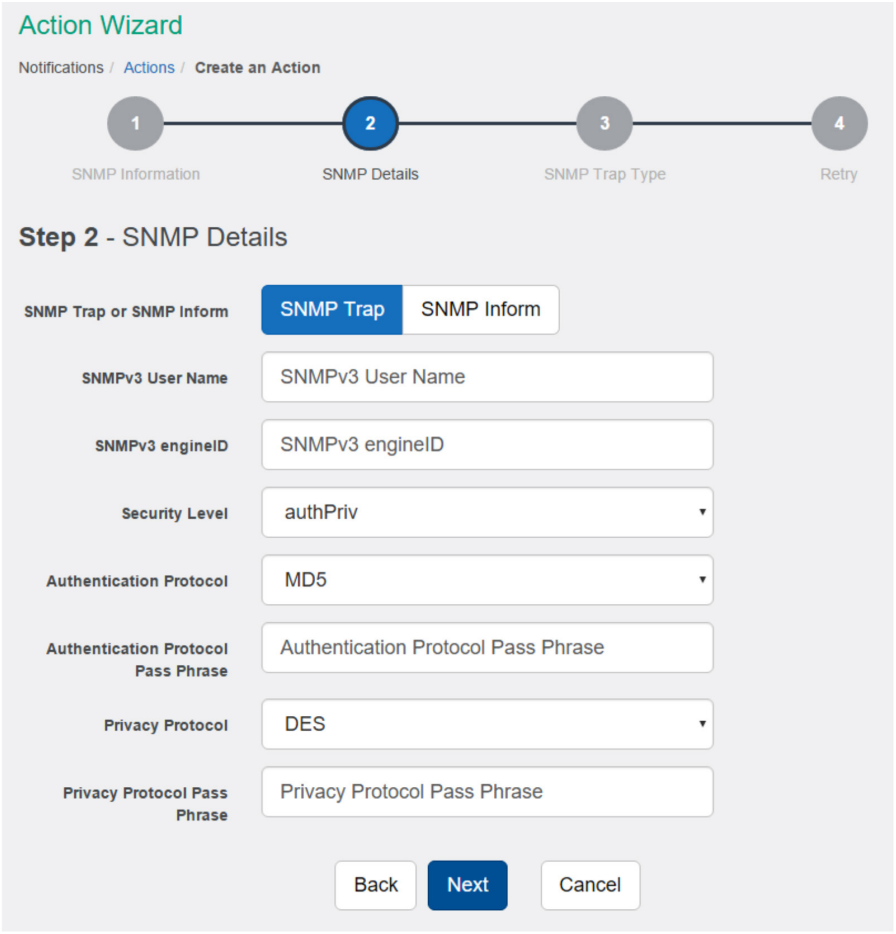

FIGURE 5-39. SNMP DETAILS SCREEN

You can choose the packet to be sent between SNMP Trap or Inform packet.

Configure the settings for authentication, and access privileges.

Next, we'll give a quick description of each setting.

Level	Authentication	Encryption	Description
noAuthNoPriv	Username	No	Match Username (same as SNMP v1/v2c)
authNoPriv	MD5 or SHA	No	Auth Based on Algorithms (check password)
authPriv	MD5 or SHA	Yes - DES	Auth Algorithms and Encryption

Basically, if you select noAuthNoPriv then the setup will be the same as with SNMP v1 and v2c versions: authentication is only checked by unencrypted username.

authNoPriv will provide password protection but no encryption.

authPriv provides encrypted username and password protection.

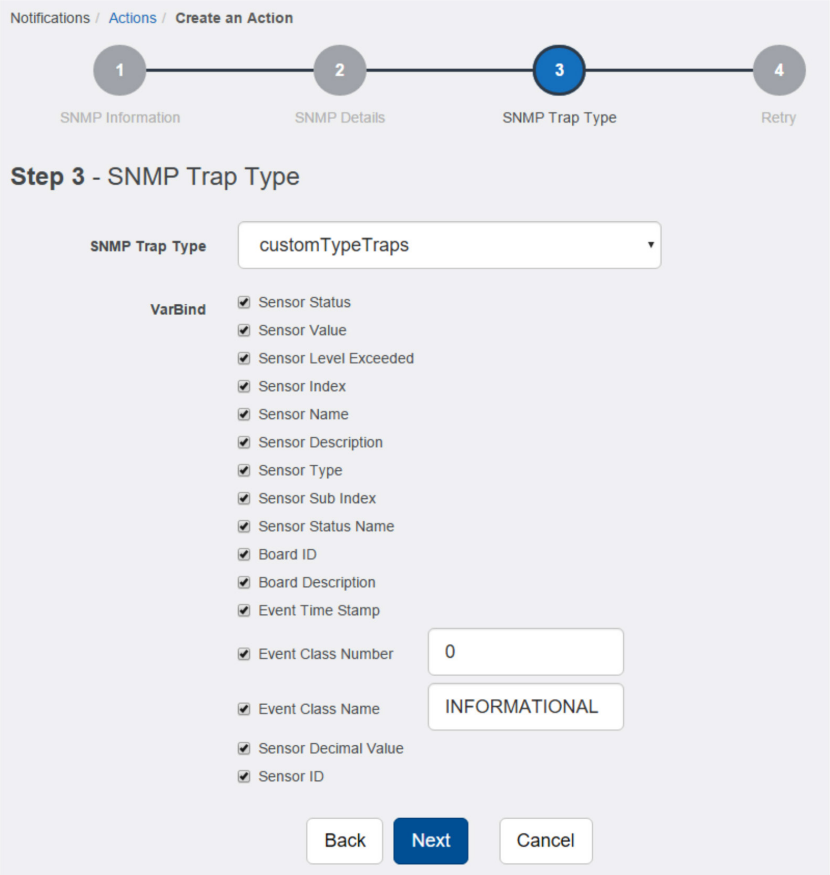

FIGURE 5-40. SNMP TRAP TYPE SCREEN

A different trap message is sent for each sensor type such as temperature, humidity, and switch.

The trap messages include VarBind fields that include the current sensor status (Normal, Critical High, Warning High, Critical Low, Warning Low, and sensorError), the current sensor value, the level exceeded, the sensor index, the sensor name, and the sensor description.

You can enable or disable specific fields if you choose the customTypeTraps from the drop-down list.

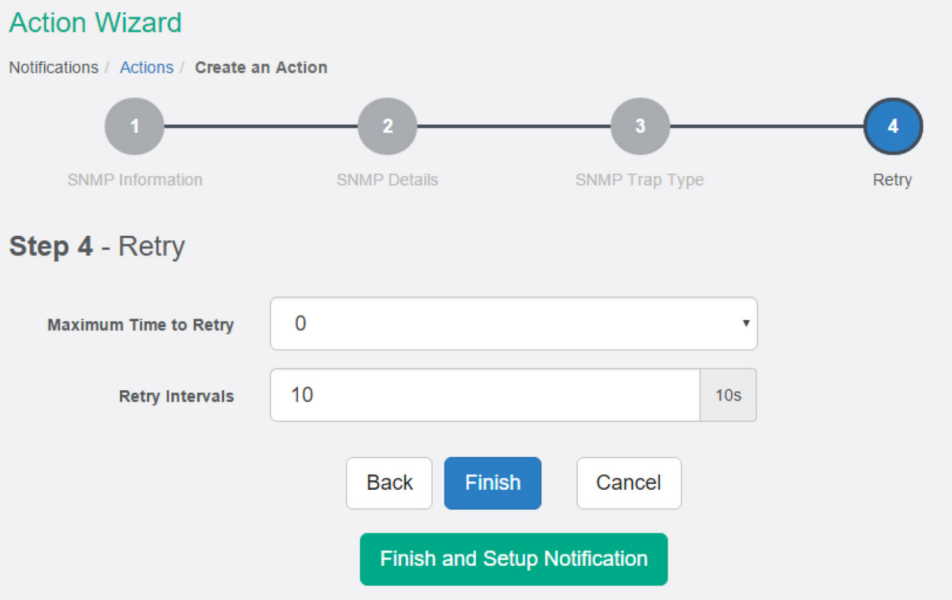

FIGURE 5-41. RETRY SCREEN

These parameters set the maximum number of times to send the trap notification and the time interval between each notification.

If you click on the Finish and Setup Notification button, this will launch the Link Notification Wizard where you can use the new action for making a notification.

5.2.9 TELEPHONE CALL ACTION SETUP

You can use the Telephone Call Action to send custom voice call alerts to your phone when a sensor reaches a certain threshold.

The unit can send an SMS, or Voice alert to many different phone numbers, but you can specify only one phone number per action when setting it up. Keep in mind that both the SMS and the dial up actions such as Voice will call to the first number, then after sending to this number, it will call to the second number and so on. So, if you have many numbers in the call list, it will take that much more time to finish sending the SMS or dial up Voice call alerts.

NOTE: The modem module is needed and must be configured for this action.

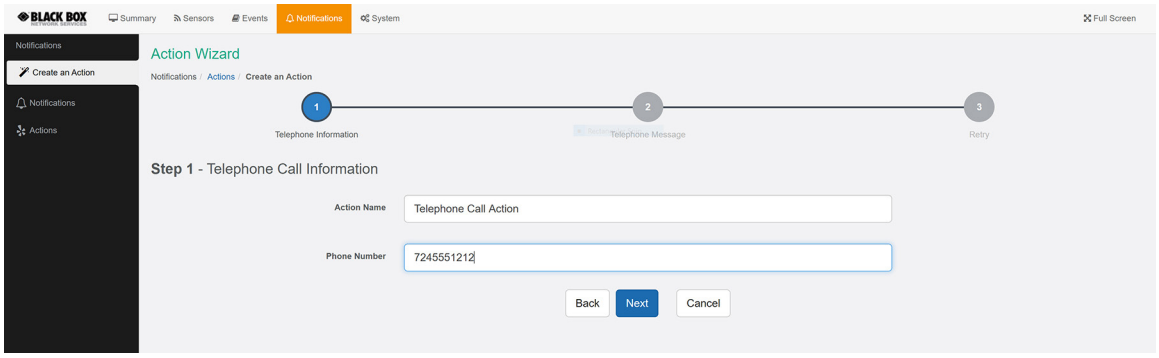

FIGURE 5-42. TELEPHONE CALL INFORMATION SCREEN

After typing in your phone number, click Next.

You can specify only one phone number per action.

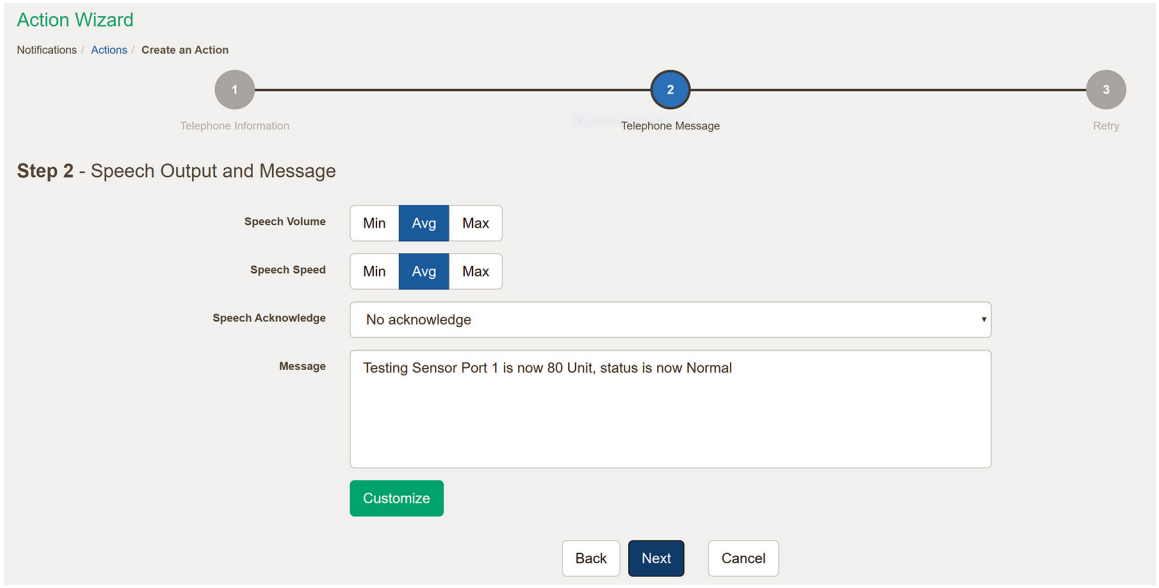

FIGURE 5-43. MESSAGE SCREEN

Now you can select the volume and playback speed for your phone call. The call will be made by using a Text to Speech module.

You can also specify to have the call acknowledged.

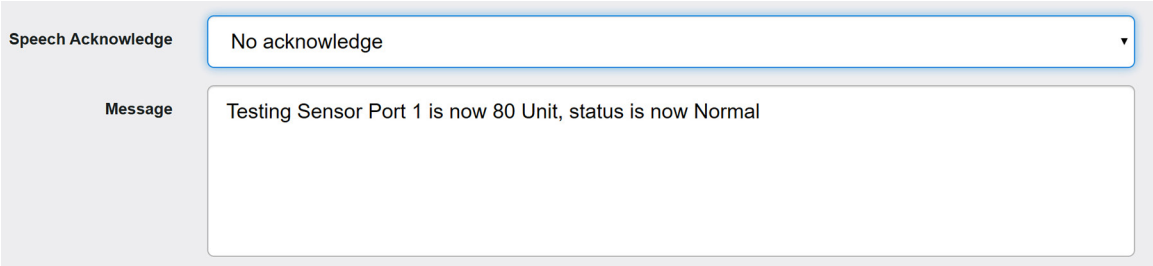

FIGURE 5-44. ACKNOWLEDGEMENT SCREEN

If Speech Acknowledgement is selected, the user will be requested to dial 1 on their phone when prompted in the call to confirm their acknowledgement.

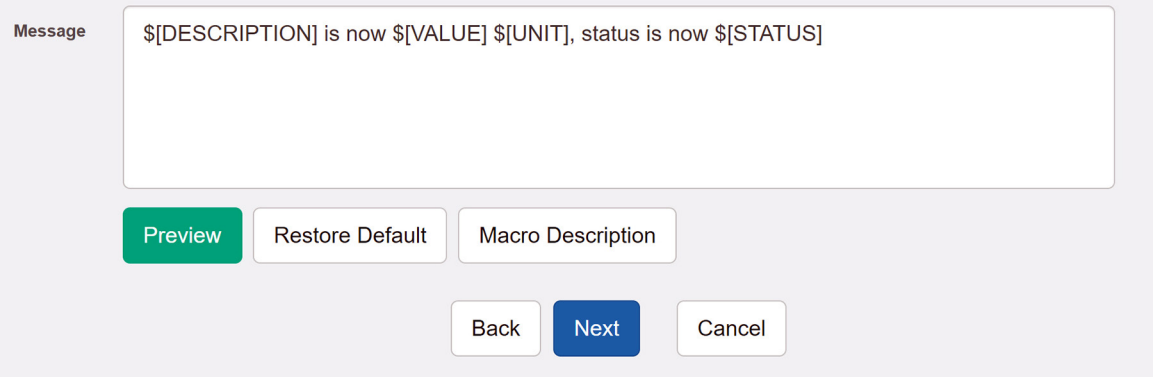

FIGURE 5-45. MESSAGE PREVIEW SCREEN

A preview of the message that will be read is displayed, which you may customize further. The sent message will include the details relevant to your sensor.

For all possible macro values (dynamic text values starting with $), you can see a detailed list in Section 5.7.

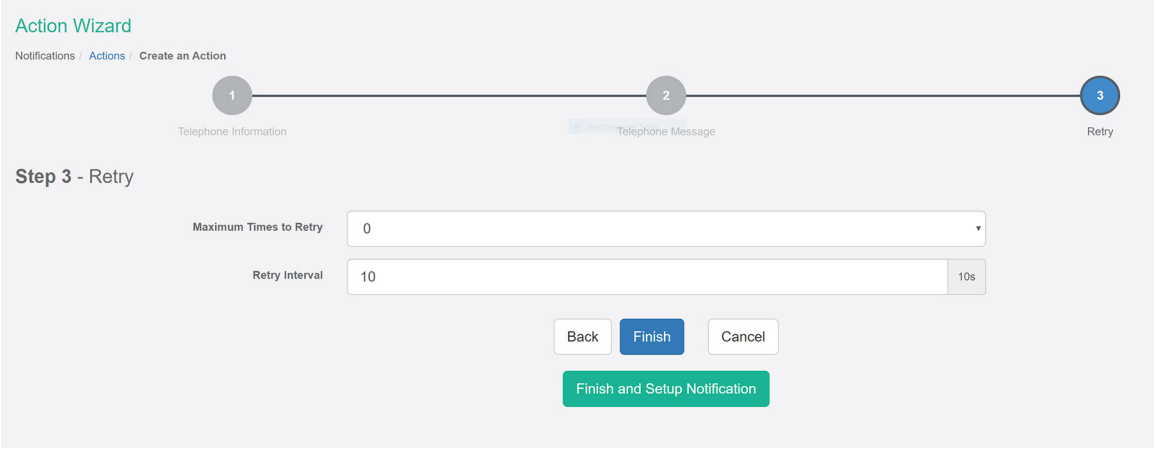

FIGURE 5-46. RETRY SCREEN

These parameters set the maximum number of times to send the call notification and the time interval between each notification.

If you click on the Finish and Setup Notification button, this will launch the Link Notification Wizard where you can use the new action for making a notification.

5.3 EXAMPLE NOTIFICATION SETUP: SMS NOTIFICATION

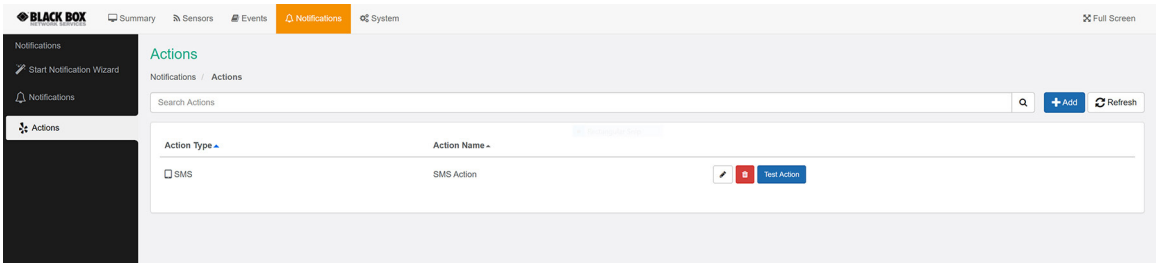

FIGURE 5-47. ACTIONS SCREEN

In our example, we've set up an SMS action and we'll link that to notify us by SMS when the Humidity sensor's value reaches High Critical.

FIGURE 5-48. NOTIFICATIONS SCREEN

On the Notifications menu, we click on Add. This will start the Link Notification Wizard.

You can set up any notification with any action with the same steps as in this example.

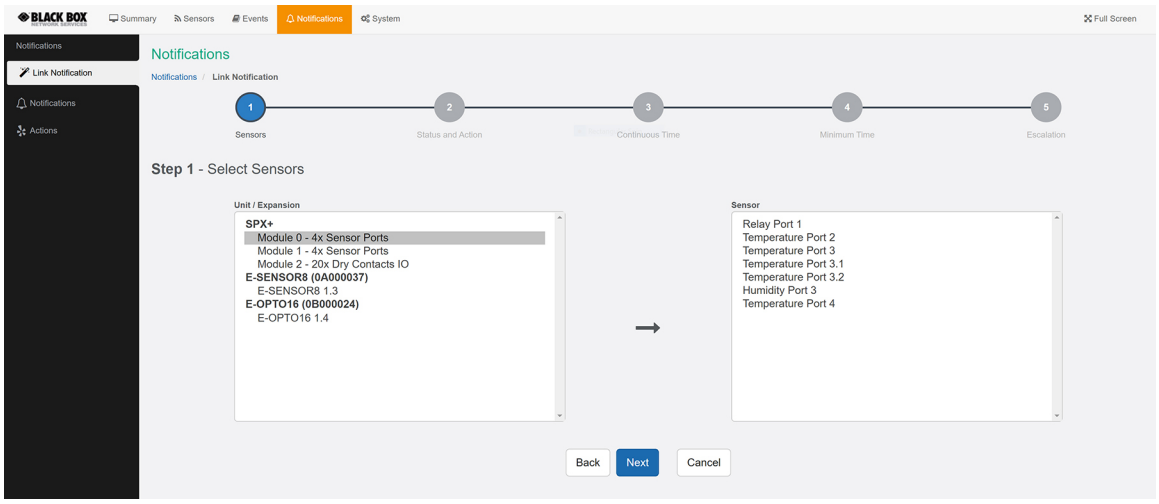

FIGURE 5-49. SELECT SENSORS SCREEN

The first step is to select the sensor that we'll link the notification to. You could also select multiple sensors for a single notification.

NOTE: If you connect an expansion board, you'll be able to select sensors from the expansion board as well, as shown next.

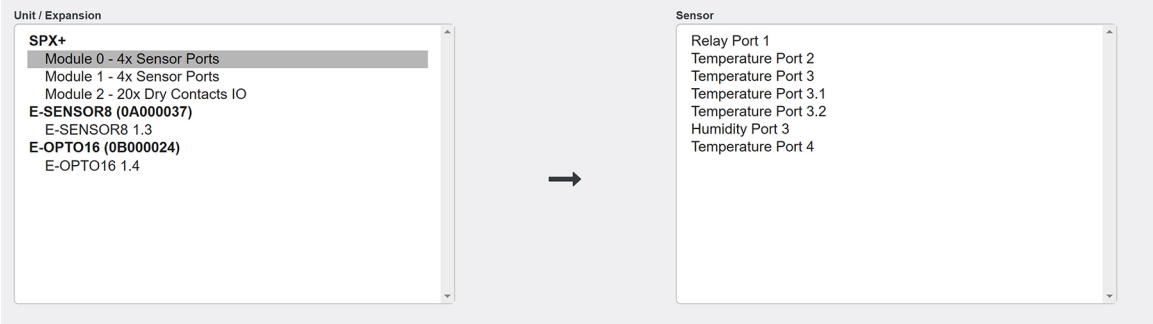

FIGURE 5-50. SELECT SENSORS SCREEN

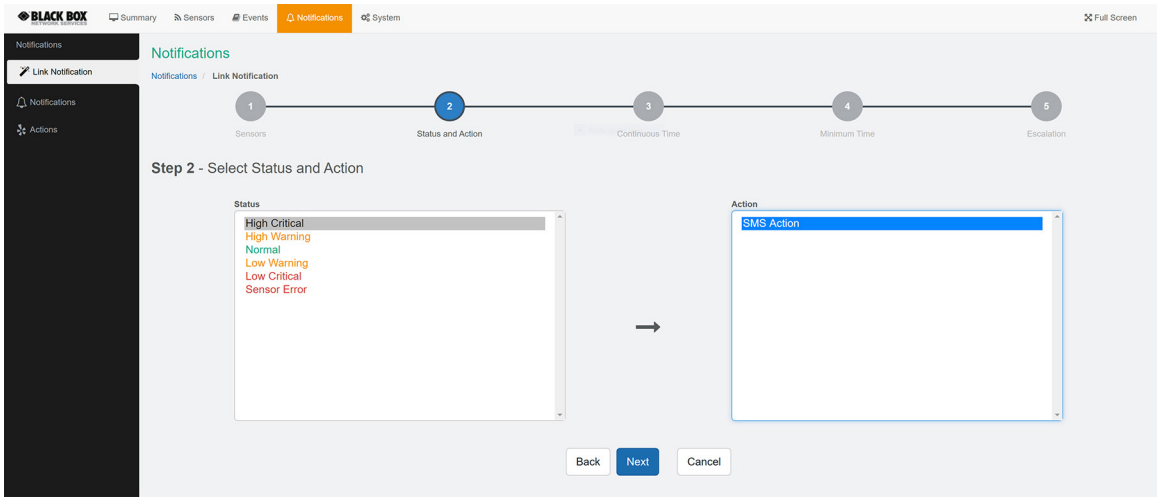

FIGURE 5-51. SELECT STATUS AND ACTION SCREEN

Next, we choose the status High Critical for the sensor, and use the previously created SMS Action. You could also select multiple statuses for a sensor.

NOTE: If you connect an expansion board, you might be able to select special statuses valid only for the expansion board, as shown next.

FIGURE 5-52. SELECT STATUSES SCREEN

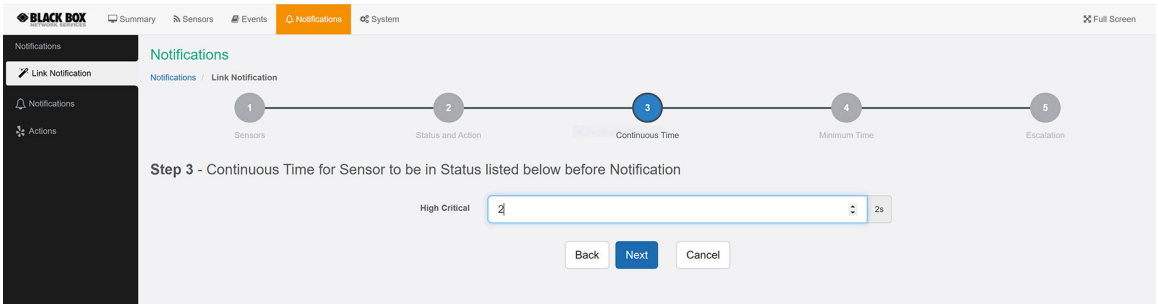

FIGURE 5-53. CONTINUOUS TIME SCREEN

We set the continuous time as 2 seconds — this means the sensor's state has to remain at least 2 seconds in the chosen state before the notification runs.

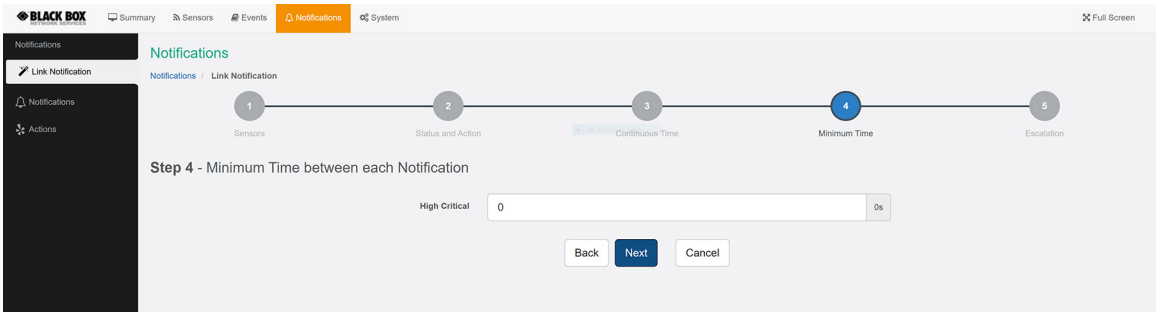

FIGURE 5-54. MINIMUM TIME SCREEN

We don't use a minimum time between notifications (default value).

If you get multiple notifications of the same type, this option could help to reduce the frequency of them.

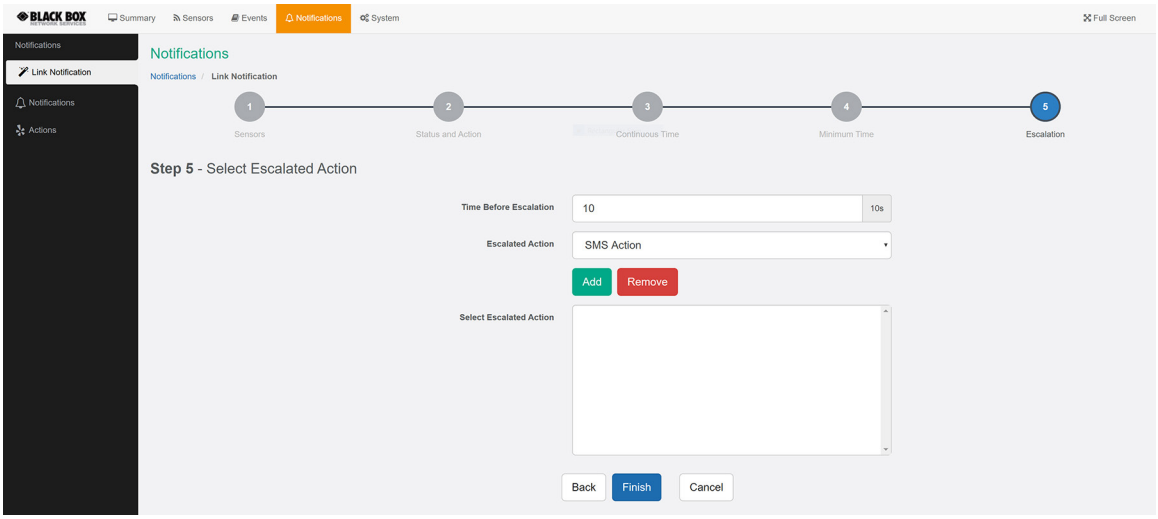

FIGURE 5-55. SELECT ESCALATED ACTION SCREEN

All actions have an option Escalation. With this, you could specify additional actions to run after the initial action, with the specified time.

Use the Add and Remove buttons to add or remove escalated actions.

The maximum number of escalated actions is 10.

NOTE: The additional actions need to be created before you can select them.

In this example, we won't use escalated action.

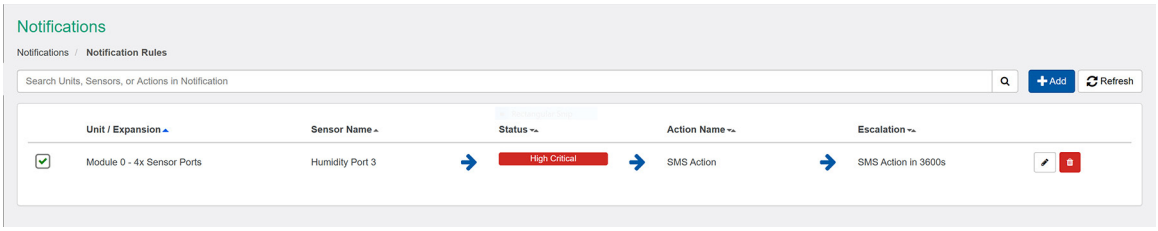

FIGURE 5-56. NOTIFICATION RULES SCREEN

After the wizard has finished, you can view, edit, or remove the completed notification in the Notifications menu.

5.4 HEARTBEAT MESSAGES

This feature allows you to set up periodic "keep alive" notifications tasks by email, SMS, or SNMP Trap to indicate the unit is still working properly.

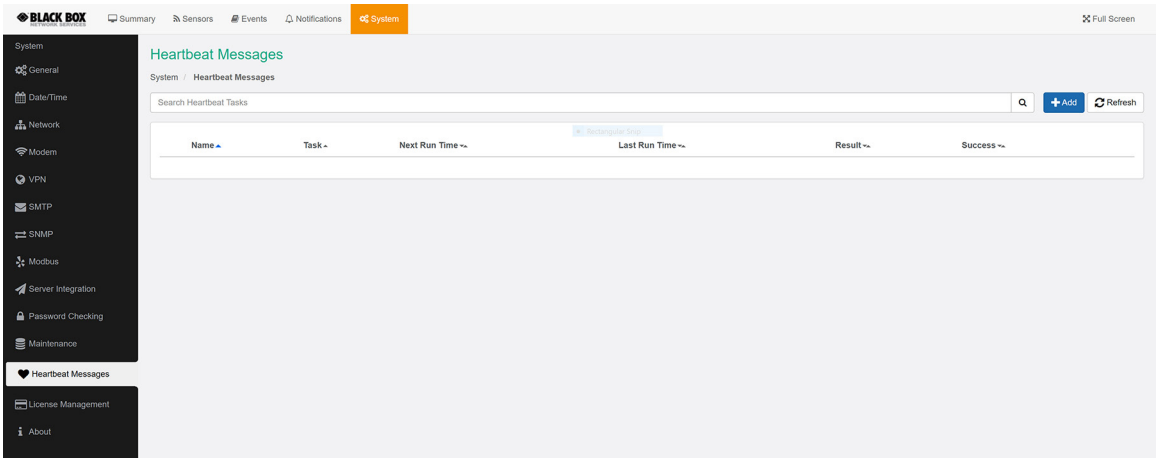

FIGURE 5-57. HEARTBEAT MESSAGES SCREEN

Navigate to System/Heartbeat Messages and click on the Add button to begin the wizard.

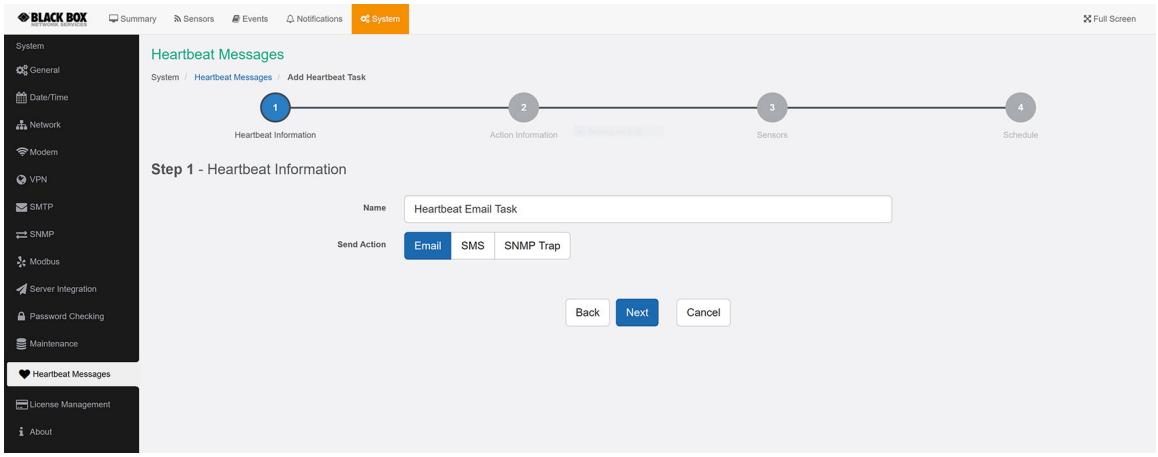

FIGURE 5-58. HEARTBEAT MESSAGES SCREEN

In the first step, you can choose the type of the heartbeat notification, which can be Email, SMS, or SNMP Trap. In our example we'll use Email notification.

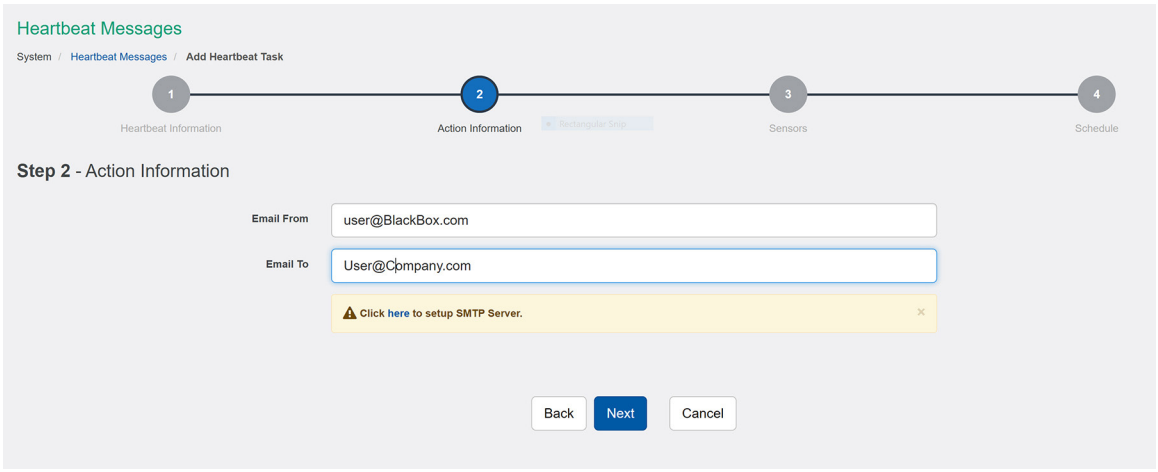

FIGURE 5-59. ACTION INFORMATION SCREEN

Choose the recipients of the action. If you haven't yet set up the SMTP server options, you'll be asked to do so.

If you choose SMS action in the previous step, then you'll need to fill in a phone number here.

For the SNMP Trap, you'll need to specify the SNMP options; see the SNMP Trap Action configuration in this manual for more help.

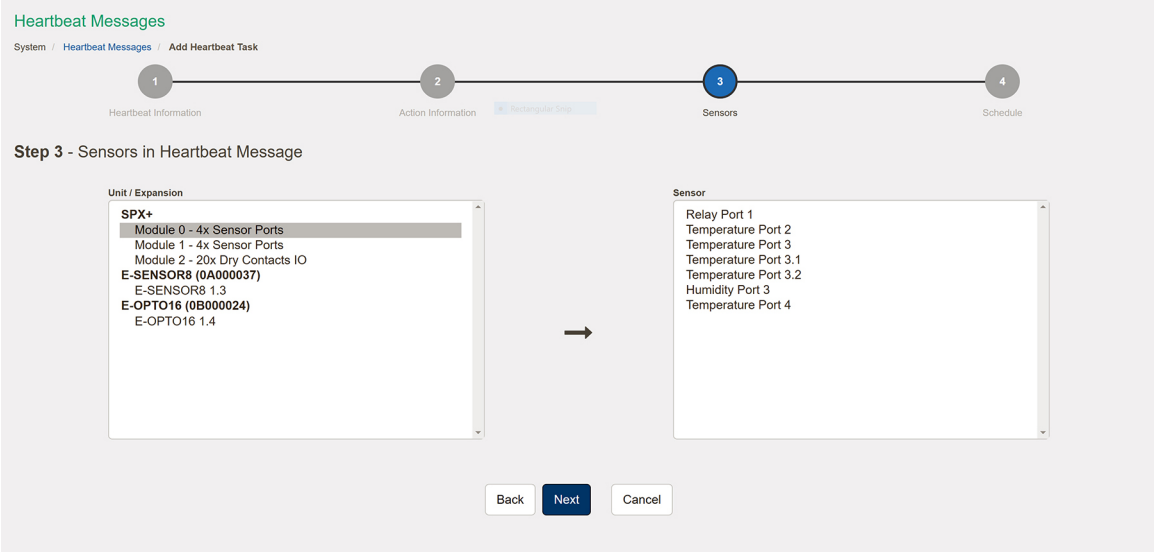

FIGURE 5-60. SENSORS SCREEN

In this step, you can choose one or more sensor's status and reading to include in the heartbeat message. Select at least one sensor.

NOTE: If you connect an expansion board, you'll be able to select sensors from the expansion board also, as shown next.

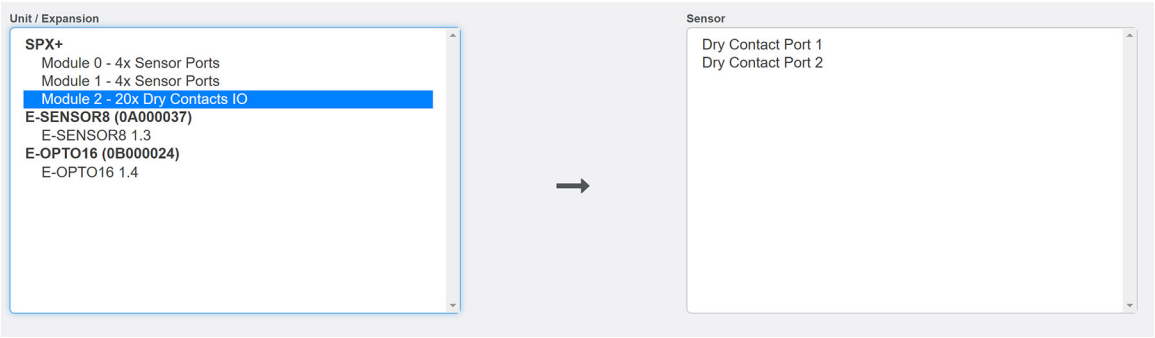

FIGURE 5-61. SELECT SENSORS FROM EXPANSION BOARD SCREEN

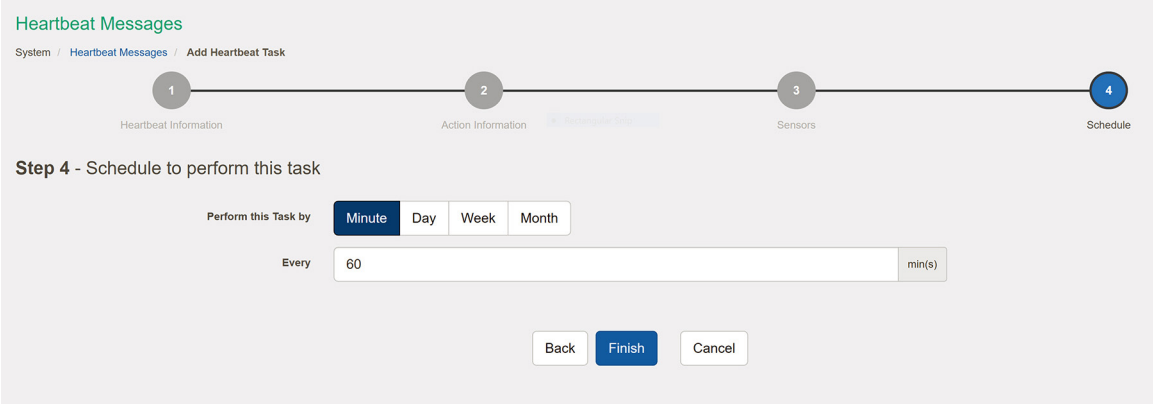

FIGURE 5-62. SCHEDULE TASK BY MINUTE

Finally, choose a schedule for the heartbeat message. This picture shows the by-minute schedule.

You can choose between Minute, Day, Week, Month.

We'll also show the configuration for all of them next.

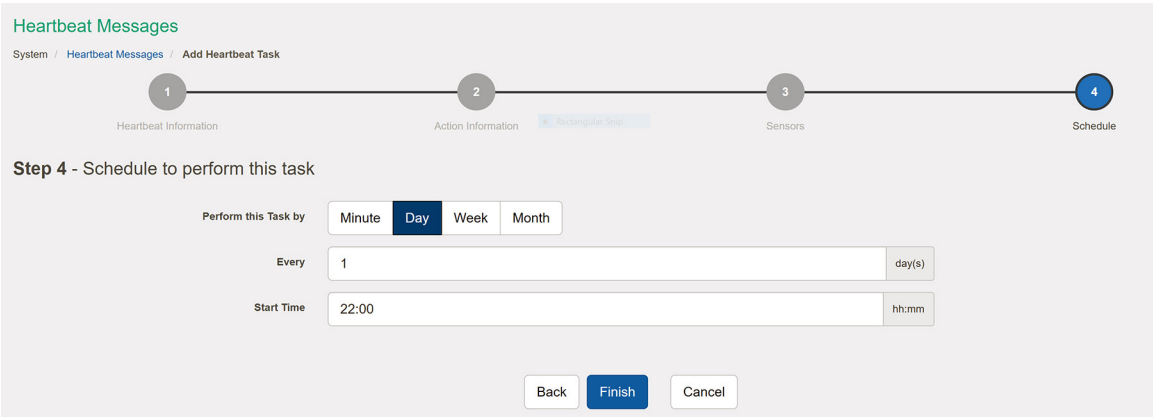

FIGURE 5-63. SCHEDULE TASK BY DAY

This is the by-daily schedule.

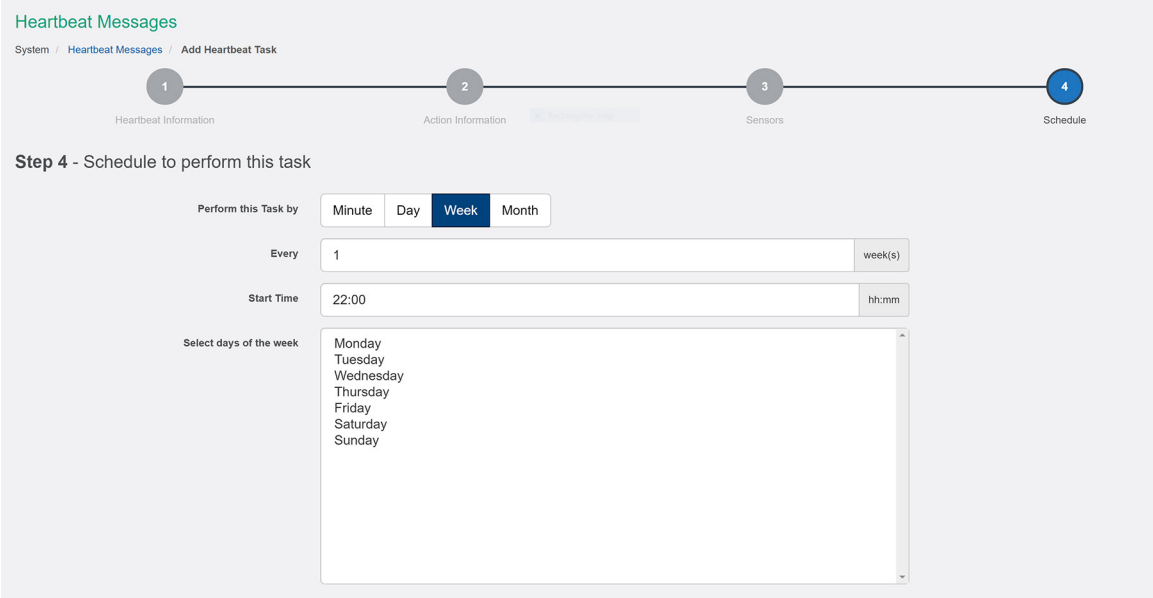

FIGURE 5-64. SCHEDULE TASK BY WEEK

This is the by-weekly schedule.

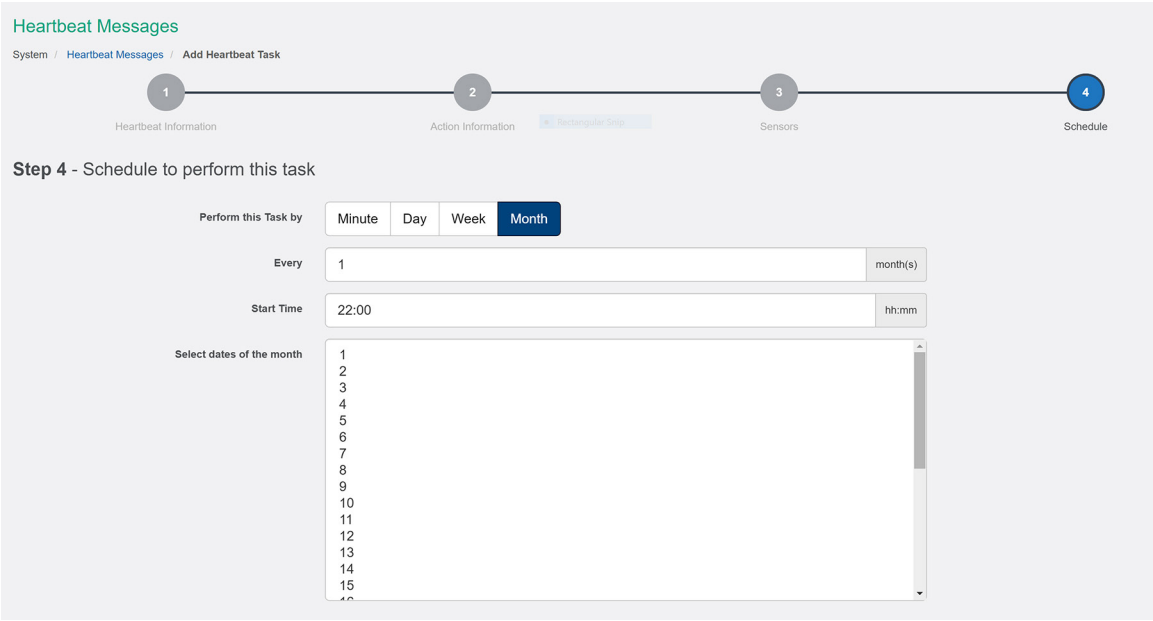

FIGURE 5-65. SCHEDULE TASK BY MONTH

This is the by-monthly schedule.

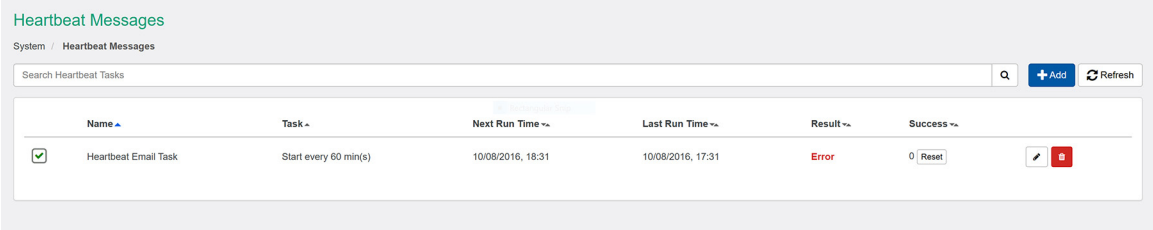

FIGURE 5-66. HEARTBEAT TASK ON LIST

When you've finished the wizard, it will appear in the list.

You can edit or remove the task, and reset the success counter.

NOTE: You can define multiple heartbeat notification tasks with different schedule or notification methods.

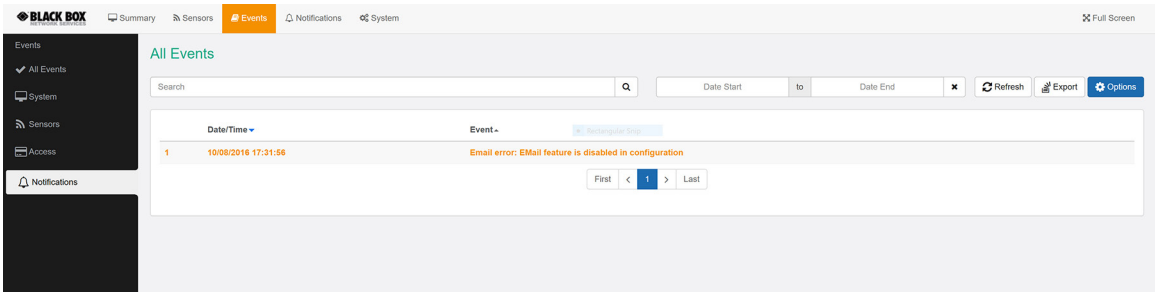

FIGURE 5-67. NOTIFICATIONS RESULT

You can view the result of the notification at the Events page's Notifications section.

5.5 VIRTUAL SENSORS

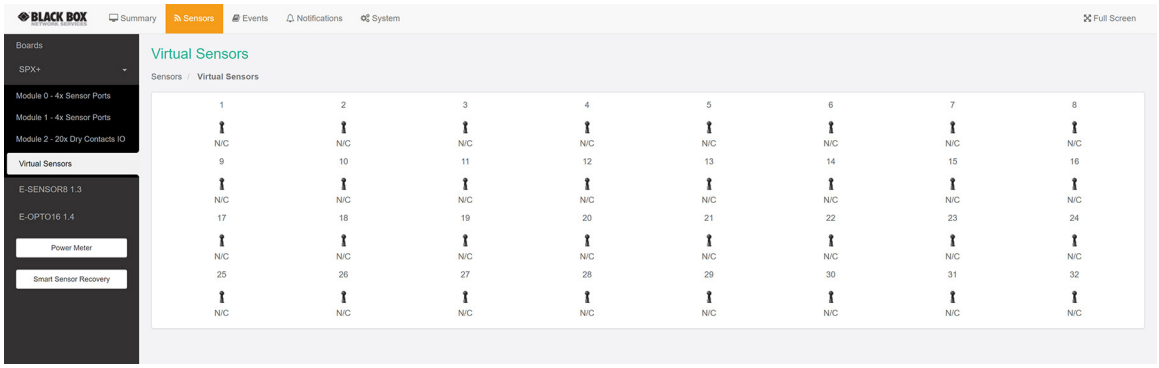

FIGURE 5-68. VIRTUAL SENSORS SCREEN

Virtual Sensors can be a very powerful tool in your monitoring system. On the AlertWerks gateways, you can have up to 32 of these virtual sensors and they allow for a multitude of applications.

SNMP Get, sensor logic evaluation, and ping commands among others are all possible from the virtual sensors. An example use of this could be to use the AlertWerks Gateway as a probe manager. If you had an AlertWerks Gateway and multiple virtual sensors they could all be monitored, mapped and alerted via the gateway. You can perform SNMP Get commands on a server to monitor memory or CPU load, or you can ping network enabled devices and be alerted if they go offline.

You can configure the Virtual Sensors under a separate tab under the Sensors menu.

The first 5 sensors are free; if you need to use more, you can purchase additional licenses.

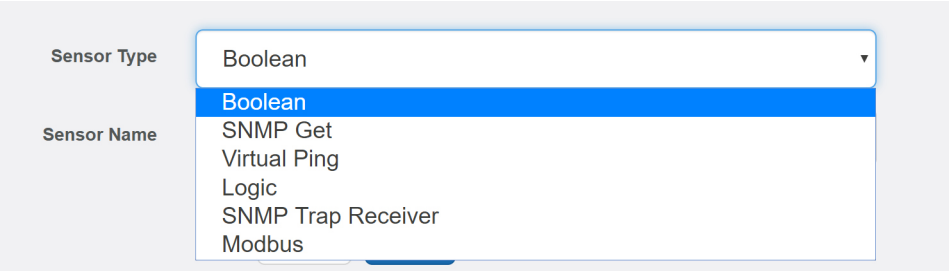

FIGURE 5-69. SENSOR TYPE MENU

Select a sensor from the list, and choose its type.

In the following sections, we'll go through each Virtual Sensor type, and how to configure them.

5.5.1 BOOLEAN

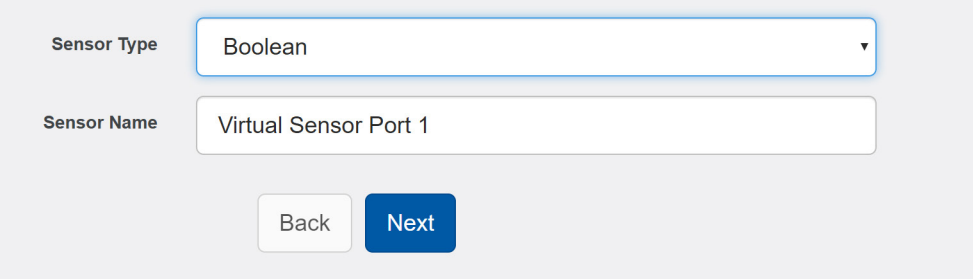

FIGURE 5-70. BOOLEAN VIRTUAL SENSOR

Boolean works on the virtual sensor by checking the status of, for example, 2 to 3 sensors and if the sensors' statuses match that of the setting, they will return a value of 1. The normal value is 0.

You can select the sensor type between AND/OR for comparison:

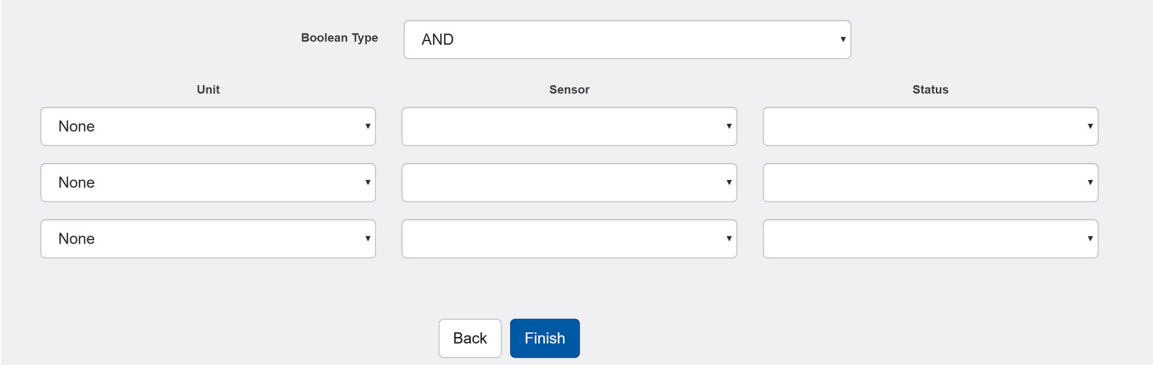

FIGURE 5-71. SELECT AND SENSOR TYPE

You can set your virtual sensor to be critical by choosing your sensors from the drop-down lists, choosing their statuses like the image example shown next, and then go to the Notifications page to make the notification using the new virtual sensor.

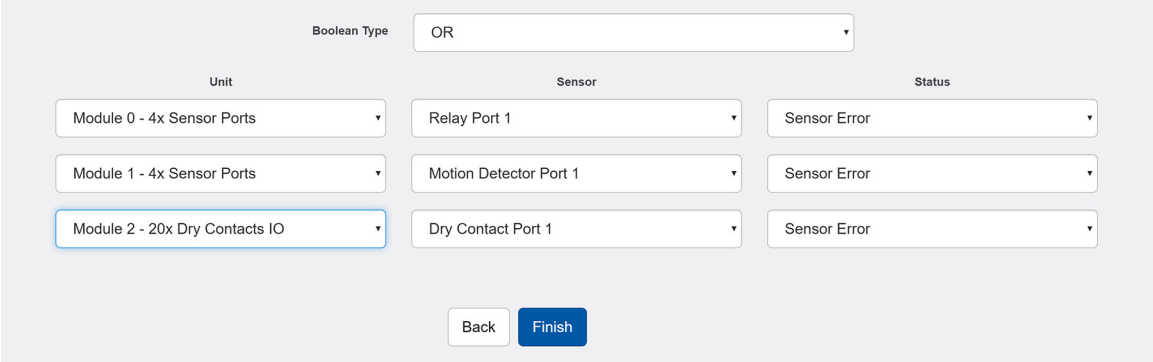

FIGURE 5-72. SELECT OR SENSOR TYPE

In this example picture, the virtual sensor's status will be critical when any of the Humidity/Temperature/Dry Contact sensors will have a high/low/critical status.

NOTE: If you connect an expansion board, you'll be able to select sensors from the expansion board also.

5.5.2 SNMP GET

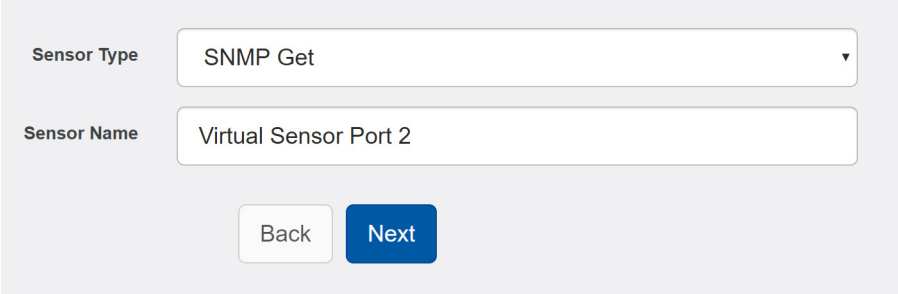

FIGURE 5-73. SNMP GET SENSOR TYPE

With SNMP Get sensor, you can get a value from any SNMP device.

NOTE: A custom string return value is not supported.

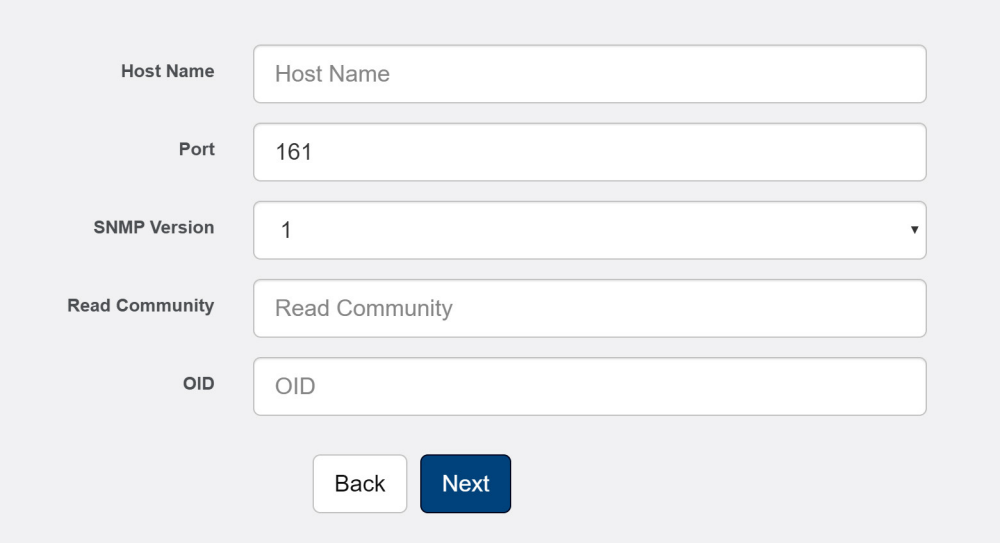

FIGURE 5-74.

Host IP: The IP address of the unit on which you wish to perform an SNMP Get command.

SNMP Version: v1 works with most devices; you can also select v2c and v3.

SNMP Read Community: The SNMP password of the unit, default is usually "public."

OID: The OID for what you wish to monitor. If, for example, you want to poll temperature data from an AlertWerks Gateway with a Temp sensor on Port 1, then you would use the following OID:

1.3.6.1.4.1.3854.1.2.2.1.16.1.3.0

Where the last digit (0) is Port 1. For Port 2 the last digit would be 1. If you are monitoring some other device, you will need the relevant OID for what you wish to measure.

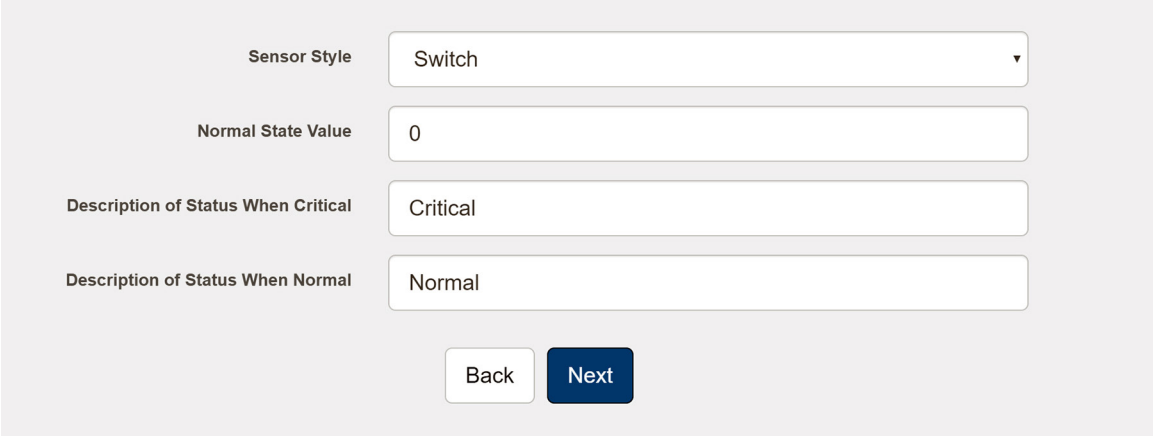

FIGURE 5-75. SWITCH SENSOR STYLE SCREEN

Sensor Style: You can choose either Switch or Analog. A Switch sensor would be, for example, a water sensor, on or off; an Analog sensor would be a Temperature sensor or Humidity sensor, or some other sensor that gives a data value.

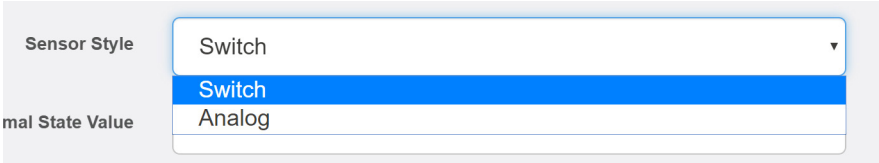

FIGURE 5-76. SENSOR STYLE MENU

Description when Normal: e.g., Normal, Critical, Online etc.

Description when Critical: e.g., Critical, Offline, Low etc.

Normal State value: 0 or 1 (for Switch type sensor only).

If you choose an Analog sensor, you will get a slightly different menu.

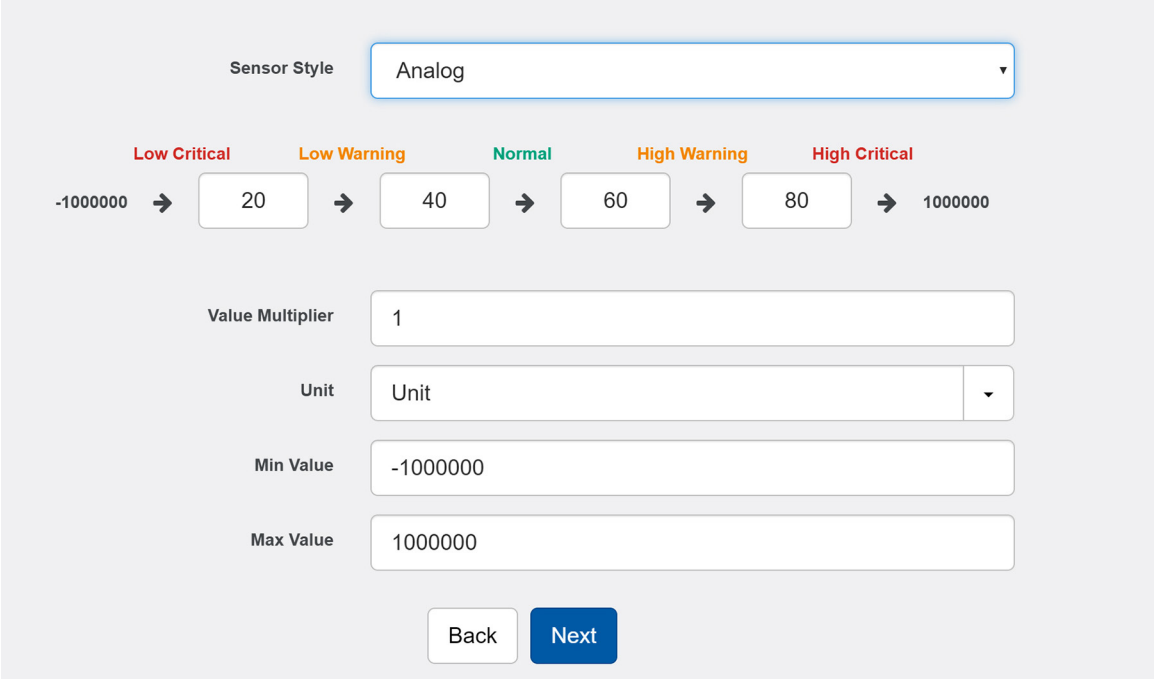

FIGURE 5-77. ANALOG SENSOR STYLE SCREEN

Value Multiplier gives you the choice to multiply the reading value by a given number.

Unit text: example, if measuring temperature “degrees centigrade” or if measuring humidity “percentage humidity” etc.

Value range: The range that you want to measure.

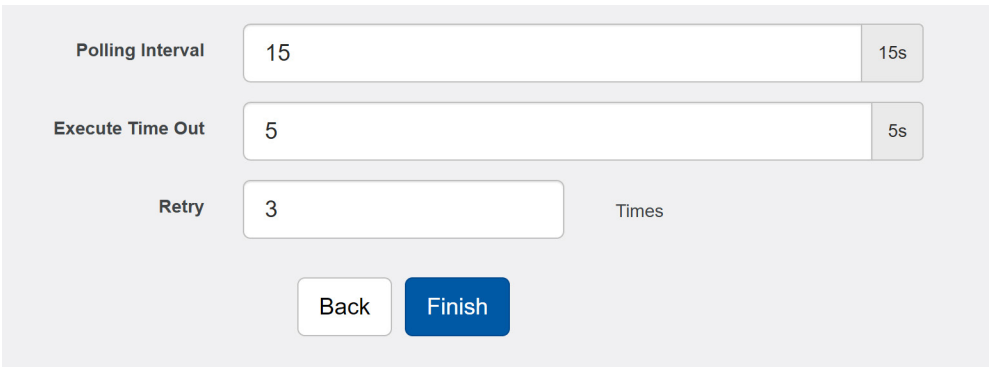

FIGURE 5-78. TIME INTERVAL SCREEN

You can also configure the time interval between data polling, timeout and retries.

5.5.3 VIRTUAL PING

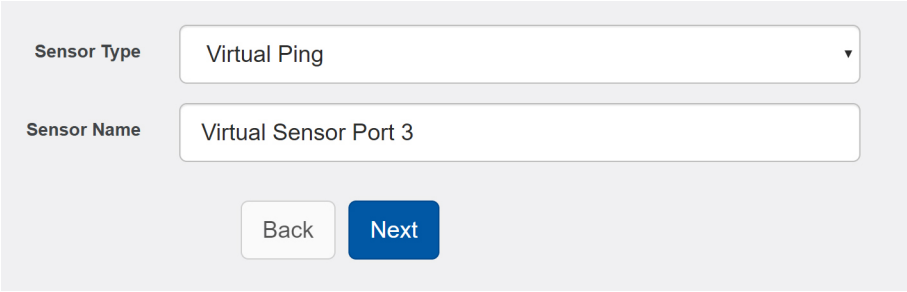

FIGURE 5-79. VIRTUAL PING SCREEN

With the ping sensor, you can set up ping monitoring of a network device or server.

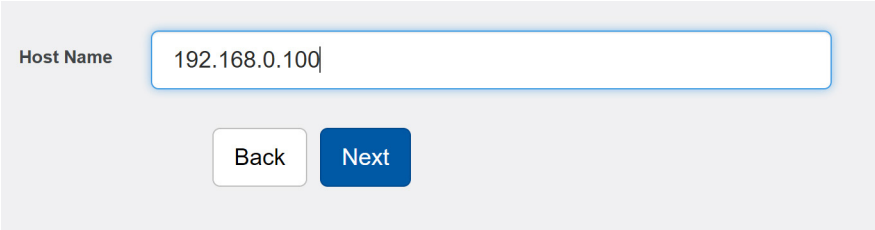

FIGURE 5-80. HOST IP SCREEN

Host: The IP address of the network device you wish to ping.

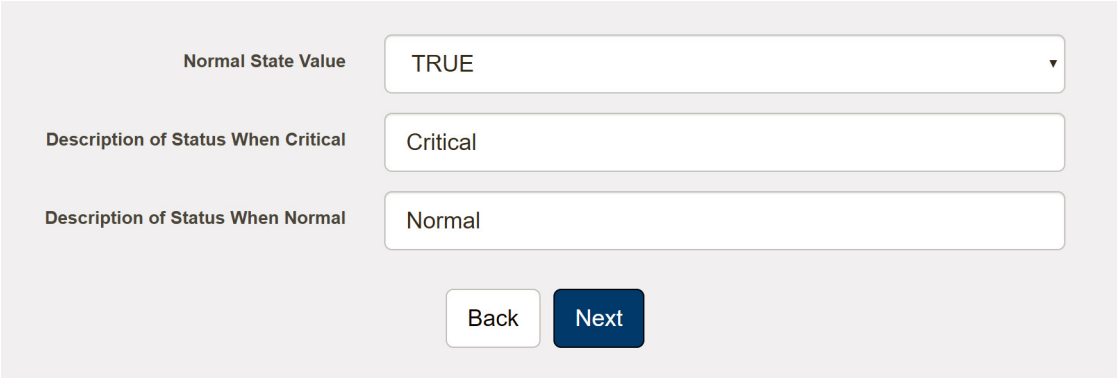

FIGURE 5-81. NORMAL/CRITICAL STATE

Description when Normal: eg, online/reachable

Description when Critical: eg, offline/unreachable

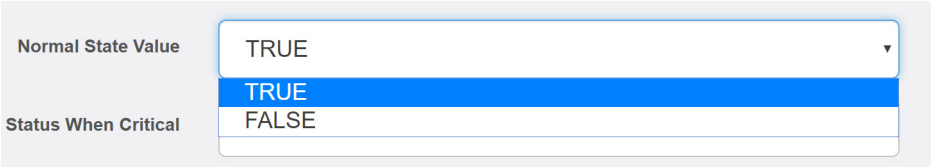

FIGURE 5-82. TRUE/FALSE STATE VALUE

Normal State Value:

TRUE = sensor will be Normal status if ping successful (otherwise it will be in Critical status)

FALSE = sensor will be Normal status if ping times out (otherwise it will be in Critical status)

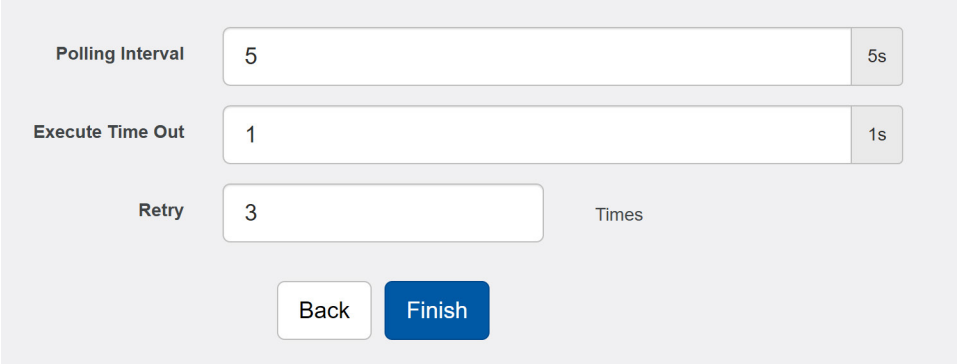

FIGURE 5-83. TIME INTERVAL SCREEN

You can also configure the time interval between data polling, timeout, and retries.

5.5.4 LOGIC

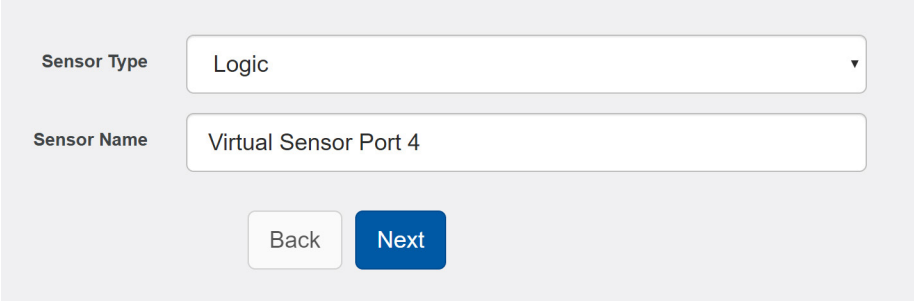

FIGURE 5-84. LOGIC SENSOR TYPE SCREEN

The logic is a virtual sensor type that uses FlipFlop logic. You can monitor physical sensor statuses with it, and change the virtual sensor's state with the pre-set values for the status of a physical sensor (SET Source Sensor).

The logic will ignore all other intermediate physical sensor statuses and only changes the virtual sensor's state back if it exactly matches the specified physical sensor status (RESET Source Sensor).

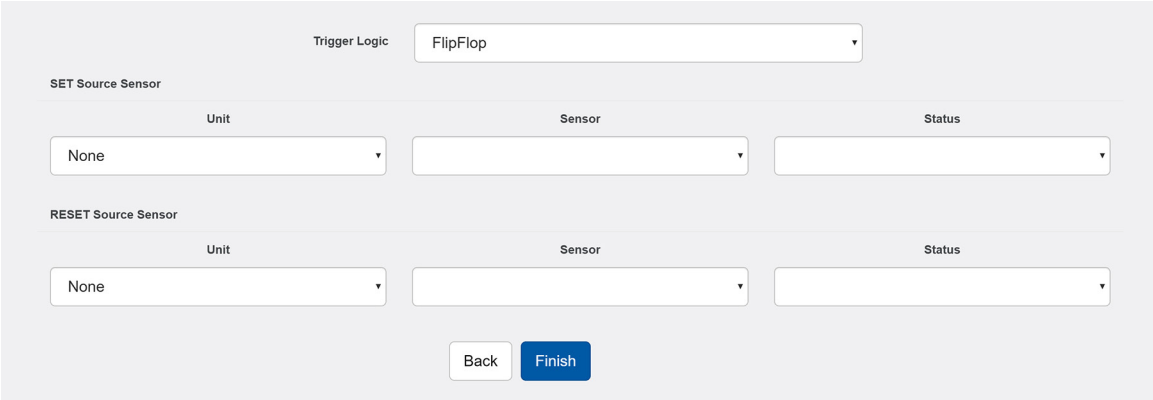

FIGURE 5-85. FLIPFLOP LOGIC SCREEN

Choose your unit, physical sensor, and the status you'd like the logic to monitor.

NOTE: If you connect an expansion board, you'll be able to select sensors from the expansion board also.

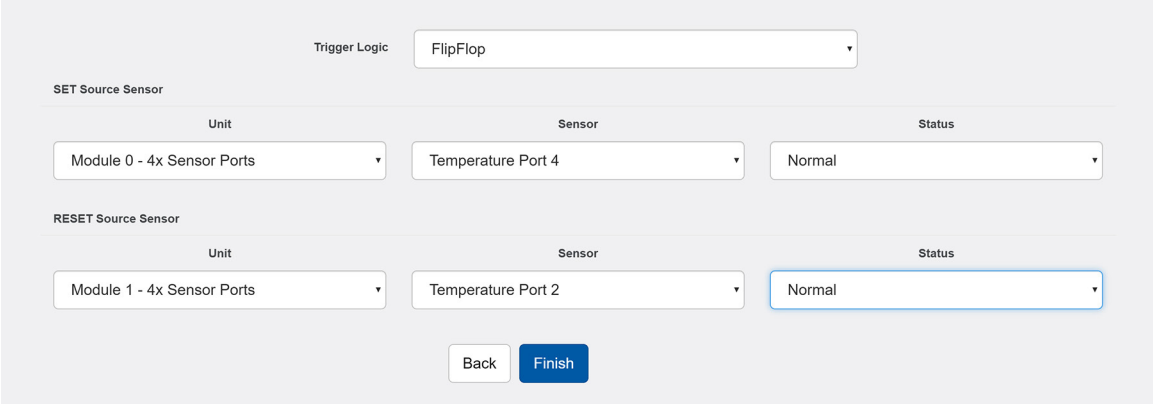

FIGURE 5-86. FLIPFLOP LOGIC EXAMPLE

On this example picture, we've set the logic to change the virtual sensor to Critical if the Temperature sensor's status becomes High Critical, and only change it back to Normal when the Temperature sensor's status also becomes Normal.

There's also support for Dual Sensors FlipFlop logic.

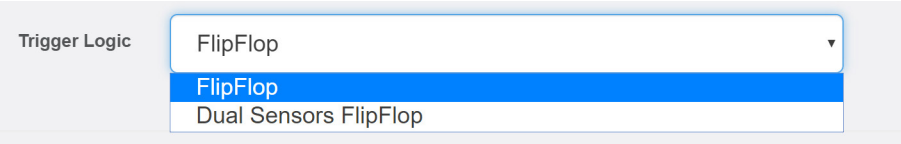

FIGURE 5-87. TRIGGER LOGIC MENU

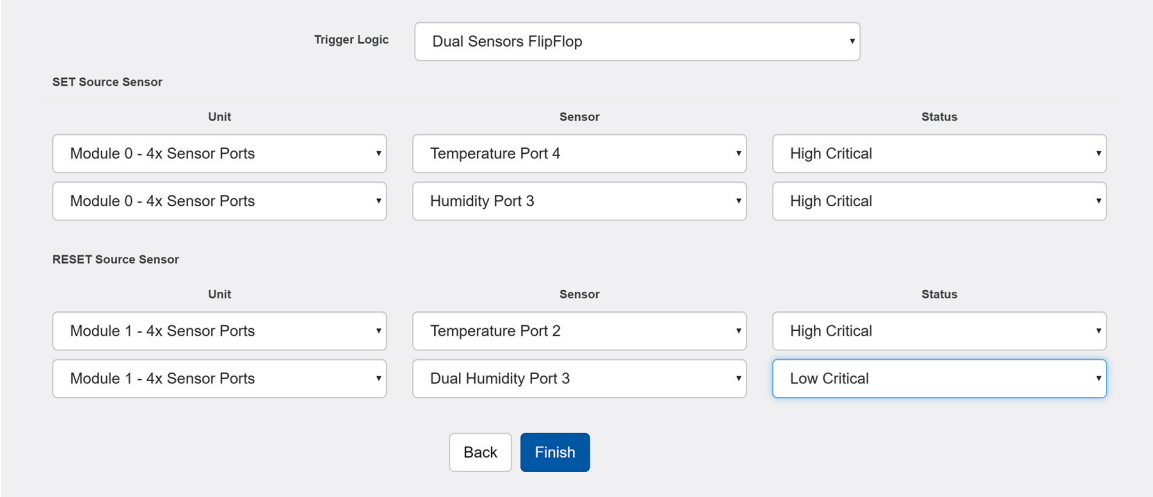

FIGURE 5-88. DUAL SENSORS FLIPFLOP LOGIC EXAMPLE

In this mode, you can choose two sensors for monitoring.

It has AND relation between them, and only changes the virtual sensor's state if there's an exact match for these statuses.

5.5.5 SNMP TRAP RECEIVER

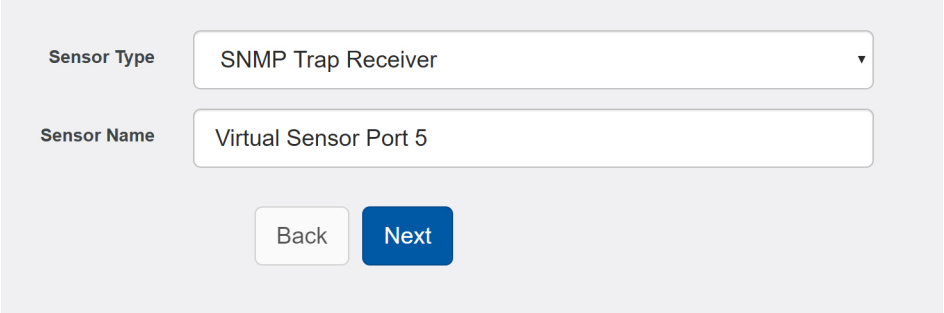

FIGURE 5-89. SNMP TRAP RECEIVER SCREEN

The SNMP Trap Receiver type will check three parameters before setting a value for the virtual sensor.

These three parameters are the IP Address, the sensor's OID, and the Trap sub-type.

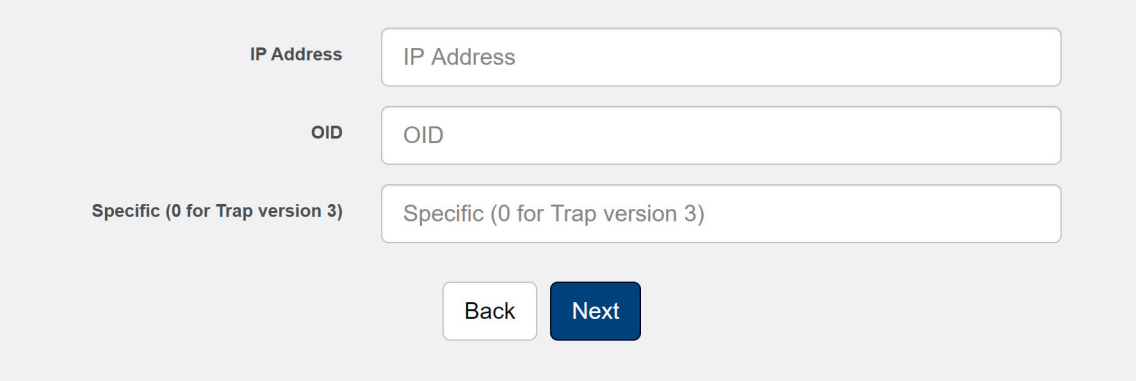

FIGURE 5-90. SNMP TRAP RECEIVER PARAMETERS

Normally the Trap will have six OIDs, you can specify the specific OID from them with the Specific option.

Example:

In our example shown next, the Trap is sent by the Motion Sensor on Port 5 of our sensorProbe unit. Our device IP is 192.168.0.100. Our hub Trap Type is set to the specific sub type and will check status of our Motion Sensor.

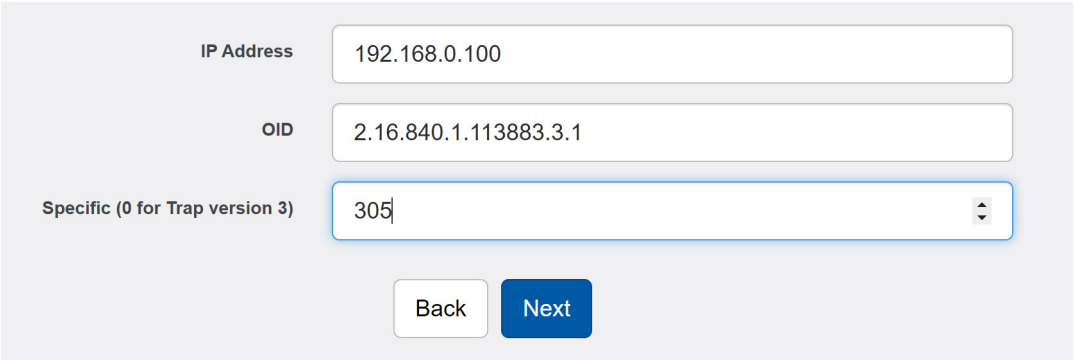

FIGURE 5-91. SNMP TRAP EXAMPLE

1. spSensorStatus (.1.3.6.1.4.1.3854.1.7.1.0). The current integer status of the sensor causing this trap to be sent: noStatus(1), normal(2), highWarning(3), highCritical(4), lowWarning(5), lowCritical(6), sensorError(7), turnOn(8), turnOff(9).
2. spSensorValue (.1.3.6.1.4.1.3854.1.7.2.0). The current integer value of the sensor causing this trap to be sent.
3. spSensorLevelExceeded (.1.3.6.1.4.1.3854.1.7.3.0). The integer level that was exceeded causing this trap to be sent.
4. spSensorIndex (.1.3.6.1.4.1.3854.1.7.4.0). The integer index of the sensor causing this trap to be sent.
5. spSensorName (.1.3.6.1.4.1.3854.1.7.5.0). The name of the sensor causing this trap to be sent.
6. spSensorDescription (.1.3.6.1.4.1.3854.1.7.6.0). The description of the sensor causing this trap to be sent.

The specific value depends on the sensorProbeTrap type (.1.3.6.1.4.1.3854.1.2.2.1.60.0).

If it is set to specificTypeTrap(1), specific value is to show the sensor type and port (Specific value of Motion Sensor port 5 is 305).

If it is set to generalTypeTrap(2), specific value is to show the sensor type (Specific value of Motion Sensor port 5 is 30).

If it is set to bothTypeTraps(3), device will send the trap two times, specific value will show sensor type and show sensor type and port (Specific value of Motion Sensor port 5 is 305 and 30).

If it is set to statusTypeTraps(4), specific value is up to status of sensor (spSenUnknownStatus(51), spSenNoemalStatus(52), spSenWarningStatus(53), spSenCriticalStatus(54)).

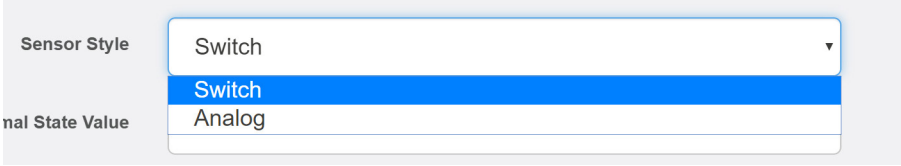

FIGURE 5-92. SELECT SWITCH SENSOR STYLE

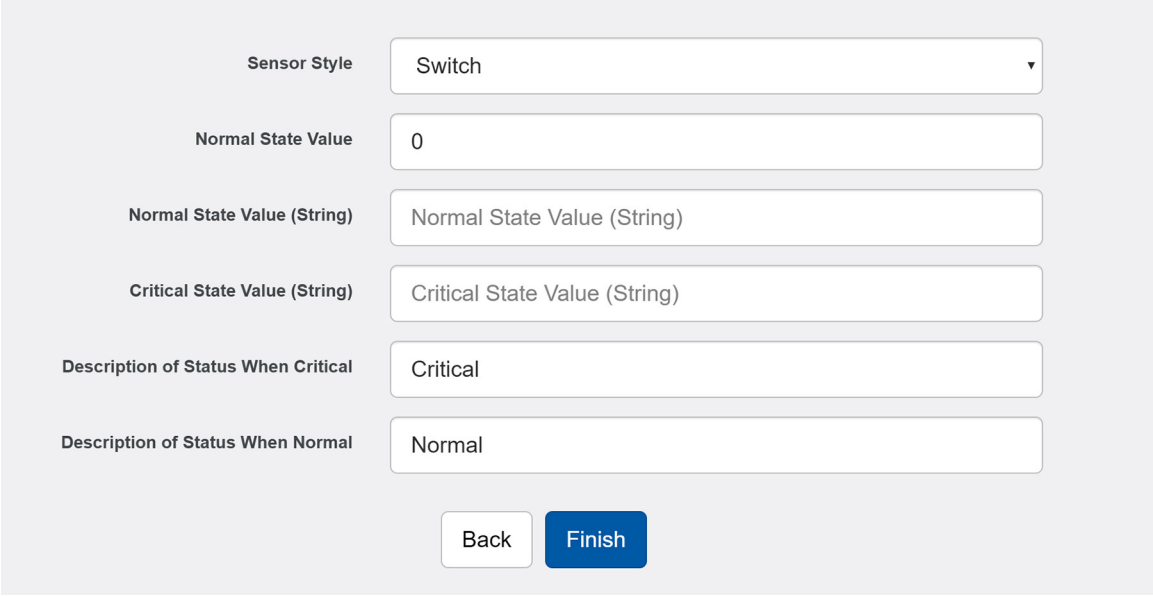

FIGURE 5-93. SWITCH SENSOR STYLE

With the Switch Sensor Style you'll need to specify the Normal State Value. Value 2 means that the sensor's status is normal so far.

If you choose an Analog sensor style, you will get a slightly different menu.

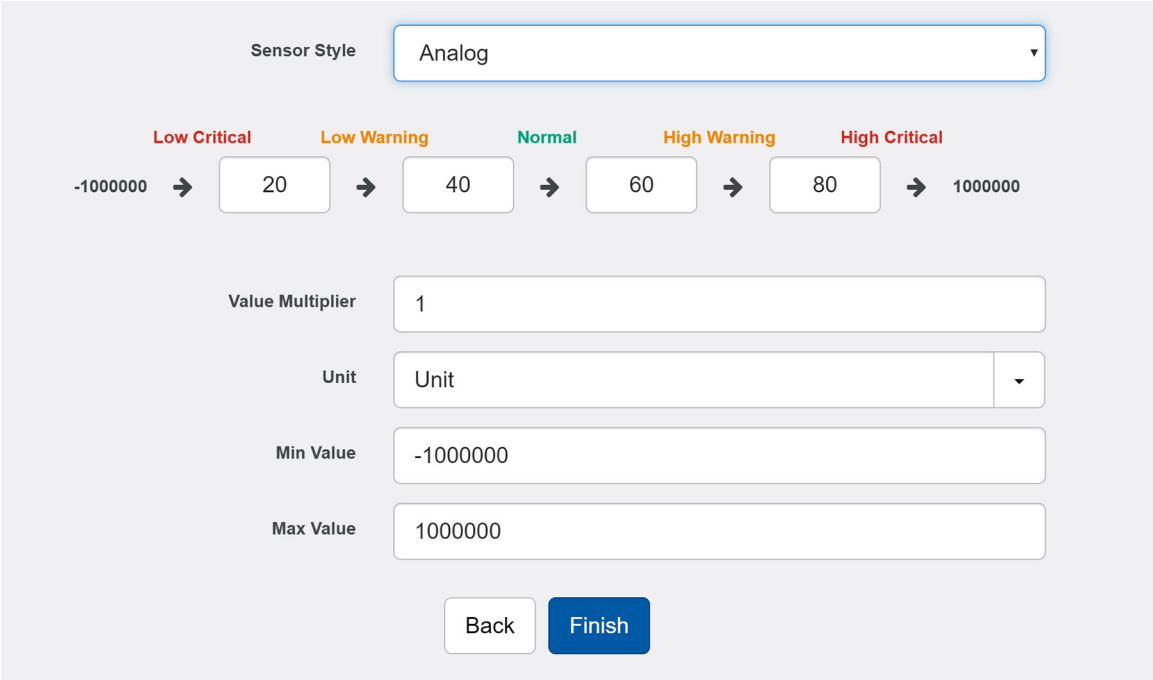

FIGURE 5-94. ANALOG SENSOR STYLE

The configuration values are similar to other analog type sensors.

5.6 MACRO DESCRIPTION FOR ACTIONS

Macro Name	Description
$[SYSNAME]	System name.
$[SYSLOCATION]	System location.
$[SYSCONTACT]	System contact.
$[SYSURL]	System URL.
$[IP]	The IP address of this system.
$[IP_ETH]	The IP address of ethernet interface.
$[IP_VPN]	The IP address of VPN interface.
$[TIME]	The time when a sensor transmits the notification in the format of HH:MM:SS Ex: 18:45:10.
$[DATE]	The date when the sensor transmits the notification in the format of YYYY/MM/DD Ex: 2005/01/31.
$[DAY_OF_WEEK]	The day of the week when the sensor transmits the notification. Ex: Monday, Tuesday, etc.
$[DAY]	The date of the month when the sensor transmits the notification. Ex: 1,2,3,...
$[MONTH]	The month when the sensor transmits the notification. Ex: January, February, etc.
$[YEAR]	The year when the sensor transmits the notification. Ex: 2014.
$[PORT]	The port number when the sensor transmits the notification. Ex: 2.
$[DESCRIPTION]	The description to identify the reporting sensor transmitting the notification. Ex: Temperature of computer room.
$[STATUS]	The status of the sensor transmitting the notification. Ex: High Critical.
$[VALUE]	The current reading of the sensor when a notification occurs. Ex: 40 Percent, 20 Volts, etc.
$[UNIT]	The unit of the sensor. Ex: Percent, Volts, etc.

FIGURE 5-95. MACRO HELP WINDOW

NOTE: This macro help window is also available from the Web UI when you click on the Macro Description button.

CHAPTER 6: TROUBLESHOOTING

I am having problems with the unit but not sure what to do next?

Contact Black Box Technical Support at 877-877-2269 or techsupport@blackbox.com

Please provide the following detailed information.

NOTE: The more details you can provide the easier and faster we can provide you with a resolution, so please be as detailed as possible.

1. The details of the problem, condition of the LEDs, etc.
2. What you did to determine the unit has this problem?
3. Was there anything done to the unit prior to having the problem?
4. Did the unit always have this problem, if not when did this start?
5. Do you have more than one unit having the same problem?
6. What did you do to try and fix the problem?
7. What version of firmware is running on the unit? Did you try and upgrade it?
8. Include the settings and backup configuration files to support (both files).
9. If you can put the unit online this would be the fastest way for us to solve the problem.
10. What is the MAC ID of the unit?

Contact Black Box Technical Support at 877-877-2269 or techsupport@blackbox.com if you have any further technical questions or problems.

APPENDIX A: EME160A-UC

EME160A units are shipped with two RJ-45 sensors ports unlocked. The remaining two sensors ports will be LOCKED and unusable unless the EME160A-UC is purchased.

The EME160A is field upgradable with the EME160A-UC unlock code. To unlock the ports your units MAC ID must be provided.

Contact Black Box Technical Support at 877-877-2269 or techsupport@blackbox.com if you have any further technical questions or problems.

APPENDIX B: REGULATORY INFORMATION

B.1 FCC STATEMENT

Class B Digital Device. This equipment has been tested and found to comply with the limits for a Class B computing device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation. This equipment generates, uses, and can radiate radio frequency energy, and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. If this equipment does cause harmful interference to radio or telephone reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

Reorient or relocate the receiving antenna.

- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult an experienced radio/TV technician for help.

CAUTION:

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

To meet FCC requirements, shielded cables and power cords are required to connect this device to a personal computer or other Class B certified device.

This digital apparatus does not exceed the Class B limits for radio noise emission from digital apparatus set out in the Radio Interference Regulation of Industry Canada.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de classe B prescrites dans le Règlement sur le brouillage radioélectrique publié par Industrie Canada.

APPENDIX B: REGULATORY INFORMATION

B.2 NOM STATEMENT

1. Todas las instrucciones de seguridad y operación deberán ser leídas antes de que el aparato eléctrico sea operado.
2. Las instrucciones de seguridad y operación deberán ser guardadas para referencia futura.
3. Todas las advertencias en el aparato eléctrico y en sus instrucciones de operación deben ser respetadas.
4. Todas las instrucciones de operación y uso deben ser seguidas.
5. El aparato eléctrico no deberá ser usado cerca del agua—por ejemplo, cerca de la tina de baño, lavabo, sótano mojado o cerca de una alberca, etc.
6. El aparato eléctrico debe ser usado únicamente con carritos o pedestales que sean recomendados por el fabricante.
7. El aparato eléctrico debe ser montado a la pared o al techo sólo como sea recomendado por el fabricante.
8. Servicio—El usuario no debe intentar dar servicio al equipo eléctrico más allá a lo descrito en las instrucciones de operación. Todo otro servicio deberá ser referido a personal de servicio calificado.
9. El aparato eléctrico debe ser situado de tal manera que su posición no interfiera su uso. La colocación del aparato eléctrico sobre una cama, sofá, alfombra o superficie similar puede bloquea la ventilación, no se debe colocar en libreros o gabinetes que impidan el flujo de aire por los orificios de ventilación.
10. El equipo eléctrico deber ser situado fuera del alcance de fuentes de calor como radiadores, registros de calor, estufas u otros aparatos (incluyendo amplificadores) que producen calor.
11. El aparato eléctrico deberá ser connectado a una fuente de poder sólo del tipo descrito en el instructivo de operación, o como se indique en el aparato.
12. Precaución debe ser tomada de tal manera que la tierra fisica y la polarización del equipo no sea eliminada.
13. Los cables de la fuente de poder deben ser guiados de tal manera que no sean pisados ni pellizcados por objetos colocados sobre o contra ellos, poniendo particular atención a los contactos y receptáculos donde salen del aparato.
14. El equipo eléctrico debe ser limpiado únicamente de acuerdo a las recomendaciones del fabricante.
15. En caso de existir, una antena externa deberá ser localizada lejos de las lineas de energia.
16. El cable de corriente deberá ser desconectado del cuando el equipo no sea usado por un largo periodo de tiempo.
17. Cuidado debe ser tomado de tal manera que objectos liquidos no sean derramados sobre la cubierta u orificios de ventilación.
18. Servicio por personal calificado deberá ser provisto cuando:
    - A: El cable de poder o el contacto ha sido dañado; u
    - B: Objectos han caído o líquido ha sido derramado dentro del aparato; o
    - C: El aparato ha sido expuesto a la lluvia; o
    - D: El aparato parece no operar normalmente o muestra un cambio en su desempeño; o
    - E: El aparato ha sido tirado o su cubierta ha sido dañada.

APPENDIX C: DISCLAIMER/TRADEMARKS

C.1 DISCLAIMER

Black Box Corporation shall not be liable for damages of any kind, including, but not limited to, punitive, consequential or cost of cover damages, resulting from any errors in the product information or specifications set forth in this document and Black Box Corporation may revise this document at any time without notice.

C.2 TRADEMARKS USED IN THIS MANUAL

Black Box and the Black Box logo type and mark are registered trademarks of Black Box Corporation.

Any other trademarks mentioned in this manual are acknowledged to be the property of the trademark owners.

NEED HELP?
LEAVE THE TECH TO US

LIVE 24/7 TECHNICAL SUPPORT

1.877.877.2269

BLACK BOX®