MONNIT®
Remote Monitoring for Business

PoE•X Open / Close Sensor
USER GUIDE

TABLE OF CONTENTS

I. ABOUT THE PoE•X OPEN/CLOSE SENSOR

The Power-over-Ethernet (PoE) Open/Close Sensor uses an external magnetic switch to detect the presence or removal of a trigger magnet. When the sensor detects that the magnet is removed or returned it sends the information to iMonnit. Notifications can be set up through the online system to alert the user when a magnetic source is present or not with the ability to only notify within time of day parameters.

The Power-over-Ethernet (PoE) Sensor products measure various conditions (environmental, power, access). All devices come with flexible settings — including notifications, alerts, reports, and maps — can be customized in the iMonnit online sensor management interface.

PoE•X SENSOR FEATURES

- Power-over-Ethernet ready (injector hardware required)
- Embedded LEDs for transmission & online condition indicators
- 50,000 sensor message memory (non-volatile)
- Modbus TCP & SNTP v1 interface capabilities
- No PC required (managed through apps and smart devices)
- Remote update capable w/automatic updates
- Works with iMonnit Cloud and Enterprise software applications
- Optional 5V DC power supply available

EXAMPLE APPLICATIONS

- Doors and windows
- IT server closets
- Freezer and cooler door
- Cabinets and lockers
- Additional applications

II. SENSOR SECURITY

Security is paramount for the PoE•X Sensor when it comes to managing your data and transferring it to sensors. iMonnit is the online software and central hub for configuring your device settings. All data is secured on dedicated servers operating Microsoft SQL Server.

Data Security on the Sensor

The fortified sensor secures your data from attackers and secures the sensor from becoming a relay for malicious programs. Even when the sensor is at rest, the PoE•X Sensor is designed to prevent prying eyes from accessing the data. The Monnit PoE•X Sensor does not run on an off-the-shelf multi-function OS (operating system). Instead it runs a purpose-specific real-time embedded state machine that can't be hacked to run malicious processes. It also provides no active interface listeners that can be used to gain access to the device over the network.

iMONNIT Security

Access is granted through the iMonnit user interface, or an Application Programming Interface (API) safeguarded by 256-bit Transport Layer Security (TLS 1.2) encryption. TLS is a blanket of protection to encrypt all data exchanged between iMonnit and you. The same encryption is available to you whether you are a Basic or Premiere user of iMonnit. You can rest assured that your data is safe with iMonnit.

III. ORDER OF OPERATIONS

It is important to understand the order of operations for activating your PoE•X Sensor. If performed out of sequence, your sensor may have trouble communicating with iMonnit. Please follow the steps below to make sure you are performing your set-up correctly.

SET-UP STEPS

1. **Register your PoE•X Sensor on iMonnit.**

   Add your PoE•X Sensor to the iMonnit account (see page 3 for step-by-step directions).

2. **Connect the Ethernet and optional power cords to the sensor.**

   Plug in powered Ethernet cable. Depending on your facility, you might need to plug in both the Ethernet cable and power cord.

3. **Mount your sensor.**

   Place your sensor in the desired location using screws or double-sided tape.

Note: Each step is covered in more detail in the following sections.

III. SETUP AND INSTALLATION

If this is your first time using the iMonnit online portal, you will need to create a new account. If you have already created an account, start by logging in. For instructions on how to register and setup your iMonnit account, please consult the iMonnit User Guide.

STEP 1: ADD DEVICE

1. **Add the sensor on iMonnit.**
   Add the sensor to your account by choosing **Sensors** in the main menu. Navigate to the **Add Sensor** button.

Desktop

Mobile

2. **Find the device ID. See Figure 1.**
   The Device ID (ID) and Security Code (SC) are necessary to add a sensor. These can both be located on the label on the side of your device.

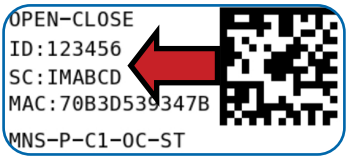

Figure 1

3. **Adding your device. See Figure 2.**
   You will need to enter the Device ID and the Security Code from your Sensor in the corresponding text boxes. Use the camera on your smartphone to scan the QR code on your device. If you do not have a camera on your phone, or the system is not accepting the QR code, you may enter the Device ID and Security Code manually.

Figure 2

- The Device ID is a unique number located on each device label.
- Next, you'll be asked to enter the Security Code from your device. A security code consists of letters and must be entered in upper case (no numbers). It can also be found on the barcode label of your device.

When completed, select the **Add Device** button.

STEP 2: SETUP

Select your use case. See Figure 3.

To get you up and running fast, your sensor comes with preset use cases. Choose from the list or create your own custom settings. You will see the heartbeat interval, and aware state settings (see page 9 for definitions) .

Select the **Skip** button when completed.

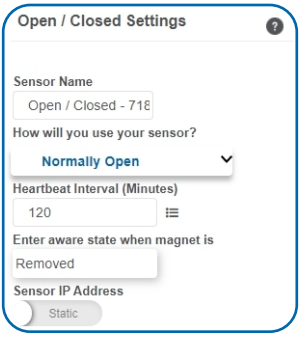

Figure 3

STEP 3: VALIDATION

Check your signal. See Figure 4.

The validation checklist will help you ensure your sensor is communicating with the gateway properly and you have a strong signal.

Checkpoint 4 will only complete when your sensor achieves a solid connection to the gateway. Once you insert the batteries (or flip the switch on an industrial sensor) the sensor will communicate with the gateway every 30 seconds for the first few minutes.

Select the **Save** button when completed.

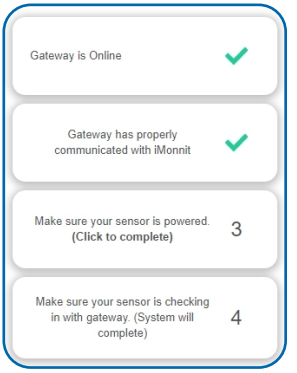

Figure 4

STEP 4: ACTIONS

Choose your actions. See Figure 5.

Actions are the alerts that will be sent to your phone or email in the event of an emergency. Low battery life and device inactivity are two of the most common actions to have enabled on your device. See page 12 for how to set actions for your sensor.

Select the **Done** button when completed.

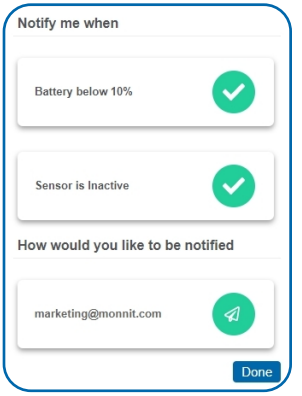

Figure 5

V. SETTING UP YOUR PoE•X SENSOR

Plug in powered Ethernet cable.

Depending on your facility, you might need to plug in both the Ethernet cable and power cord. See Figure 6.

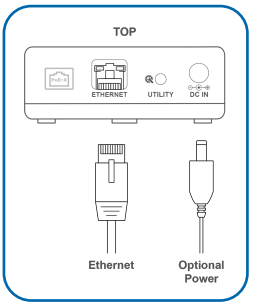

Figure 6

LIGHTING SEQUENCE

The sensor will cycle through three stages as it powers on:

Power-on stage: At this stage, the sensor will analyze electronics and programming. The LED lights will flash red and green, before all becoming green for one second. In the case of failure, the light sequence will repeat after ten seconds. Please contact technical support if the lights aren't green after two minutes.

Connection stage: The sensor will attempt to settle all operational connections. As the sensor attempts to connect, the Sensor Status LED will be off, waiting for the Ethernet connection to complete. After the Ethernet setup is complete, the Sensor Status Light will briefly blink red before turning green and then going off completely. If the Ethernet Status LED is orange, there is a failure in your Ethernet connection. Check your connection.

Operational stage: In the operational stage, the Ethernet lights will remain active while the Sensor Status light remains off — unless there is an issue. See Figure 7 & Figure 8.

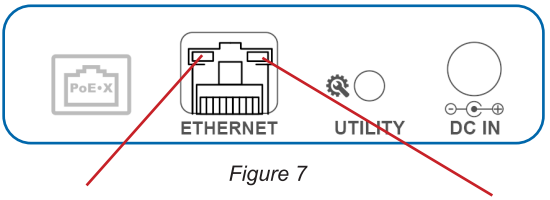

Figure 7

Ethernet Status LED

Steady Blinking Green:
Performing Ethernet set up operations

Solid Green with Flicker:
Connection successful for normal operation

Ethernet Link LED

Off:
No Ethernet cable connected

Green:
Ethernet is connected

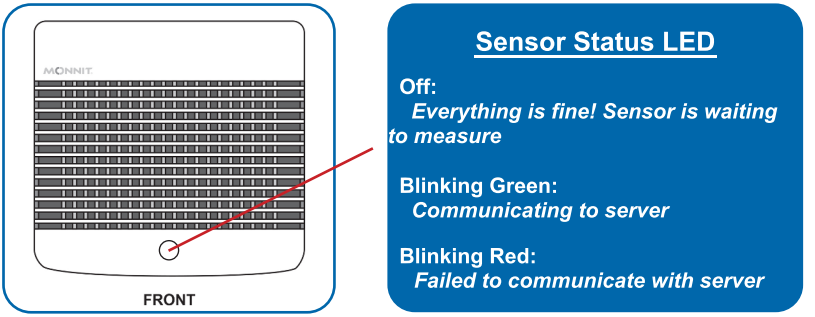

Figure 8

MOUNTING THE SENSOR

Monnit sensors feature mounting flanges and can be attached to most surfaces using the included mounting screws or double-sided tape. See Figure 9.

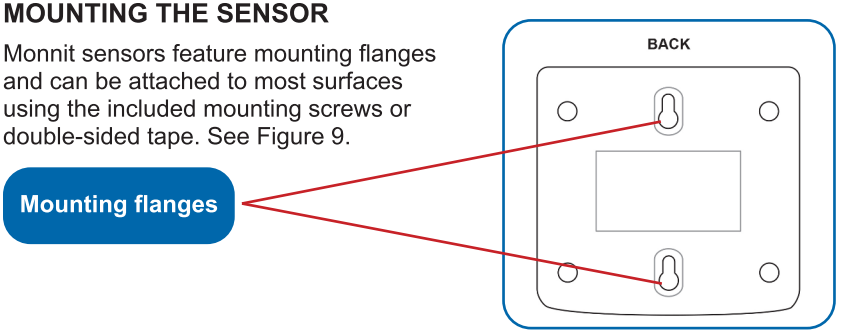

Figure 9

VI. SENSOR OVERVIEW

Select Sensors from the main navigation menu on iMonnit to access the sensor overview page and begin adjusting your PoE•X Sensors.

MENU SYSTEM

Details - Displays a graph of recent sensor data

History - List of past readings

Actions - List of actions attached to this sensor

Settings - Editable levels for your sensor

Directly under the tab bar is an overview of your sensor. This allows you to see the signal strength of the selected sensor. A colored dot in the left corner of the sensor icon denotes its status:

- **Green** indicates the sensor is checking in and is within user-defined safe parameters.
- **Red** indicates the sensor has met or exceeded a user-defined threshold or triggered event.
- **Gray** indicates that no sensor readings are being recorded, rendering the sensor inactive.
- **Yellow** indicates that the sensor reading is out of date, possibly due to a missed heartbeat check-in.

Details View

The Details View will be the first page you see upon selecting which sensor you would like to modify. See Figure 10.

A. The Sensor Overview section is at the top of every page. This will display the present reading, signal strength, battery level, and status.

B. The Recent Readings section below the chart shows your most recent data received by the sensor.

C. The Readings Chart displays how the sensor readings fluctuate throughout a set date range. To change the date range displayed in the graph, navigate up to the top of the Readings Chart section on the right-hand corner to change the “From:” and/or “To:” date.

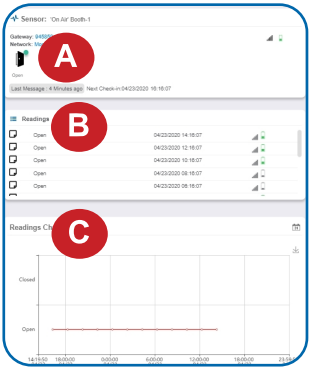

Figure 10

Readings View

Selecting the **Readings Tab** within the tab bar allows you to view the sensor's data history as time stamped data.

- On the far right of the Sensor History Data is a cloud icon. ( ) Selecting this icon will export an Excel file for your sensor into your download folder.

Note: Make sure you have the date range for the data you need input in the "From" and "To" text boxes. This will be the previous day by default. Only the first 2,500 entries in the selected date range will be exported.

The data file will have the following fields:

MessageID: Unique identifier of the message in our database.

Sensor ID: If multiple sensors are exported, you can distinguish between the sensors using this number — even if the names are the same.

Sensor Name: The name you have given the sensor.

Date: The date the message was transmitted from the sensor.

Value: Data presented with transformations applied, but without additional labels.

Formatted Value: Data transformed and presented as it is shown in the monitoring portal.

Raw Data: Raw data as it is stored from the sensor.

Sensor State: Binary field represented as an integer containing information about the state or the sensor when the message was transmitted. (See "***Sensor State***" explained below.)

Alert Sent: Boolean indicating if this reading triggered a notification to be sent from the system.

Sensor State

The integer presented here is generated from a single byte of stored data. A byte consists of 8 bits of data that we read as Boolean (True (1) / False (0)) fields.

Using a temperature sensor as an example:

If the sensor is using factory calibrations, the Calibrate Active field is set True (1) so the bit values are 00010000 and it is represented as 16.

If the sensor is outside the Min or Max Threshold, the Aware State is set True (1) so the bit values are 00000010 and it is represented as 2.

If the user has calibrated the sensor, the Calibrate Active field is set False (0) and the sensor is operating inside the Min and Max Thresholds, the bits look like 00000000 – this is represented as 0.

If the sensor is using factory calibrations and it is outside the threshold, the bit values are 00010010 and it is represented as 18 (16 + 2 because both the bit in the 16 value is set and the bit in the 2 value is set).

Settings View

To edit the operational settings for a sensor, choose the **Sensor** option in the main navigation menu and then select the **Settings Tab** to access the configuration page. See Figure 11.

A. **Sensor Name** is the unique name you give the sensor to easily identify it in a list along with any notifications.

B. **Heartbeat Interval** is how often the sensor communicates with the server if no activity is recorded.

C. **Aware State** Heartbeat is how often the sensor communicates with the server while in the Aware State.

D. **Event Aware State** when magnet is sets the sensor to detect when the magnet is removed, introduced, or a state change.

E. **Report as "Open"** when magnet is the exact time the door should enter an alert state when the magnet is removed or introduced.

F. **Time to Re-Arm** is the time in seconds after a triggering event that the sensor will wait before re-arming itself.

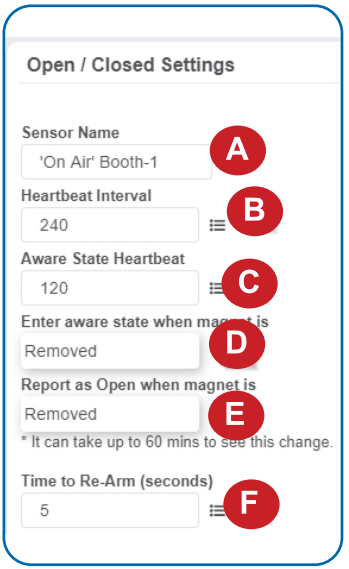

Figure 11

Finish by selecting the **Save** button.

Note: Be sure to select the Save button anytime you make a change to any of the sensor parameters. All changes made to the sensor settings will be downloaded to the sensor on the next sensor heartbeat (check-in). Once a change has been made and saved, you will not be able to edit that sensor's configuration again until it has downloaded the new setting.

INTERFACE SETTINGS

The PoE•X Sensor supports SNMP, Modbus, SNTP, and HTTP Interfaces. Toggle on these interfaces by going to the sensor settings page and choosing the **Interface Settings** button.

Interface Activation

To activate these interfaces, choose the switch under to access their individual settings. See Figure 12.

SNMP Interface – SNMP (Simple Network Management Protocol) is an Internet application protocol that manages and monitors network device functionality. Monnit uses SNMP version 1. These settings can both be configured on iMonnit and the local interface.

Inbound IP Range Start and End – This is the IP address for the SNMP client. If you have one device to communicate with, the start and end IP addresses will be the same. Exchanging information with multiple machines will require a set of different start and end IP addresses.

Inbound Port – Server port where data from the device is received.

SNMP Community String – This is used to support SNMPv1 protocol by giving access to a router's or other device's statistics. The default will be set to "public."

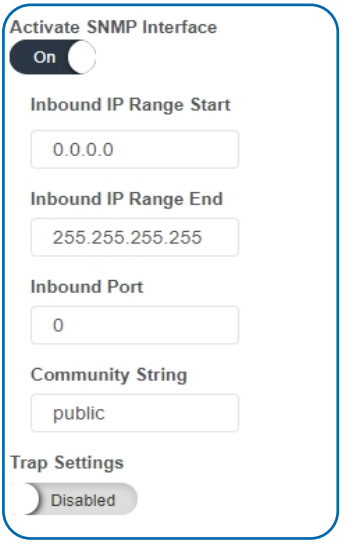

Figure 12

Trap Settings – The switch for Trap Settings will be disabled by default. Enable to view the trap settings.

Trap IP Address – The IP Address for the SNMP Server where the trap will be sent.

Trap Port – The server port where the trap alert state is sent when active.

Modbus Interface – Monnit provides the Modbus TCP interface for you to pull sensor data. You can use Modbus without the server interface active. The data will not be sent to a server, but you can continue to poll for new data as it is received by the server.

SNTP Interface – SNTP (Simple Network Time Protocol) is a synchronized computer clock on a network. An SNTP server can be set up on the same LAN as the server, such as on a router or a Linux computer. The sensor should be configured to retrieve time from only trusted servers, such as the ones maintained by your ISP. Incorrect time can affect the delivery of sensor traffic. See Figure 13.

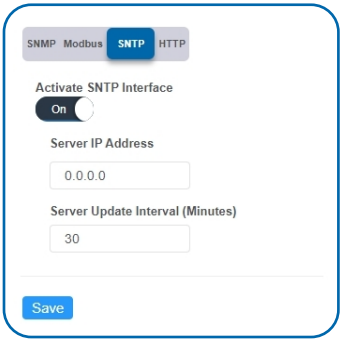

Figure 13

If the Monnit Server is active, it will be utilized for time synchronization in ordinary operation. So SNTP will be used as a backup. If you disable the default server interface, you must configure the SNTP Interface.

HTTP Interface – The HTTP Interface allows you to set how long you wish the local interface to be active before being automatically disabled. For increased Security, your choices are to have the local HTTP interface disabled after 1 minute, 5 minutes, 30 minutes, or always active. See page 15 of this guide for more on the local interface. See Figure 14.

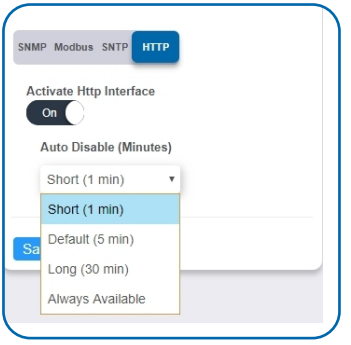

Figure 14

VII. ACTIONS OVERVIEW

Device notifications can be created, deleted, and edited by selecting the **Actions Tab** in the tab bar.

You can toggle the Action Trigger on or off by selecting the switch under Current Action Triggers. See Figure 15

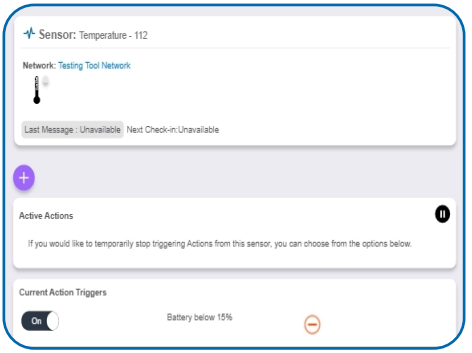

Figure 15

CREATING AN ACTION

- Actions are triggers or alarms set to notify you when a sensor reading identifies that immediate attention is needed. Types of actions include sensor readings, device inactivity, and scheduled data. Any one of these can be set to send a notification or trigger an action in the system.

Choose **Actions** in the main navigation menu.

Figure 16

- A list of previously created actions will display on the screen. From here, you have the ability to filter, refresh, and add new actions to the list.

Note: If this is your first time adding an action, the screen will be blank.

From the Actions page, tap **Add Action** in the left hand corner.

Figure 17

Step 1: What triggers your action?

The drop-down menu will have the following options for Action Types (See Figure 18):

- **Sensor Reading:** Set actions based on activity or reading.
- **Device Inactivity**: Actions when the device doesn't communicate for an extended period of time.
- **Advanced:** Actions based on advanced rules, such as comparing past data points with current ones.
- **Scheduled:** These actions are performed at a time set basis.

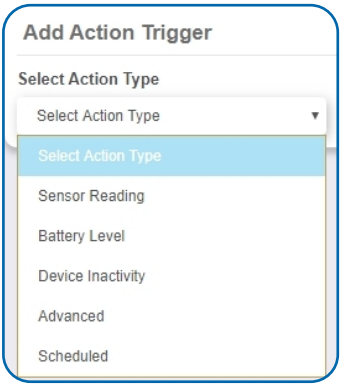

Figure 18

- Select Sensor Reading from the drop-down menu.
- A second drop-down menu will appear. From here, you will be able to see a list of the different type of sensors registered to your account. Choose **Open / Close** in the drop-down menu.
- Next, you will be asked to input the trigger settings. You have the option of setting this trigger to notify when the door position or magnet is either "Open / No Magnet Detected" or "Closed / Magnet Detected."

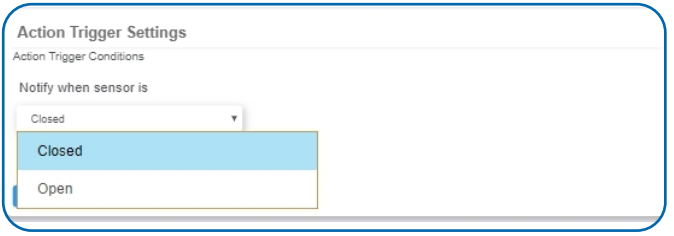

Figure 19

Press the **Save** button.

Step 2: Actions

- Press the **Add Action** button under the information header, available action types will then be presented in a select list.
- **Notification Action:** Specify account users to receive notification when this event triggers.
- **System Action:** Assign actions for the system to process when this event triggers.
- Choose **Notification Action** from the notification list.

A. Input the subject for the notification. See Figure 20.

B. Customize the message body for the notification. See Figure 20.

C. Recipient list identifies who will receive the notification. See Figure 21.

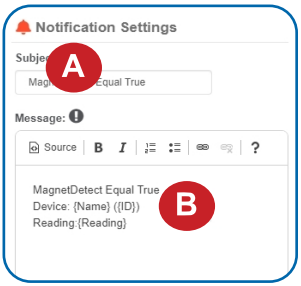

Figure 20

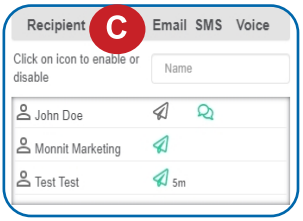

Figure 21

- Select the icon next to a user to specify how they will be notified.
- Choose if you want notifications sent immediately, when triggered, or if you want a delay before sending and press **Set**.
- A **green** icon indicates that the users that will receive the notifications.
- If a delay has been selected, the delay time will display beside the icon.

Select **System Action** from the Add Action list. See Figure 22.

- Scroll down to the System Action section.
- The Action to be done select list has the following options:

  Acknowledge: Automatically signals that you have been notified of an action. When an action has been triggered, alerts will continue processing until the action returns to a value that no longer triggers an action.

  Full Reset: Reset your trigger so it is armed for the next reading.

  Activate: Enable an action trigger.

  Deactivate: Disable an action trigger.

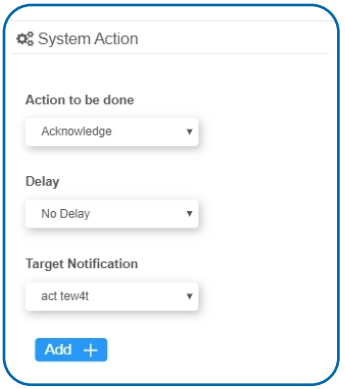

Figure 22

Step 3: Action Name and Devices

- By default, the sensor(s) will not be assigned to the action conditions you've just set. To assign a sensor, find the device(s) you want to designate for this action and select. Selected sensor boxes will turn green when activated. Choose the sensor box again to unassign the sensor from the action. See Figure 23.
- Continue toggling the sensor(s) corresponding to this new action until you are satisfied with your selection. These can be adjusted later by returning to this page.

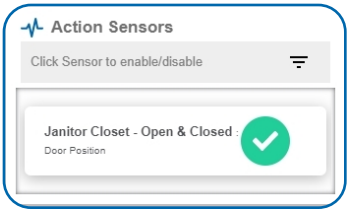

Figure 23

Press the **Check-mark** button to complete the process.

VIII. USING THE LOCAL INTERFACE

If using iMonnit is not an option, you can set up your sensor offline through the local interface.

Connect the sensor to a router or network switch using an Ethernet cable. Plug in the sensor to a power outlet. The device will automatically power on. Press and hold the utility button. At the end of the boot process, the Sensor Status LED will shift to red. Release the button and the Sensor Status LED will blink green and red signaling that the sensor has force-enabled the HTTP Interface. This interface will be temporarily active for five minutes, even if the interface is configured to be disabled.

If the button is not released after 10 seconds, the Sensor Status LED will begin to blink red. When the button is released, the device will perform a factory reset.

Use a PC on the local network to access your router's configuration page first (see your router documentation). Use your router's web interface to determine the IP address it assigns your device.

Use your web browser to connect to your sensor using the assigned IP address. You should be redirected to the **Status Tab**.

Find the **Settings Tab** and select the "**Miscellaneous**" page. Enable the **HTTP Interface** and set it to be available for one hour (3600 seconds). Choose "**Save Changes**" when completed.

Note: Each time a page is refreshed or every time the sensor restarts, the HTTP interface time resets. After it times out, the web interface will be disabled until either the device restarts with a non-zero timeout value, or the special restart mode is enabled using the utility button. After configuration, set this to a small integer.

STATUS TAB

This is a read only section listing the current conditions for your Local Area Network (LAN). See Figure 24.

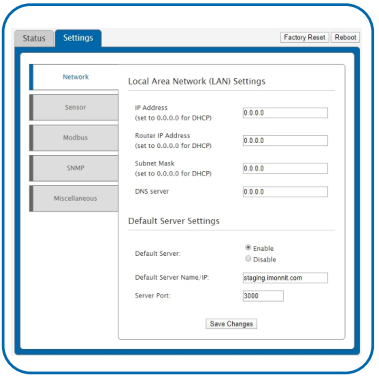

Figure 24

Device MAC Address – This is the Media Control Address of your device to exclusively identify the device to a Network Interface Controller.

Device IP Address – This is a numerical identifier for your device when it is connected to the Internet.

Router IP Address – This is a numerical identifier for your router when it is connected to the Internet.

Network Mask – Also known as a “Subnet Mask,” this masks the IP address by dividing it into the network address and the host address.

DNS Address – A Domain Name System (DNS) is the method employed by a URL of translating the alphabetic entry in an address bar into a numerical address associated with a server.

Sensor Statuses

Temperature – Reading of the device temperature.

Data Cache Used – This percentage represents the amount of internal flash memory storage for holding sensor messages that has been used out of the maximum (896 kb). Messages sent from the sensor are stored temporarily in the sensor cache until a data interface (i.e. Default Server, SNMP, Modbus, etc.) confirms the data has been stored or transmitted elsewhere.

Interface Status

This section lists the interfaces communicating with the device and indicates whether they are on or off. Options include: Default Server, Modbus TCP, SNMP, and SNTP. These can all be enabled or disabled under the **Settings Tab**.

SETTINGS TAB

The **Settings Tab** will open to the Network Page. See Figure 25.

The Network Page

From the Network Page, you can modify settings for your IP address, Router IP Address, Subnet Mask, DNS Server, and Default Server Settings.

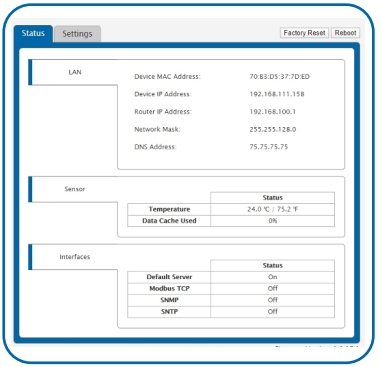

Figure 25

IP Address – A unique number typically formatted as XXX.XXX.XXX.X. It can be dynamic, meaning the IP address is constantly changing, or static, meaning the IP address stays the same.

Router IP Address – This is a unique number identifying your router to the default server.

Subnet Mask – This number hides the network half of an IP address. The most common Subnet Mask number is 255.255.255.0.

DNS – The Domain Name Server takes alphanumerical data (like a url address) and returns the IP address for the server containing the information you're looking for.

Under **Default Server Settings**, choose the radio button to enable or disable the Default Server. Enter the name of your **Default Server Name/IP** in the text box. Lastly, input the **Server Port** number. Finish by choosing the **Save Changes** button.

The Settings View Page

- The Settings View Page is where you can adjust settings for your sensor. These will be the same as in iMonnit (See page 8 for definitions of settings for your PoE•X Sensor.

The Modbus Page

Modbus TCP interface runs on an Ethernet connection. TCP makes sure all data is received. Modbus TCP is a non-streaming data interface standard. This means data must be requested in order for it to be received. The Modbus TCP Interface will store all data values in 16-bit registers. See Figure 26 on the next page.

The registers and their associated data fields are mapped on the next page.

To access the sensor holding registers, the assigned slot number for the device needs to be known. When reviewing added devices through the default server, the order in which devices are presented may not necessarily correspond to the order in which the devices are stored in the network list as the default server will sort the devices based on their ID. To be certain which device is in a particular slot, go to the local web interface (wsn.htm page) or status page and note which slot the desired device is assigned to.

After the slot number(s) for the desired devices to read from are known, the following formula may be applied to determine the correct starting register to read from to retrieve the recorded data from the device: starting register=101+16(slot no.-1). Each reading will report the most recent message received from that device by the device, so the polling frequency should be greater than the device heartbeat frequency to avoid missing device updates.

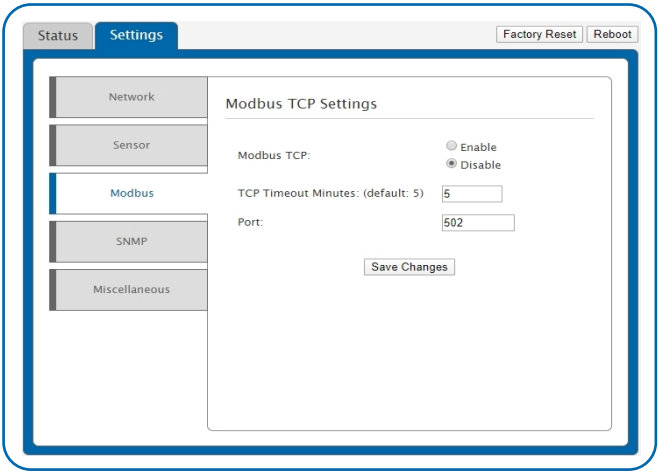

Figure 26

DEVICE HOLDING REGISTERS			
NAMED FIELDS	DESCRIPTION	FUNCTION SPECIFIC ADDRESS	RAW ADDRESS
Sensor ID_High	The first 16 bits of a 32-bit serial ID number	40101	100
Sensor ID_Low	The last 16 bits of a 32-bit serial ID number	40102	101
Device Type	The unique type identifier for the sensor profile	40103	102
Data Age	The number of seconds that have elapsed since the last data was retrieved	40104	103
Is Device Active	0 indicates no data for this slot	40105	104
Is Aware	Becomes aware when a sensor threshold has been breached	40106	105
Voltage	Battery voltage	40107	106
RSSI	Signal Strength Indicator — 0-100%	40108	107
Data 1	Sensor Data Field 1	40109	108
Data 2	Sensor Data Field 2	40110	109
Data 3	Sensor Data Field 3	40111	110
Data 4	Sensor Data Field 4	40112	111
Data 5	Sensor Data Field 5	40113	112
Data 6	Sensor Data Field 6	40114	113
Data 7	Sensor Data Field 7	40115	114
Data 8	Sensor Data Field 8	40116	115
Sensor ID_High	The first 16 bits of a 32-bit serial ID number	40117	116
Sensor ID_Low	The last 16 bits of a 32-bit serial ID number	40118	117
Device Type	The unique type identifier for the sensor profile	40119	118
Data Age	The number of seconds that have elapsed since the last data was retrieved	40120	119
Is Device Active	0 indicates no data for this slot	40121	120
Is Aware	Becomes aware when a sensor threshold has been breached	40122	121
Voltage	Battery voltage	40123	122
RSSI	Signal Strength Indicator — 0-100%	40124	123
Data 1	Sensor Data Field 1	40125	124

The SNMP Page

SNMP settings for your device can be adjusted on the offline local interface. You can continue to use SNMP without the server interface active. The data will not be sent to a server, but you can continue to poll for the data as it is received. See Figure 27.

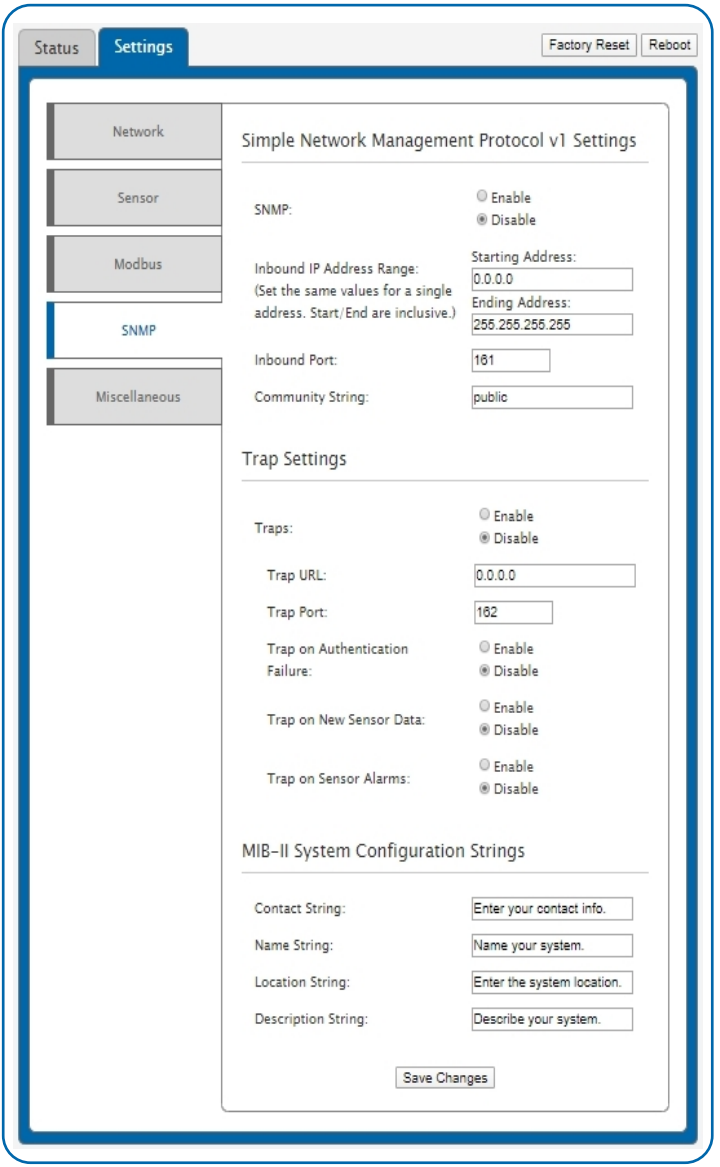

Figure 27

- **Inbound IP Range Start and End** – This is the IP address for the SNMP client. If you have one device to communicate with, the start and end IP addresses will be the same. Exchanging information with multiple machines will require a set of different start and end IP addresses.

- **Inbound Port** – This is the number for where specifically in the server data from the device is received.

- **SNMP Community String** – This is used to support SNMPv1 protocol by giving access to a router's or other device's statistics. The default will be set to "public".

Trap Settings

- **Trap IP Address** – The IP Address for the SNMP Server where the trap will be sent.

- **Trap Port** – The server port where the trap alert state is sent when active.

MIB-II System Configuration Strings

The HTTP Interface should be enabled to keep your local interface session open.

HTTP Service Timeout: This is a security setting for allowing this web interface to be active. The default is 5 minutes. Setting the field to 0 will turn off the local interface, ending your session. See Figure 28.

Your **Data Management Settings** control how long sensor data is accessible. The Data Expiration field sets an expiration period for data before it is considered to be "old" meaning data interfaces will not report this sensor data. The maximum setting is 65535.

Choose the **Clear Sensor Data** button to clear your cache. Pressing this button will purge all old device messages from the device to start from a clean slate. You will lose all messages for all data interfaces.

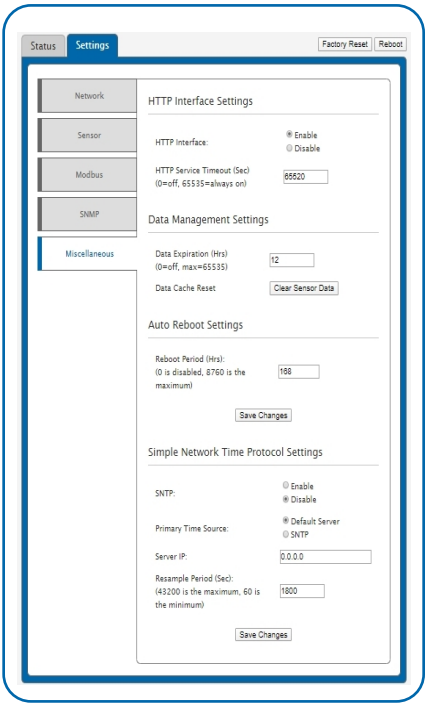

Figure 28

Auto Reboot Settings assign a reboot period to the sensor so the device can reboot.

Simple Network Time Protocol (SNTP) synchronizes computer clocks on a network when the Monnit Interface is unavailable.

SNTP IP Address: This is the IP Address for the server the time is being pulled from.

SNTP Resample Period: The time in seconds when the device will check the server for the correct time.

Epoch between Default Server and SNTP: This is the difference in seconds between the standard SNTP Epoch (start date 01/01/1900) and Monnit's Epoch (start date 01/01/2012).

System Reset Period: The time in hours it takes for the system to reset.

Secondary Time Source Failover Period: The time in seconds that the device will continue to attempt to poll the Primary System Time Source unsuccessfully for an updated time before switching over and using time from the secondary time source. This time period should be longer than the SNTP Resample Period if SNTP is being used.

SUPPORT

For technical support and troubleshooting tips please visit our support library online at monnit.com/support/. If you are unable to solve your issue using our online support, email Monnit support at support@monnit.com with your contact information and a description of the problem, and a support representative will call you within one business day.

For error reporting, please email a full description of the error to support@monnit.com.

WARRANTY INFORMATION

(a) Monnit warrants that Monnit-branded products (Products) will be free from defects in materials and workmanship for a period of one (1) year from the date of delivery with respect to hardware and will materially conform to their published specifications for a period of one (1) year with respect to software. Monnit may resell sensors manufactured by other entities and are subject to their individual warranties; Monnit will not enhance or extend those warranties. Monnit does not warrant that the software or any portion thereof is error free. Monnit will have no warranty obligation with respect to Products subjected to abuse, misuse, negligence or accident. If any software or firmware incorporated in any Product fails to conform to the warranty set forth in this Section, Monnit shall provide a bug fix or software patch correcting such non-conformance within a reasonable period after Monnit receives from Customer (i) notice of such non-conformance, and (ii) sufficient information regarding such non-conformance so as to permit Monnit to create such bug fix or software patch. If any hardware component of any Product fails to conform to the warranty in this Section, Monnit shall, at its option, refund the purchase price less any discounts, or repair or replace nonconforming Products with conforming Products or Products having substantially identical form, fit, and function and deliver the repaired or replacement Product to a carrier for land shipment to customer within a reasonable period after Monnit receives from Customer (i) notice of such non-conformance, and (ii) the non-conforming Product provided; however, if, in its opinion, Monnit cannot repair or replace on commercially reasonable terms it may choose to refund the purchase price. Repair parts and replacement Products may be reconditioned or new. All replacement Products and parts become the property of Monnit. Repaired or replacement Products shall be subject to the warranty, if any remains, originally applicable to the product repaired or replaced. Customer must obtain from Monnit a Return Material Authorization Number (RMA) prior to returning any Products to Monnit. Products returned under this Warranty must be unmodified.

Customer may return all Products for repair or replacement due to defects in original materials and workmanship if Monnit is notified within one year of customer's receipt of the product. Monnit reserves the right to repair or replace Products at its own and complete discretion. Customer must obtain from Monnit a Return Material Authorization Number (RMA) prior to returning any Products to Monnit.

Products returned under this Warranty must be unmodified and in original packaging. Monnit reserves the right to refuse warranty repairs or replacements for any Products that are damaged or not in original form. For Products outside the one year warranty period repair services are available at Monnit at standard labor rates for a period of one year from the Customer's original date of receipt.

(b) As a condition to Monnit's obligations under the immediately preceding paragraphs, Customer shall return Products to be examined and replaced to Monnit's facilities, in shipping cartons which clearly display a valid RMA number provided by Monnit. Customer acknowledges that replacement Products may be repaired, refurbished or tested and found to be complying. Customer shall bear the risk of loss for such return shipment and shall bear all shipping costs. Monnit shall deliver replacements for Products determined by Monnit to be properly returned, shall bear the risk of loss and such costs of shipment of repaired Products or replacements, and shall credit Customer's reasonable costs of shipping such returned Products against future purchases.

(c) Monnit's sole obligation under the warranty described or set forth here shall be to repair or replace non-conforming products as set forth in the immediately preceding paragraph, or to refund the documented purchase price for non-conforming Products to Customer. Monnit's warranty obligations shall run solely to Customer, and Monnit shall have no obligation to customers of Customer or other users of the Products.

Limitation of Warranty and Remedies

THE WARRANTY SET FORTH HEREIN IS THE ONLY WARRANTY APPLICABLE TO PRODUCTS PURCHASED BY CUSTOMER. ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE EXPRESSLY DISCLAIMED. MONNIT'S LIABILITY WHETHER IN CONTRACT, IN TORT, UNDER ANY WARRANTY, IN NEGLIGENCE OR OTHERWISE SHALL NOT EXCEED THE PURCHASE PRICE PAID BY CUSTOMER FOR THE PRODUCT. UNDER NO CIRCUMSTANCES SHALL MONNIT BE LIABLE FOR SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES. THE PRICE STATED FOR THE PRODUCTS IS A CONSIDERATION IN LIMITING MONNIT'S LIABILITY. NO ACTION, REGARDLESS OF FORM, ARISING OUT OF THIS AGREEMENT MAY BE BROUGHT BY CUSTOMER MORE THAN ONE YEAR AFTER THE CAUSE OF ACTION HAS ACCRUED.

IN ADDITION TO THE WARRANTIES DISCLAIMED ABOVE, MONNIT SPECIFICALLY DISCLAIMS ANY AND ALL LIABILITY AND WARRANTIES, IMPLIED OR EXPRESSED, FOR USES REQUIRING FAIL-SAFE PERFORMANCE IN WHICH FAILURE OF A PRODUCT COULD LEAD TO DEATH, SERIOUS PERSONAL INJURY, OR SEVERE PHYSICAL OR ENVIRONMENTAL DAMAGE SUCH AS, BUT NOT LIMITED TO, LIFE SUPPORT OR MEDICAL DEVICES OR NUCLEAR APPLICATIONS. PRODUCTS ARE NOT DESIGNED FOR AND SHOULD NOT BE USED IN ANY OF THESE APPLICATIONS.

SAFETY RECOMMENDATIONS - READ CAREFULLY

Be sure the use of this product is allowed in the country and in the environment required. The use of this product may be dangerous and has to be avoided in the following areas:

- *Where it can interfere with other electronic devices in environments such as hospitals, airports, aircraft, etc.*
- *Where there is risk of explosion such as gasoline stations, oil refineries, etc.*

It is responsibility of the user to enforce the country regulation and the specific environment regulation.

Do not disassemble the product; any mark of tampering will compromise the warranty validity. We recommend following the instructions of this user guide for correct setup and use of the product.

Please handle the product with care, avoiding any dropping and contact with the internal circuit board as electrostatic discharges may damage the product itself.

The European Community provides some Directives for the electronic equipment introduced on the market. All the relevant information's is available on the European Community website:

http://ec.europa.eu/enterprise/sectors/rtte/documents/

The text of the Directive 99/05 regarding telecommunication equipment is available, while the applicable Directives (Low Voltage and EMC) are available at: http://ec.europa.eu/enterprise/sectors/electrical

Additional Information and Support

For additional information or more detailed instructions on how to use your Monnit Sensors or the iMonnit Online System, please visit us on the web at https://www.monnit.com/support/documentation.