



## GEN 2 Ethernet Gateway

### Part#: RFR-0526-2

# USER GUIDE

#### **IMPORTANT!**

For best results, please wait to power on your Ethernet Gateway until after you have registered an account on Scigiene Premier and added your gateway and sensors to the online system.

## Table of Contents

<b>1. ABOUT THE ETHERNET GATEWAY</b>	<b>1</b>
GEN 2 ETHERNET GATEWAY FEATURES	1
EXAMPLE APPLICATIONS	1
<b>II. HOW YOUR GATEWAY WORKS</b>	<b>2</b>
<b>III. GATEWAY SECURITY</b>	<b>3</b>
SENSOR COMMUNICATION SECURITY	3
DATA SECURITY ON THE GATEWAY	3
SERVER COMMUNICATION SECURITY	3
<b>IV. GATEWAY REGISTRATION</b>	<b>4</b>
REGISTERING THE EGW4 GATEWAY	4
<b>V. USING THE ETHERNET GATEWAY</b>	<b>5</b>
USING THE ETHERNET GATEWAY	5
UNDERSTANDING THE GATEWAY LIGHTS	5
EGW4 GATEWAY SETTINGS	6
<b>VI. INSTALLING SCIGIENE EXPRESS SOFTWARE</b>	<b>11</b>
INSTALLING SCIGIENE EXPRESS SOFTWARE	11
INSTALLING SCIGIENE SOFTWARE	11
<b>VII. USING THE LOCAL INTERFACE</b>	<b>12</b>
STATUS TAB	12
SETTINGS TAB	13
<b>TROUBLESHOOTING</b>	<b>20</b>
<b>SUPPORT</b>	<b>21</b>
<b>WARRANTY INFORMATION</b>	<b>21</b>
<b>CERTIFICATIONS</b>	<b>23</b>
<b>SAFETY RECOMMENDATIONS</b>	<b>25</b>

## I. ABOUT THE ETHERNET GATEWAY

Scigiene's [GEN 2 Ethernet Gateway 4](#) allows Scigiene Wireless Sensors to communicate with the Scigiene Premier Online Wireless Sensor Monitoring and Notification System without the need for a PC. Provide power and plug the gateway into an open Ethernet port with an Internet connection. It will automatically connect with our online servers, providing the perfect solution for commercial locations with an Internet connection.

GEN 2 Ethernet Gateways are advanced wireless IoT gateways that enable fast time-to-market solutions. Scigiene's Ethernet Gateway 4 is specifically designed to respond to the increasing market need for global technology that accommodates various vertical IoT application segments and remote wireless sensor management solutions.

### GEN 2 ETHERNET GATEWAY FEATURES

- Wireless range of 1,200+ feet through 12+ walls \*
- Frequency Hopping Spread Spectrum (FHSS)
- Improved interference immunity
- Encrypt-RF Security (Diffie-Hellman Key Exchange + AES-128 CBC for sensor data messages)
- 30,000 sensor message memory \*\*
- Over the air updates (future proof)
- True plug & play, no hassles for Internet configuration set-up
- No PC required for operation
- Low-cost cellular service packages
- Local status LEDs with transmission and online status indicators
- AC power supply

\* Actual range may vary depending on environment.

\*\* Total messages in memory varies with sensor type (30K total messages for Temperature. Additional information available from [support@scigiene.com](mailto:support@scigiene.com))

### EXAMPLE APPLICATIONS

- Remote Location Monitoring
- Shipping and Transportation
- Agricultural Monitoring
- Vacant Property Management
- Vacation Home Property Management
- Construction Site Monitoring
- Data Center Monitoring

## II. HOW YOUR GATEWAY WORKS

Your GEN 2 Ethernet Gateway manages communication between your sensors and Scigiene Premier. When running, the gateway will periodically transmit data on a heartbeat. The gateway will store information received from sensors until its next heartbeat.

The GEN 2 Ethernet Gateway is an Ethernet gateway. It uses an Ethernet connection to relay data received from sensors to Scigiene Premier. Sensors communicate with the gateway; then, the gateway forwards information to the cloud.

For your wireless sensors to work optimally, orient all antennas for your sensor(s) and gateway(s) in the same direction (typically vertical). Sensors must also be at least three feet away from other sensors and the wireless gateway to function correctly. See Figure 1.

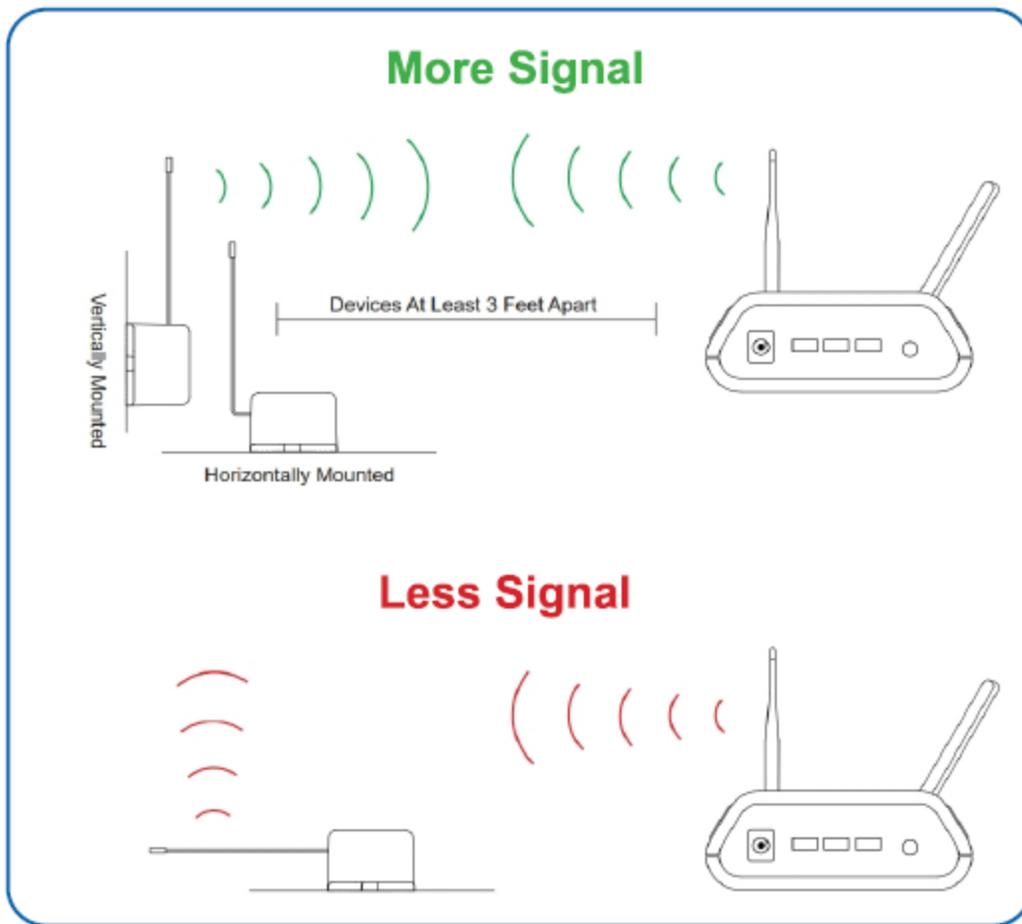


Figure 1

### **III. GATEWAY SECURITY**

The GEN 2 Ethernet Gateway has been designed and built to manage data from sensors monitoring your environment and equipment securely. Hacking from botnets are in the headlines; Scigiene Corporation has taken extreme measures to ensure your data security is handled with the utmost care and attention to detail. The same methods utilized by financial institutions to transmit data are also used in Scigiene security infrastructure. Security features of the gateway include tamper-proof network interfaces, data encryption, and bank-grade security.

Scigiene's proprietary sensor protocol uses low transmit power and specialized radio equipment to share application data. Wireless devices listening on open communication protocols cannot eavesdrop on sensors. Packet level encryption and verification are vital in ensuring traffic aren't altered between sensors and gateways. Paired with a best-in-class range and power consumption protocol, all data is transmitted securely from your devices. Thereby ensuring a smooth, worry-free experience.

#### **SENSOR COMMUNICATION SECURITY**

Scigiene sensor to gateway secure wireless tunnel is generated using ECDH-256 (Elliptic Curve Diffie-Hellman) public key exchange to develop a unique symmetric key between each pair of devices. Sensors and gateways use this link specific key to process packet-level data with hardware-accelerated 128-bit AES encryption, which minimizes power consumption to provide industry best battery life. Thanks to this combination, Scigiene proudly offers robust bank-grade security at every level.

#### **DATA SECURITY ON THE GATEWAY**

The GEN 2 Ethernet Gateway is designed to prevent prying eyes from accessing the data stored on the sensors. The GEN 2 Ethernet Gateway 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 cannot be hacked to run malicious processes. There are also no active interface listeners that can be used to gain access to the device over the network. The fortified gateway secures your data from attackers and secures the gateway from becoming a relay for malicious programs.

#### **SERVER COMMUNICATION SECURITY**

Communication between your GEN 2 Ethernet Gateway and Scigiene Premier is secured by packet-level encryption. Similar to the security between the sensors and gateway, the gateway and server also establish a unique key using ECDH-256 for encrypting data. The packet-level data is encrypted end to end, removing additional requirements to configure specialized cellular VPN's. The gateway can still operate within a VPN if it is present.

## IV. GATEWAY REGISTRATION

If this is your first time using the Scigiene Premier 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 for an Scigiene Premier account, please consult the Scigiene Premier User Guide.

### REGISTERING THE ETHERNET GATEWAY

You will need to enter the Device ID and the Security Code from your Ethernet Gateway in the corresponding text boxes. Use the camera on your smartphone to scan the QR code on your gateway. If you do not have a camera on your phone or are accessing the online portal through a desktop computer, you may manually enter the Device ID and Security Code. See Figure 2.

- The **Device ID** is a unique number located on each device label.
- Next, you'll be asked to enter the **Security Code (SC)** on your device. A security code will be all letters, no numbers. It can also be found on the barcode label of your gateway.

When completed, select the “Submit” button.

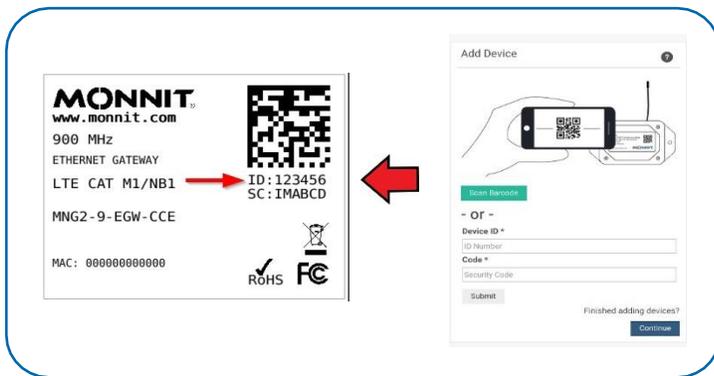


Figure 2

**IMPORTANT:** Add the gateway and all sensors to the Scigiene Premier portal so that the gateway can download and whitelist the sensors from the account on boot.

## V. USING THE ETHERNET GATEWAY

### USING THE ETHERNET GATEWAY

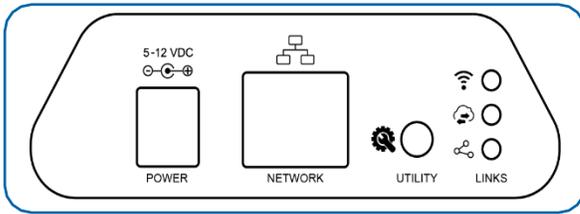


Figure 3

In Figure 3, from left to right, we see:

**Power:** This is where your power cord will be plugged into.

**Network:** This is the socket where your Ethernet cable will go.

**Utility Button:** During the boot sequence, a short, five-second, press of this button will enable the local interface. When powered on, pressing the utility button for 10-15 seconds will reset the gateway. Pressing the button for 15+ seconds will clear all memory in addition to the factory reset.

1. Connect your antennas to the gateway as seen in the below diagram.
2. Plug the power supply cord into an outlet.
3. After the three LED lights switch to green, your network is ready to use.

### UNDERSTANDING THE ETHERNET GATEWAY LIGHTS

The gateway will enter three stages as it powers on:

**Power-on Stage:** The gateway will analyze electronics and programming. The LED lights will flash red and green before becoming green for one second and entering a “waterfall” pattern. In case of failure, the light sequence will repeat after ten seconds. The gateway will continue trying to boot until it succeeds. Please contact technical support if the lights aren't green after two minutes.

**Connection Stage:** When the LEDs turn solid green for 1.5 seconds, the power-on step will be complete. After the Network Uplink Connectivity LED displays a solid green LED, the gateway will attempt to connect to its default server and other configured surfaces. The gateway will attempt to settle all active connections. As the gateway first relates to the network, all other lights will be dark.

**Operational Stage:** All of the lights will remain green while powered externally unless there is an issue. A blinking link light is a signal that the gateway has encountered a problem in the network.

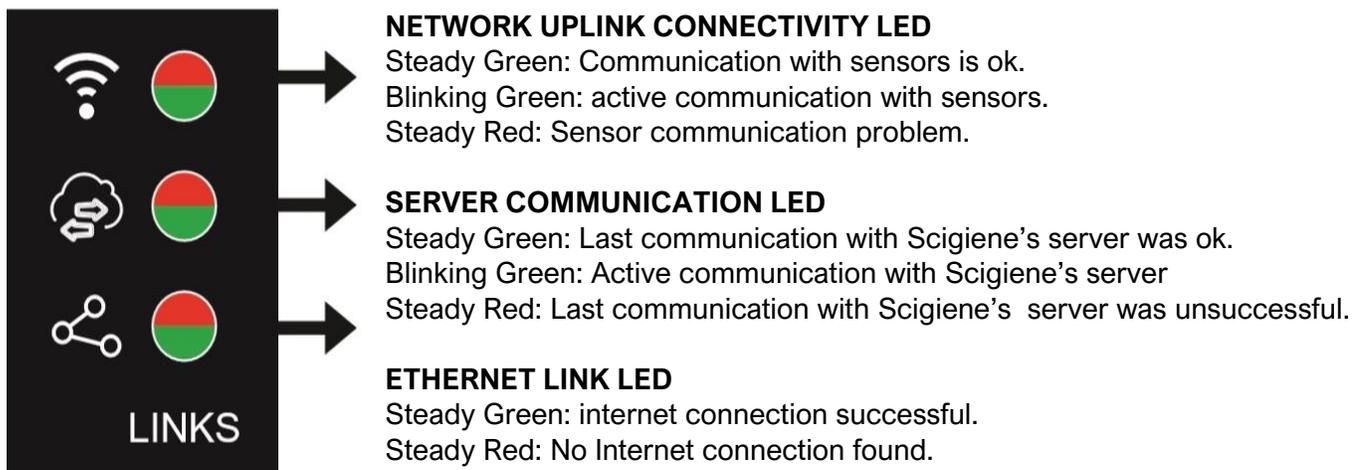


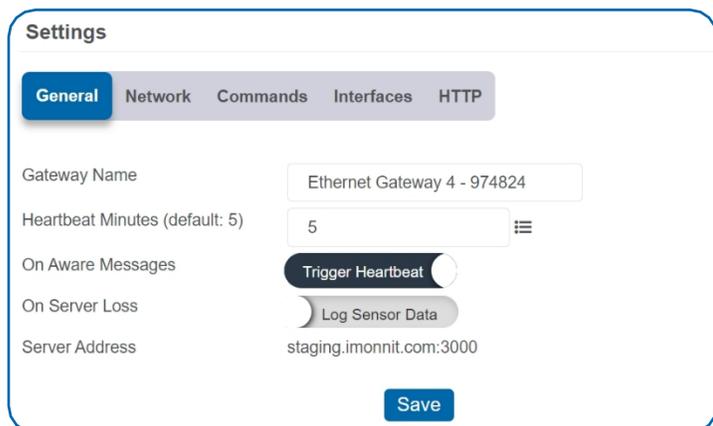
Figure 4

## ETHERNET GATEWAY SETTINGS

### General

The Ethernet Gateway will receive data from all sensors assigned to the network and within range, then return this data to the server in a series of heartbeats.

You can access gateway settings by selecting “Gateways” in the main navigation panel (See Figure 5). Choose the Ethernet Gateway from the list of gateways registered to your account. Select the “Settings” tab to edit the gateway:



The screenshot shows the 'Settings' page for an Ethernet Gateway. At the top, there are five tabs: 'General' (selected), 'Network', 'Commands', 'Interfaces', and 'HTTP'. Below the tabs, the 'Gateway Name' field contains 'Ethernet Gateway 4 - 974824'. The 'Heartbeat Minutes (default: 5)' field is set to '5'. The 'On Aware Messages' toggle is set to 'Trigger Heartbeat'. The 'On Server Loss' toggle is set to 'Log Sensor Data'. The 'Server Address' field contains 'staging.imonnit.com:3000'. A 'Save' button is located at the bottom right of the settings area.

Figure 5

The **Gateway Name** field is where you assign your gateway a unique title. By default, the gateway name will be the type followed by the Device ID.

The **Heartbeat Minutes** configures the interval that the gateway checks in with the server. The default is five minutes. So, every five minutes your gateway will report to the server.

When your sensors detect a threshold breach, they enter what is called an "aware state." The **On Aware Messages** toggle is set to "Trigger Heartbeat" by default. This means the gateway will check in with the server address immediately and relay the aware state information to Scigiene Premier.

Toggling this to "Wait for Heartbeat" will set the gateway to wait for its set heartbeat to elapse before communicating with the server.

The **On Server Loss** toggle switch sets what you wish to happen when the gateway loses communication with the server. The default setting "Log Sensor Data" commands the gateway to continue communicating with your sensors and store readings until it can re-establish a connection to the server.

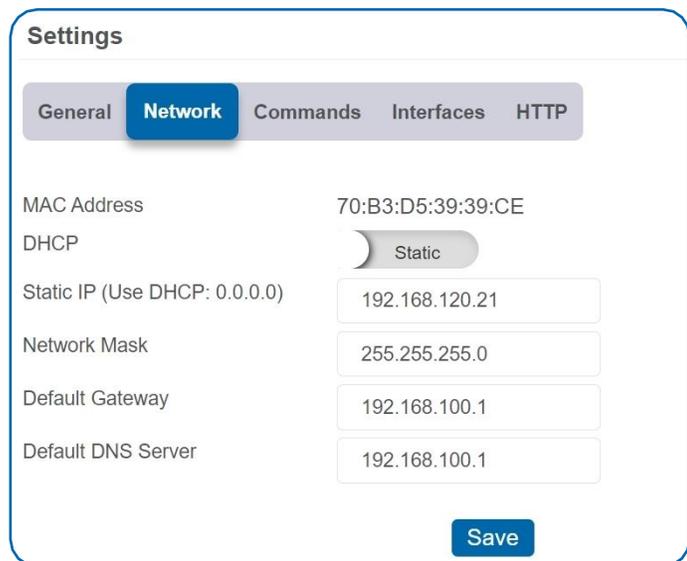
Toggling this to "Disable Wireless Network" will force the sensors communicating with this gateway to find a new gateway in order to deliver sensor messages to the server immediately.

## Network

Choose the Local Area Network bullet under the Settings title to open up the local area network configuration page. The Local Area Network includes the ability to switch your network IP address from DHCP to Static. DHCP will be the default network IP address.

Multiple interfaces can be active; if using any of the polling interfaces, we recommend using a static IP address on the gateway. An IP address is a unique number typically formatted as XXX.XXX.XXX.XXX.

To change your IP address to a Static IP, navigate to the network IP option, and switch it from DHCP to Static. Then input your data for the **Static IP, Network Mask, Default Gateway, and Default DNS Server**. See Figure 6.



The screenshot shows a 'Settings' window with a 'Network' tab selected. The configuration is as follows:

Field	Value
MAC Address	70:B3:D5:39:39:CE
DHCP	Static
Static IP (Use DHCP: 0.0.0.0)	192.168.120.21
Network Mask	255.255.255.0
Default Gateway	192.168.100.1
Default DNS Server	192.168.100.1

A 'Save' button is located at the bottom right of the settings panel.

Figure 6

**Static IP** - A static Internet Protocol (IP) address is a numerical sequence assigned to a computer by a Network Administrator. This is different from a Dynamic IP Address in that a Static IP doesn't periodically change and remains constant.

**Network Mask** - Also known as a "subnet mask" this number hides the network half of an IP address. The most common Network Mask number is 255.255.255.0.

**Default Gateway** - This is the forwarding host a computer utilizes to relay data to the Internet.

**Default DNS Server** - DNS Servers take alphanumerical data (like a URL address) and return the ip address for the server containing the information you're looking for.

## Commands

Choose the bullet for **Commands** located just under the Settings title to access the commands page. See Figure 7.

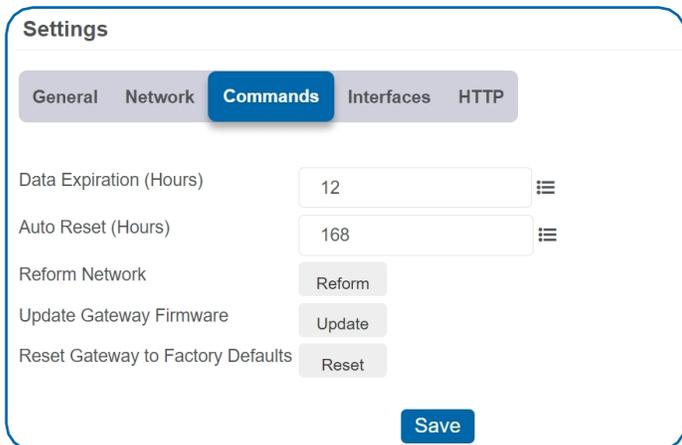


Figure 7

**Data Expiration (Hours)** - Data expiration in the Gateway. After this time has elapsed, the data pulled for Modbus and SNMP will be zero-ed out.

The **Auto Reset** field is the amount of time in hours that the Local Interface will automatically reboot. Setting this to 0 will disable the feature. The maximum setting is 8760 hours.

Selecting the **Reform Network** command will trigger the gateway to remove all sensors from the internal whitelist, and then request a new sensor list from the server. This command will force all sensors to reinitialize their connection with the gateway.

Reforming the network cleans up communication when multiple networks are in range of each other so they are all in sync. This is especially useful if you must move sensors to a new network, and would like to clear these sensors from the gateway's internal list.

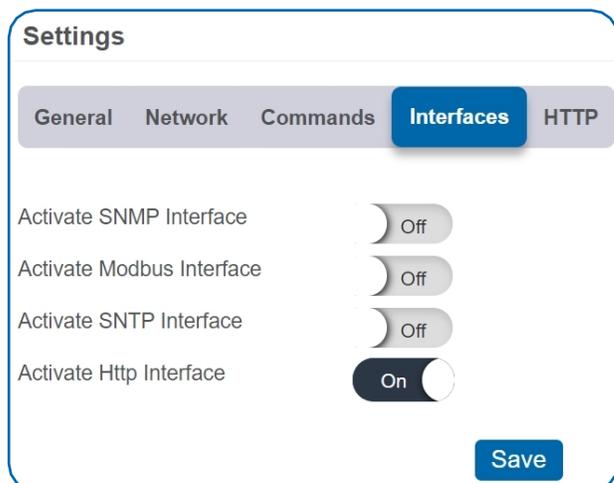
Reforming the network will place a new list of sensors that will continue to exchange data.

Picking the **Update Gateway Firmware** button signals the gateway to download and apply the latest firmware version available.

Choosing the **Reset Gateway to Factory Defaults** button will erase all your unique settings and return the gateway to factory default settings.

## Interface Activation

There are additional interfaces available for activation on your Gateway Settings page. To activate them, choose the Interface Activation bullet. Toggle on each of the interfaces to access their individual settings. See Figures 8 through 12.



Settings

General Network Commands **Interfaces** HTTP

Activate SNMP Interface  Off

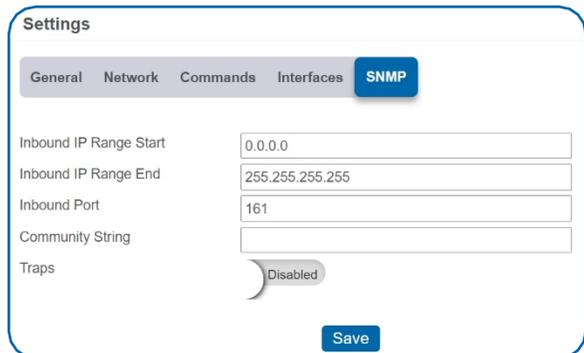
Activate Modbus Interface  Off

Activate SNTP Interface  Off

Activate Http Interface  On

Save

Figure 8



Settings

General Network Commands Interfaces **SNMP**

Inbound IP Range Start

Inbound IP Range End

Inbound Port

Community String

Traps  Disabled

Save

Figure 9

**SNMP Interface** — SNMP stands for Simple Network Management Protocol) is an Internet application protocol that manages and monitors network device functionality.

Scigiene uses SNMP version

1. These settings can both be configured both on Scigiene Premier and the local interface. See Figure 9.

**Inbound IP Range Start and End** - This is the accepted IP address range for the SNMP client. The gateway will only accept communication requests from IP addresses in this range.

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

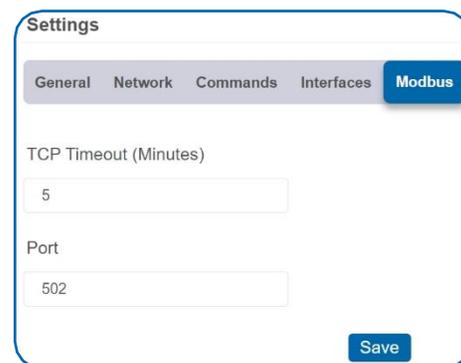
**SNMP Community String** — This is used as a configurable password for clients within the accepted IP Range. Communication will not be allowed if the Community String does not match. The default will be set to “public”

**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.

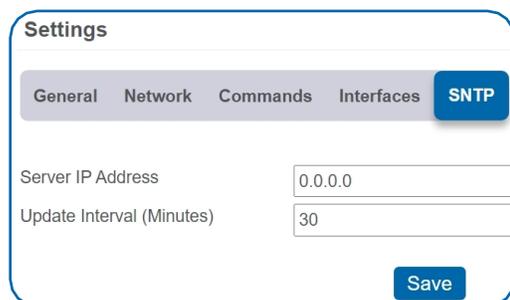
**Trap Port** — The server port where the trap alert state is sent when active.

**Modbus Interface** — Modbus TCP (Transmission Control Protocol) is the Modbus RTU protocol with a TCP interface that runs on Ethernet. Scigiene provides the Modbus TCP interface for you to pull gateway and 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 gateway. See Figure 10.



The screenshot shows the 'Settings' page with the 'Modbus' tab selected. It features two input fields: 'TCP Timeout (Minutes)' with the value '5' and 'Port' with the value '502'. A 'Save' button is located at the bottom right.

Figure 10



The screenshot shows the 'Settings' page with the 'SNTP' tab selected. It features two input fields: 'Server IP Address' with the value '0.0.0.0' and 'Update Interval (Minutes)' with the value '30'. A 'Save' button is located at the bottom right.

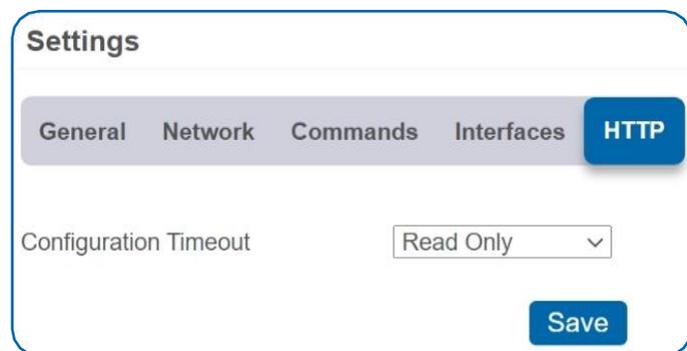
Figure 11

**SNTP Interface** — SNTP is a synchronized computer clock on a network. An SNTP server can be set up on the same LAN as the gateway, such as on a router or a Linux computer. The gateway should be configured to retrieve time from only trusted servers, such as ones maintained by your ISP. Incorrect time can affect the delivery of sensor traffic.

If the ScigieneServer 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. See Figure 11.

**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, you may configure the local HTTP interface to remain Read Only, or to be disabled after 1 minute, 5 minutes, 30 minutes, or always active. See the next section for more on the local interface.

See Figure 12.



The screenshot shows the 'Settings' page with the 'HTTP' tab selected. It features a dropdown menu for 'Configuration Timeout' with 'Read Only' selected. A 'Save' button is located at the bottom right.

Figure 12

## VI. INSTALLING SCIGIENE EXPRESS AND MINE

Gateways can be used to locally monitor wireless sensors on a computer without needing an external Internet connection. In order to use an Ethernet Gateway 4 with the PC application, you need to make sure that both the gateway and PC are connected to the same network, and configure the gateway to talk directly to the computer software instead of using the Internet.

### INSTALLING SCIGIENE EXPRESS SOFTWARE

When you purchase the Scigiene Express software you will receive an activation code. See Figure 13.

1. Visit to download and install the Scigiene Express software. When you finish installing the software, launch the program and click on **Configuration** then **Enter Key**. Enter your key in the box and select **Activate**.



Figure 13

2. Next, you will need to add your Ethernet gateway and any sensors you wish to use with the software.
  - Go to Scigiene Software
  - Enter the Gateway ID and Security Code included on the label directly under the QR code on the bottom of your gateway.
  - Select the button for Gateway Server Settings.
  - You must have an IP address to your server running the Express software. Choose your port and whether this is a dynamic or static DHCP. Then press the Submit button.
  - Enter the key code.

### INSTALLING SCIGIENE MINE SOFTWARE

Scigiene MINE is an open software platform that provides the ability to integrate Scigiene wireless sensors and gateways with your own software system. Scigiene wireless gateways can be unlocked, allowing them to be directed to a custom host or IP address, where an installation of Scigiene MINE works as a translation application between Scigiene wireless sensors networks and existing or custom software applications.

Next, you will need to add your Ethernet gateway and any sensors you wish to use with the software.

- Go to Scigiene Software
- Enter the Gateway ID and Security Code included on the label directly under the QR code on the bottom of your gateway.
- Select the button for **Gateway Server Settings**.
- You must have an IP address to your server running your custom software that implements the mine libraries. Choose your port and whether this is a dynamic or static DHCP. Then press the **Submit** button.
- Enter the key code.

## VII. USING THE LOCAL INTERFACE

If using Scigiene Premier is not an option, you can set up your gateway and sensors offline through the local web interface. This interface is enabled by default, but is configured to be read only. To make changes using this interface, the interface must be configured to allow changes to the device. Follow this procedure to enable configuration temporarily:

- Connect the gateway's Ethernet cable to your computer directly.
- Plug in the gateway to a power outlet.
- Press and hold the utility button while the gateway is booting and the lights are scrolling. At the end of the boot process, all lights will be green for two seconds then shift to red. Release the button and the local web interface will be temporarily write-enabled (indicated by the lights flashing green quickly).
- After 30 seconds, the gateway's lights will all blink red rapidly. This means the gateway is in AUTO IP mode if DHCP is enabled. After an additional 30 seconds, the computer will also be in this networking mode (no internet).
- Using a web browser type in the IP Address currently assigned to the gateway. When the gateway is in AUTO IP mode, the IP Address is always 169.254.100.1. The browser should then load the status page for this gateway.

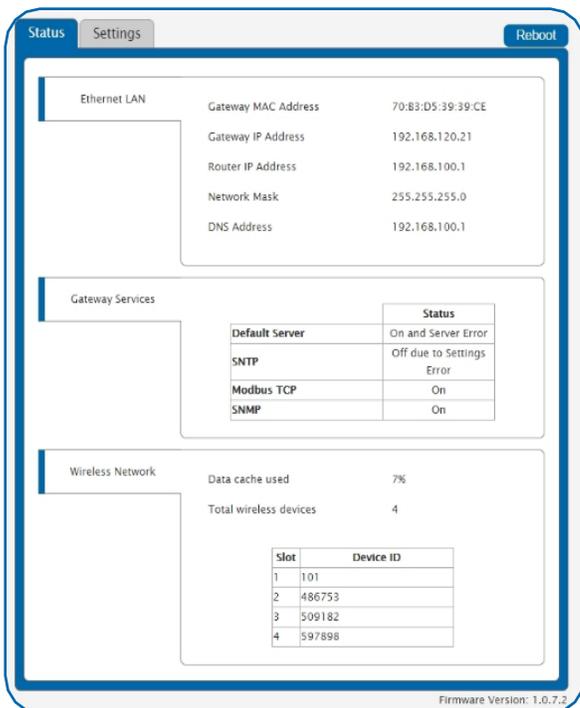
### Note

- When the gateway is connected to a router or other internet access point, the local interface is reachable through the DHCP assigned IP Address, or the configured Static IP Address.
- Each time a page is refreshed, the temporary timer to access these pages with configuration authorized will reset.
- If the interface is not used for 5 minutes or the gateway restarts, the HTTP interface will become read-only.

## STATUS TAB

### Ethernet LAN (Local Area Network Status)

This is a read only section listing the current conditions for your Local Area Network. see Figure 14.



**Gateway MAC Address** - This is the media control address of your gateway to exclusively identify the device to a Network Interface Controller.

**Gateway IP Address** - This is a network address for your gateway when it is connected to the Internet.

**Router IP Address** - This is a network address 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.

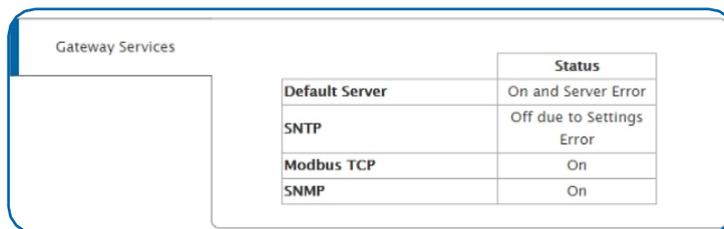
**DNS Address** - A Domain Name System is the method employed by a URL of translating the alphabetic entry in an address bar into a numerical address associated with a server.

Figure 14

## Gateway Services

See Figure 15.

**Gateway Services Table** - These status fields indicate the current operation status for each data interface. The status field will indicate when the appropriate service is "On," "On and Server Error," "On and Synced," "On and Traps Ready," "Off," "Off due to Settings Error."



	Status
Default Server	On and Server Error
SNTP	Off due to Settings Error
Modbus TCP	On
SNMP	On

Figure 15

## Wireless Network Status

See Figure 14.

**Gateway data cache used** - This percentage represents the amount of internal flash memory storage for holding sensor messages has been used out of the maximum (896 kB). Messages sent from wireless sensors are stored temporarily in the gateway cache until a data interface (i.e., Default Server, SNMP, Modbus, etc.) confirms the data has been stored or transmitted elsewhere.

**Total Wireless Devices** - Below the gateway data cache is a section listing the number of sensors communicating with the gateway. A table below this number shows the exact slot number and device identification number associated with the gateway. There is a maximum of 256 available slots.

## SETTINGS TAB

### Ethernet LAN

See Figure 16.

From the Local Area Network Configuration tab, you can modify settings for your IP address, NeMork Mask, Default Gateway, and DNS Server.

### Local Area Network Settings

In this section, you can make edits to your Local Area Network settings discussed on page 12.

### HTTP Interface Settings

**HTTP Interface:** The radio button for "Enable" will be active by default, allowing you to access the local interface. Choosing the "Disable" radio button and saving your changes will automatically log you out of the local interface. Follow the steps on page 12 to log back in.

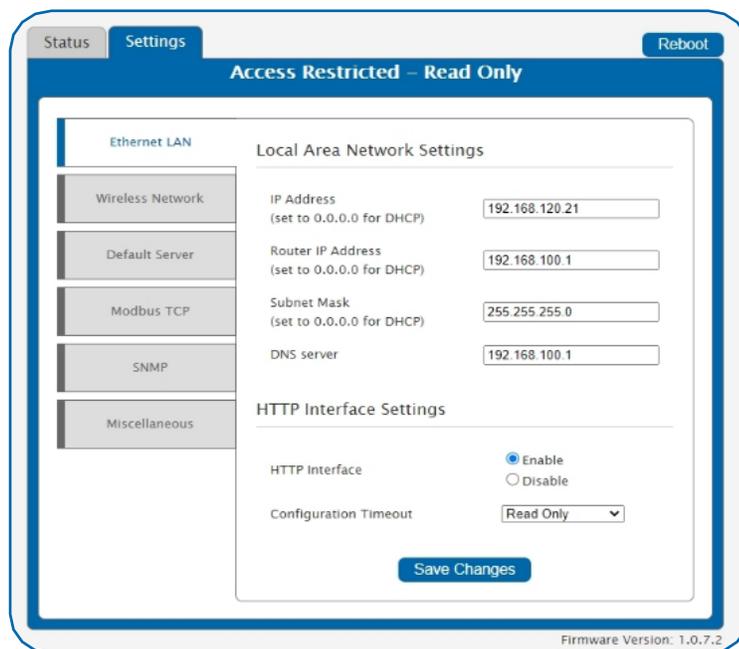
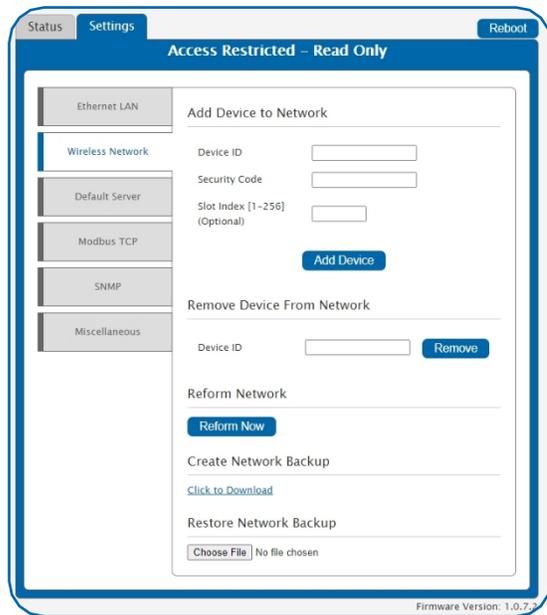


Figure 16

**Configuration Timeout:** This allows you to set a time limit of 1 minute, 5 minutes, and 30 minutes for how long the local interface is active. "Read Only" keeps the interface active, but you cannot make any changes. You can only change the settings out of read through the HTTP Interface on Scigiene Premier; see page 10. "Always Available" makes the interface always open and editable.

## Wireless Network

See Figure 17.



### **Add Device to Network**

This section will allow you to add sensors and gateways to your account through the local interface.

**Device ID** - This is a unique numerical identifier included with your gateway and sensors listed on the back label.

**Security Code** - This is an alphabetical six letter code included with your devices listed on the back label.

**Slot Index** - The slot index is an optional setting for assigning your gateway. If a Slot ID is entered, the device will be added to the appropriate slot in the Wireless Device List. If a slot ID is not entered, the device will be added to the first available slot.

### **Remove Device from Network**

This section will allow you to remove a sensor or gateway from your account by typing in the numerical Device ID and selecting the "Remove" button.

### **Reform Network**

Selecting the "Reform Now" button will remove all devices from the current Wireless Device List.

### **Create Network Backup**

Choosing the "Click to Download" link will download a network backup for your gateway and sensors contained within an XML file.

### **Restore Network Backup**

Choose a previously downloaded XML network backup file to load through the Local Interface.

## Default Server

See Figure 18.

### **Default Server Settings**

The default server is the Scigiene server. It is the only option enabled by default.

The **Heartbeat Minutes** configures the interval that the gateway checks in with the server. The default is five minutes. So, every five minutes your gateway will report to the server.

When your sensors detect a threshold breach, they enter what is called an "aware state." The **On Aware Messages** toggle is set to "Trigger Heartbeat" by default. This means the gateway will check in with the server address immediately and relay the aware state information to Scigiene Premier.

Leaving this set to the default "Wait for Heartbeat" setting will tell the gateway to wait for its set heartbeat to elapse before communicating with the server.

The **On Server Loss** field sets what you wish to happen when the gateway loses communication with the server. The default setting "Log Sensor Data" commands the gateway to continue communicating with your sensors and store readings until it can re-establish a connection to the server.

toggling this to "Disable Wireless Network" will force the sensors communicating with this gateway to find a new gateway in order to deliver sensor messages to the server immediately.

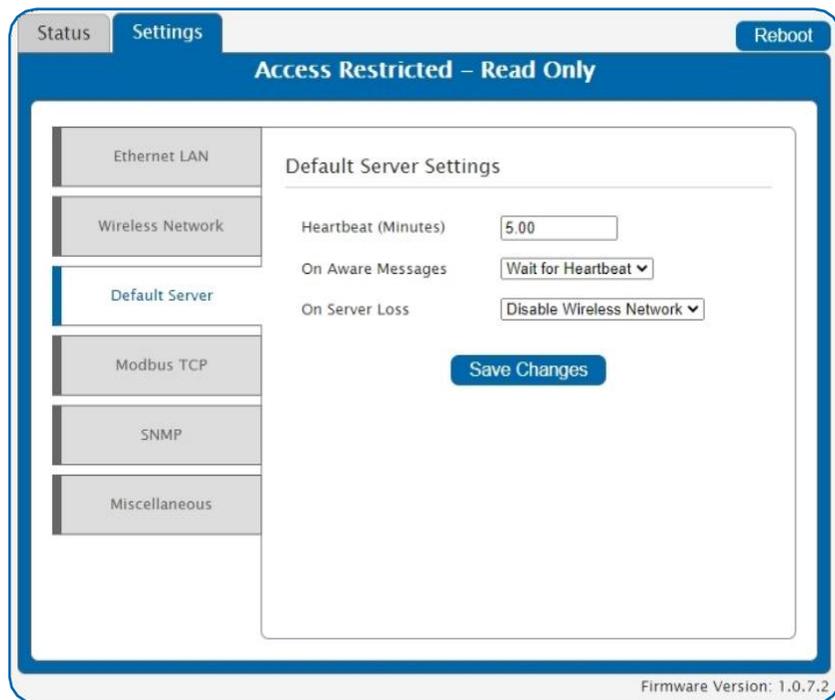


Figure 18

## **Modbus TCP (Transmission Control Protocol)**

See Figure 19.

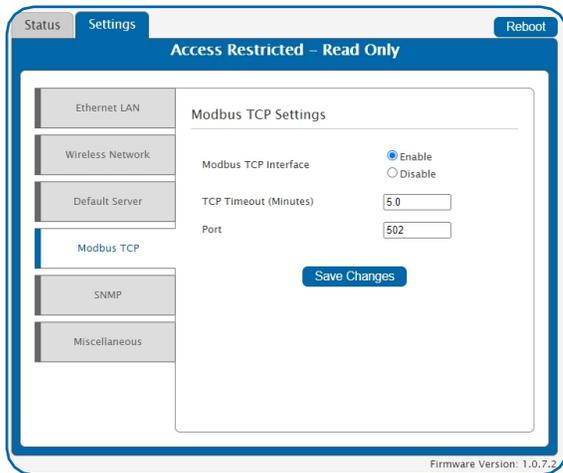


Figure 19

### **Modbus TCP Settings**

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. Additionally, only the "current" data points are available for reading. Historical sensor information is not available. See Figure 19.

The Modbus TCP Interface will store all data values in 16-bit registers. The registers and their associated data fields are mapped below. To access the sensor holding registers for a particular device, 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 gateway 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 gateway local web interface status.htm 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:

#### **DATA ADDRESS:**

Sensors information starts at  $100 + 16 ( \text{Slot Number} - 1 )$

#### **REGISTER ADDRESS:**

Sensors information starts at  $40101 + 16 ( \text{Slot Number} - 1 )$

Slot Number	Data Address	Register Address
1	100	40101
2	116	40117
256	4180	44181

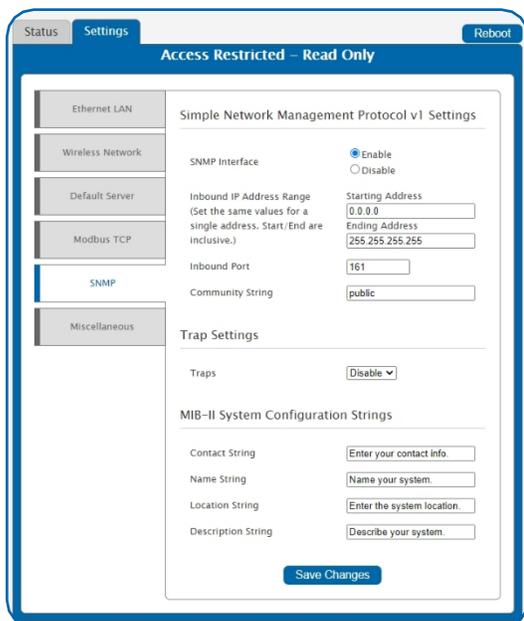
GATEWAY HOLDING REGISTERS			
Field	Description	Register	Data Address
Gateway ID_High	The first 16 bits of a 32-bit serial ID number.	40001	0
Gateway ID_Low	The last 16 bits of a 32-bit serial ID number.	40002	1
Gateway Version Revision + Major	The gateway firmware Revision and Major version numbers (1 byte each)	40003	2
Gateway Version Minor + Release	The gateway firmware Minor and Release version numbers (1 byte each)	40004	3
Gateway Device Count	The number of devices in its wireless network.	40005	4

SENSOR HOLDING REGISTERS (Slot 1)			
Field	Description	Register	Data 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

The data listed in the registers above will be in raw format and will need to be converted to into usable information. The Modbus TCP Data Interpretation document can be requested from Scigiene.

## SNMP

See Figure 20.



The screenshot shows a web interface for configuring SNMP settings. The page title is "Access Restricted - Read Only". On the left, there is a navigation menu with options: Ethernet LAN, Wireless Network, Default Server, Modbus TCP, SNMP (selected), and Miscellaneous. The main content area is titled "Simple Network Management Protocol v1 Settings". It includes a "SNMP Interface" section with radio buttons for "Enable" (selected) and "Disable". Below this is the "Inbound IP Address Range" section, which includes fields for "Starting Address" (0.0.0.0) and "Ending Address" (255.255.255.255), and an "Inbound Port" field (161). The "Community String" field is set to "public". There is also a "Trap Settings" section with a "Traps" dropdown menu set to "Disable". At the bottom, there is a "MIB-II System Configuration Strings" section with fields for "Contact String", "Name String", "Location String", and "Description String". A "Save Changes" button is located at the bottom center of the form.

Figure 20

### Simple Network Management Protocol v1 Settings

**SNMP**, Simple Network Management Protocol, settings for a gateway 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 by the gateway. This gateway supports SNMP version 1. See Figure 20 through 22.

- **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 gateway is received.
- **SNMP Community String** — This is used as a configurable password for clients within the accepted IP Range. Communication will not be allowed if the Community String does not match. The default will be set to "public"

### Trap Settings

You have the option to "Enable" or "Disable" your trap settings. Choosing "Enable" brings up selections for on **Authentication Failure, on New Sensor Data, and on Sensor Alarms**. Your **Trap Address** is the IP Address for the SNMP Server where the trap will be sent. Your **Trap Port** is the server port where the trap alert state is sent when active.

### MIB-II System Configuration Strings

Although it is not necessary, it is a good idea to set the contact, name, location and description strings available at the bottom of the SNMP configuration page on the local interface.

## SNMP Client Configuration

The MONNIT-EGW4.mib file is available to download from monnit.com and will provide proper field names for data points specific to EGW4 and sensor data in your SNMP client.

### Data Interpretation

After loading the MONNIT-EGW4.mib file to your SNMP Client you will be able to poll data in several table view formats that have already been configured by Scigiene.

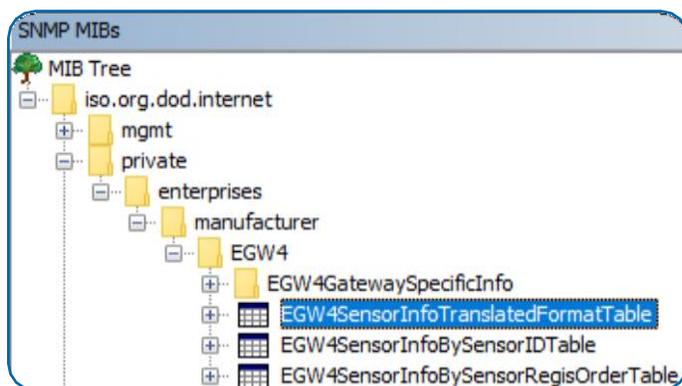


Figure 21

Data presented in the EGW4SensorInfoTranslatedFormat Table will be converted into usable information. The other tables listed here will display raw data. The SNMP Data Interpretation document can be requested by contacting Scigiene directly. It will explain how the raw data can be converted into usable information.

### Miscellaneous System

See Figure 22.

### Simple Network Time Protocol Settings



Figure 22

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

**Enable / Disable:** You have the option to enable or disable the SNTP Interface. Disabling the the SNTP will cause your time settings to be synchronized through Scigiene Premier.

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

#### Interface Data Management

**Data Expiration (Hours) -** Data expiration in the Gateway. After this time has elapsed, the data pulled for Modbus and SNMP will be zero-ed out.

## Auto Reboot Settings

The **Auto Reset** field is the amount of time in hours that the Local Interface will automatically reboot. Setting this to 0 will disable the feature. The maximum setting is 8760 hours.

## Reset Memory

**Reset Data Memory button:** Pressing this wipes stored sensor readings from the gateway, but all the changes you made to your settings remain intact.

**Reset Configuration Memory button:** Pressing this reboots all your settings back to the factory defaults.

## TROUBLESHOOTING

### LED Indicators

**Ethernet Cable Not Detected** - The Bottom LED will blink red twice rapidly to indicate the Ethernet Cable is not being detected. Double check the Ethernet connection or change Ethernet Cable if the problem continues.

\*Note - If the Ethernet Cable is not detected the Middle LED on the gateway will turn Solid Red. This indicates the gateway is not able to communicate with the Default Server, or other configured services.

**Gateway Services** - Problems with any of the gateway services will be indicated by the Middle LED being Solid Red. This includes HTTP, NTP, Modbus TCP, SNMP, and the Default Server. To see which service is encountering the error use the Local Interface.

When ALL of these services have been configured OFF, the Middle LED will be OFF. If this occurs, a Factory Reset will recover the device.

**Wireless Sensor Network** - If there is a problem communicating with the Wireless Sensor Network (WSN) then the Top LED will be Solid Red. Power off the gateway for 10 seconds. If the problem persists please contact ScigieneSupport.

\*Note - The gateway can be configured to disable the WSN when communication with the server fails. In this case, the Top LED will be Solid Red.

### Will Not Connect to Scigiene Premier

The Ethernet Gateway operates on a local Ethernet network which requires a connection to the Internet in order to deliver data to the Scigiene Premier Online portal. There are a few conditions which must be met in order to allow for the traffic to be successfully delivered to the Scigiene Premier Online portal:

- Confirm the device has been added to an Scigiene Premier Online account.
- Confirm the gateway is connected to power and completes the start-up test.
- Confirm the gateway is operating on the local Ethernet network with a valid IP address.
- Confirm the network allows for traffic to the internet over outbound TCP port 3000 (inbound port is not specified), and the DNS server on the network can resolve sensorsgateway.com.
- Restore Factory Defaults - Press and hold the Utility Button for 10 seconds.
- Update the gateway's firmware if an update is available once the gateway has successfully connected to Scigiene Premier.

## SUPPORT

For technical support and additional troubleshooting tips, please visit our support knowledge base online. If you are unable to solve your issue using our online support, email Scigiene support at [support@scigiene.com](mailto:support@scigiene.com) with your contact information and a description of the problem, and a support representative will contact you within about one business day.

For error reporting, please email a full description of the error to [support@scigiene.com](mailto:support@scigiene.com).

## WARRANTY INFORMATION

(a) Scigiene warrants that Scigiene-branded products (Product) 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. Scigiene may resell sensors manufactured by other entities and are subject to their individual warranties; Scigiene will not enhance or extend those warranties. Scigiene does not warrant that the software or any portion thereof is error free. Scigiene 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, Scigiene shall provide a bug fix or software patch correcting such non-conformance within a reasonable period after Scigiene receives from customer (i) notice of such non-conformance, and (ii) sufficient information regarding such non-conformance so as to permit Scigiene to create such bug fix or software patch. If any hardware component of any Product fails to conform to the warranty in this section, Scigiene 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 Scigiene receives from customer (i) notice of such non-conformance, and (ii) the non-conforming Product provided; however, if, in its opinion, Scigiene 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 Scigiene. 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 Scigiene a Return Material Authorization Number (RMA) prior to returning any Products to Scigiene. 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 Scigiene is notified within one year of customer's receipt of the Product. Scigiene reserves the right to repair or replace Products at its own and complete discretion. Customer must obtain from Scigiene a Return Material Authorization Number (RMA) prior to returning any Products to Scigiene. Products returned under this Warranty must be unmodified and in original packaging. Scigiene 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 Scigiene at standard labor rates for a period of one year from the customer's original date of receipt.

(b) As a condition to Scigiene's obligations under the immediately preceding paragraphs, customer shall return Products to be examined and replaced to Scigiene's facilities, in shipping cartons which clearly display a valid RMA number provided by Scigiene. 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. Scigiene shall deliver replacements for Products determined by Scigiene to be properly returned.

(c) Scigiene'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. Scigiene's warranty obligations shall run solely to customer, and Scigiene 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. SCIGIENE'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 SCIGIENE BE LIABLE FOR SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES. THE PRICE STATED FOR THE PRODUCTS IS A CONSIDERATION IN LIMITING SCIGIENE'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, SCIGIENE 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.

## CERTIFICATIONS

### United States FCC

This equipment has been tested and found to comply with the limits for a Class B digital devices, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television 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 more 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 the dealer or an experienced radio/TV technician for help

**Warning:** Changes or modifications not expressly approved by Scigiene could void the user's authority to operate the equipment.

### RF Exposure

---

 **WARNING:** To satisfy FCC RF exposure requirements for mobile transmitting devices, the antenna used for this transmitter must not be co-located in conjunction with any antenna or transmitter.

---

### **Scigiene and GEN 2 Wireless Sensors, Wireless Sensor Adapters and Ethernet Gateways:**

*This equipment complies with the radiation exposure limits prescribed for an uncontrolled environment for fixed and mobile use conditions. This equipment should be installed and operated with a minimum distance of 20 cm between the radiator and the body of the user or nearby persons.*

### **All GEN 2 Wireless Sensors and Gateways Contain FCC ID: ZTL-G2SC1.**

#### **Approved Antennas**

*GEN 2 devices have been designed to operate with an approved antenna listed below, and having a maximum gain of 14 dBi. Antennas having a gain greater than 14 dBi are strictly prohibited for use with this device. The required antenna impedance is 50 ohms.*

- Xianzi XQZ-900E (5 dBi Dipole Omnidirectional)
- HyperLink HG908U-PRO (8 dBi Fiberglass Omnidirectional)
- HyperLink HG8909P (9 dBd Flat Panel Antenna)
- HyperLink HG914YE-NF (14 dBd Yagi)
- Specialized Manufacturing MC-ANT-20/4. 0C (1 dBi 4" whip)

## Canada (IC)

---

### **English**

*Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the Equivalent isotopically Radiated Power (E.I.R.P.) is not more than that necessary for successful communication.*

*The radio transmitters (IC: 9794A-RFSC1, IC: 9794A-G2SC1, IC: 4160a-CNN0301, IC: 5131A-CE910DUAL, IC: 5131A-HE910NA, IC: 5131A-GE910 and IC: 8595A2AGQN4NNN) have been approved by Industry Canada to operate with the antenna types listed on previous page with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.*

*This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.*

**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 same precautions should be taken if manually inserting a SIM card, checking carefully the instruction for its use. Do not insert or remove the SIM when the product is in power saving mode.*

*Every device has to be equipped with a proper antenna with specific characteristics. The antenna has to be installed with care in order to avoid any interference with other electronic devices and has to guarantee a minimum distance from the body (23 cm). In case this requirement cannot be satisfied, the system integrator has to assess the final product against the SAR regulation.*

**Additional Information and Support**

For additional information or more detailed instructions on how to use your Scigiene Wireless Sensors or the Scigiene Premier Online System, please visit us on the web.



1295 Morningside Avenue, Unit 16-18  
Scarborough, ON M1B 4Z4 Canada  
Phone: 416-261-4865 Fax: 416-261-7879  
[www.scigiene.com](http://www.scigiene.com)

