



# GEN 2 4G Cellular Gateway USER GUIDE



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)

## IMPORTANT!

For best results, please wait to power on your GEN 2 4G Cellular Gateway until after you have created an Scigiene Premiere account and added the gateway and sensors to your new 4G Cellular network.

# Table of Contents

<b>1. ABOUT THE GEN 2 4G Cellular GATEWAY</b>	<b>1</b>
GEN 2 4G Cellular 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	3
DATA SECURITY ON THE GATEWAY	3
SERVER COMMUNICATION SECURITY	3
<b>IV. GATEWAY REGISTRATION</b>	<b>4</b>
REGISTERING THE GEN 2 4G Cellular GATEWAY	4
<b>V. USING THE 4G Cellular GATEWAY</b>	<b>5</b>
USING THE 4G Cellular GATEWAY	5
UNDERSTANDING THE GATEWAY LIGHTS	5
4G Cellular GATEWAY SETTINGS	6
<b>VI. USING THE LOCAL INTERFACE</b>	<b>11</b>
GATEWAY STATUS TAB	11
ETHERNET NETWORK SETTINGS	14
CELLULAR NETWORK	15
WIRELESS NETWORK	17
MISCELLANEOUS	18
<b>SUPPORT</b>	<b>19</b>
<b>WARRANTY INFORMATION</b>	<b>19</b>
<b>SAFETY INFORMATION</b>	<b>22</b>

## I. ABOUT THE GATEWAY

The Scigiene GEN 2™ 4G Cellular Gateway uses 4G LTE CAT-M1/NB2 cellular technology to control GEN 2 Wireless Sensor settings without additional IT infrastructure. All you need is a power source and the Scigiene Premiere cloud platform to monitor your environment and equipment using Scigiene's industry-leading wireless devices.

The GEN 2 4G Cellular Gateway will communicate with GEN 2 Sensors and Scigiene Premiere to deliver data and send alerts about various machine, equipment, or area conditions.

The 4G Cellular Gateway and Scigiene Premiere work together to connect and configure GEN 2 Sensor over the Internet and make their data accessible virtually anytime, anywhere. The 4G Cellular Gateway provides the crucial link that connects GEN 2 Sensors to Scigiene Premiere using 4G LTE CAT-M1/NB2 (4G Long-Term Evolution Category M1/NarrowBand-Internet of Things (NB-4G Cellular) 2) cellular technology. The gateway is equipped with a 24-hour backup battery. GEN 2 Sensors will continue to communicate with Scigiene Premiere via cellular transmission in the event of a power outage. Additionally, the cellular gateway comes with an RJ-45 Ethernet jack (future capability) for local device configuration. The 4G Cellular Gateway, however, is ideal for applications without a wired Internet connection or where infrastructure is dedicated to other resources.

### GEN 2 4G Cellular GATEWAY FEATURES

- 4G LTE CAT-M1/NB2 cellular technology
- Wireless range of 1,200+ feet through 12+ walls<sup>1</sup>
- Frequency-Hopping Spread Spectrum (FHSS)
- Best-in-class interference immunity
- Encrypt-RF Security (256-bit Diffie-Hellman Key Exchange + AES-128 CBC for sensor data messages)
- 32,000 sensor message memory<sup>2</sup>
- Over-the-air (OTA) updates (future-proof)
- True plug and play, no hassles for Internet configuration setup
- No PC required for operation
- Local status LEDs with transmission and online status indicators
- AC power supply
- 24-hour battery backup in the event of a power outage
- RJ-45 10/100BASE-TX Ethernet jack for configuration (future capability)

Actual range may vary depending on the environment.

Total messages in memory varies with sensortype. (32,000 is for Temperature Sensors. Additional information available at Scigiene.com)

### EXAMPLE APPLICATIONS

Remote Location and Asset 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 4G Cellular Gateway manages communication between GEN 2 Sensors and Scigiene Premiere. When running, the gateway will periodically transmit data on a Heartbeat (a preset interval in minutes). The gateway will store data it received from sensors until its next Heartbeat.

The GEN 2 4G Cellular Gateway is a cellular (LTE-M or CAT-M1) gateway. It uses its connection to relay data received from sensors to Scigiene Premiere cloud-based software. Sensors communicate with the gateway, then the gateway relays information to Scigiene Premiere.

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

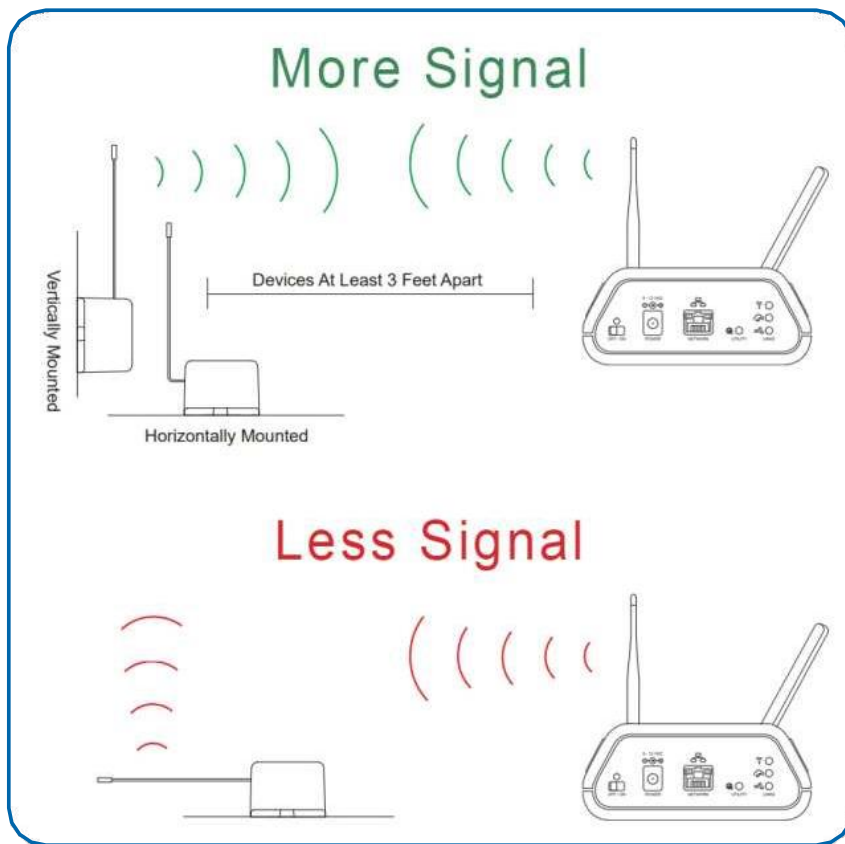


Figure 1

### **III. GATEWAY SECURITY**

The GEN 2 4G Cellular Gateway is designed and built to manage data from sensors monitoring your environment and equipment securely. The same methods used by financial institutions to transmit data are also used in Scigiene security infrastructure. The 4G Cellular Gateway's security features 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. Packet-level encryption and verification are vital in ensuring traffic isn't altered between sensors and gateways. All data is transmitted securely from your devices, with a best-in-class range and a power consumption protocol.

#### **SENSOR COMMUNICATION SECURITY**

Wireless devices listening on open communication protocols cannot eavesdrop on GEN 2 Sensors. Scigiene's sensor-to-gateway implements Encrypt-RF<sup>®</sup>. This creates a secure wireless tunnel, 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. This minimizes power consumption to optimize battery life. Thanks to this combination, Scigiene offers robust bank-grade security at every level.

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

The GEN 2 4G Cellular Gateway prevents prying eyes from accessing the data stored on the sensors. The GEN 2 4G Cellular Gateway doesn't run on an off-the-shelf, multi-function operating system. Instead, it runs a purpose-specific, real-time embedded state machine that can't 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 data from attackers and protects the gateway from becoming a relay for malicious programs.

#### **SERVER COMMUNICATION SECURITY**

Communication between your GEN 2 4G Cellular Gateway and Scigiene Premiere is secured by packet-level encryption with Encrypt-RF<sup>®</sup>. Similar to the security between the sensors and the gateway, the gateway and the 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 VPNs for privacy. The gateway can still operate within a VPN if it is present.

## IV. GATEWAY REGISTRATION

If this is your first time using the Scigiene Premiere online portal, you'll 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 Premiere account, please consult the Scigiene Premiere User Guide.

### REGISTERING THE GEN 2 4G Cellular GATEWAY

You will need to enter the **Device ID** and the **Security Code (SC)** from the GEN 2 4G Cellular Gateway in the corresponding text boxes. Use the camera on your smartphone to scan the QR code on your gateway. If you don't have a camera on your phone, or are accessing Scigiene Premiere through a desktop computer, you may enter the Device ID and SC manually. See Figure 2.

The **Device ID** is a unique number located on each device label.

Next, you'll be asked to enter the SC on your device. The SC will be all letters, no numbers. It can also be found on the barcode label of the gateway.

When completed, select the **Submit** button.



Figure 2

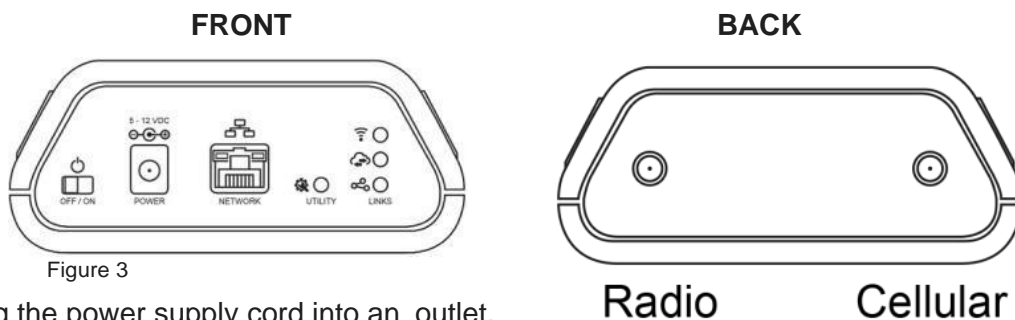
A screenshot of the 'Add Device' web form. The form has a title 'Add Device' and a help icon. It shows a diagram of a smartphone scanning a QR code on a device. Below the diagram is a green 'Scan Barcode' button. Underneath is a separator '- OR -'. Then there are two sections: 'Device ID \*' with a sub-label 'ID Number' and a text input field, and 'Code \*' with a sub-label 'Security Code' and a text input field. At the bottom left is a 'Submit' button. At the bottom right is a question 'Finished adding devices?' followed by a 'Continue' button.

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

## V. USING THE 4G Cellular GATEWAY

### USING THE 4G Cellular GATEWAY

1. Attach the cellular and GEN 2 antennas to the back of the gateway at the locations depicted in Figure 3.



2. Plug the power supply cord into an outlet.
3. Toggle the power switch on.
4. After the three LEDs switch to green, your network is ready to use.

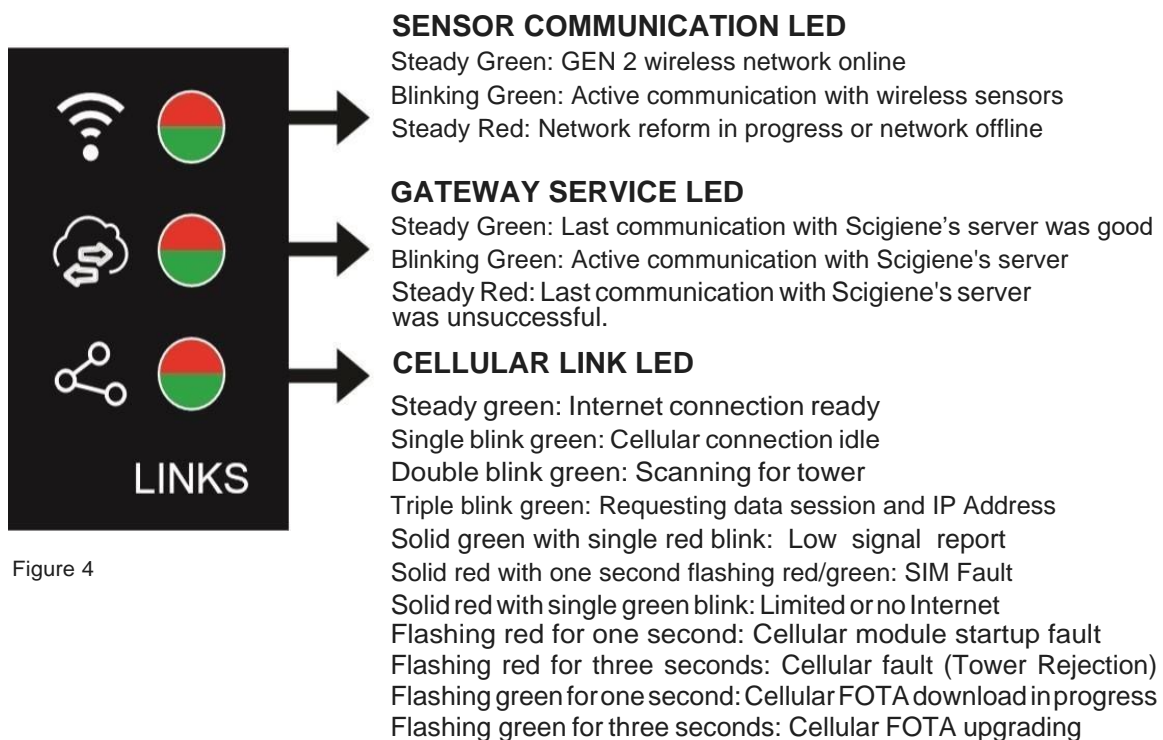
### UNDERSTANDING THE 4G Cellular GATEWAY LIGHTS

The gateway will enter three stages as it powers on:

**Power-on stage:** The gateway analyzes electronics and programming. The LEDs will flash red and green, before turning green for two seconds. In case of a hardware failure, the light sequence will repeat continually. Please contact technical support if the LEDs aren't green after five minutes.

**Connection stage:** The gateway will attempt to start the cellular, gateway service, and wireless network connections. See diagram below to decode the three LEDs and the states the LEDs indicate.

**Operational stage:** If the Gateway Power Mode is set to "Forced High Power" or "Standard Power" and Line Power is present, all of the LEDs will remain green while powered externally, unless reporting activity on a connection or if there is an issue. If the Gateway Power Mode is set to "Forced Low Power" or "Standard Power" without Line Power being present, the gateway will only use the active light sequence when the gateway is communicating to the server. Otherwise, the LEDs are powered off.





**Note: When setting up the gateway, initial tower connections may take 2-20 minutes depending on the carrier/SIM specific setup and the number of cellular bands enabled. Subsequent connections are typically faster.**

## 4G Cellular GATEWAY SETTINGS (SCIGIENE PREMIERE)

The 4G Cellular 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. Choose the 4G Cellular Gateway from the list of gateways registered to your account. Select the “Settings” tab to edit the gateway.

### General Settings

Settings

General Ethernet Cellular Commands HTTP Interface

Gateway Name  
IOT Gateway - XXXXX

Heartbeat Minutes (default: 15)  
10

On Aware Messages  
Wait for Heartbeat ☒ Trigger Heartbeat

On Server Loss  
Log Sensor Data ☒ Disable Wireless

Gateway Power Mode  
Standard

Save

Figure 5

A. 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.

B. The Heartbeat Minutes configures the interval that the gateway periodically checks in with the server. The default is fifteen minutes, meaning the gateway will report to the server every fifteen minutes.

C. On Aware Messages configuration indicates if the Aware Message arrival event will **Trigger** Heartbeat (default) or Wait for Heartbeat. When the switch is toggled to Trigger Heartbeat, the gateway is configured to immediately report to the server. When toggled to Wait for Heartbeat, the message is

stored until the gateway is scheduled to communicate before connecting with the server and delivering the message.

D. On Server Loss configuration indicates if the wireless network on the gateway will stay active and Log Sensor Data (default) or if the gateway will Disable Wireless network. In networks with multiple gateways, forcing the sensors to switch to an active gateway will enable more timely delivery of data to the server.

E. The Gateway Power Mode allows you to choose between Standard Power (default), Force Low Power, and Force High Power, from a drop-down menu. Standard means that your gateway will keep lights and cellular transmission active when plugged into an outlet. On battery power, the gateway will power down lights and the cellular connection between communications. Force Low Power means your gateway will always power down the lights and the cellular connection when not talking to the server. Force High Power means your gateway will always keep the lights and cellular transmission active, regardless of whether or not the gateway is plugged in.



### **Ethernet Settings (future capability)**

Choose the Ethernet Settings tab under **Settings** to open up the configuration page for the Local Area Network (LAN). The LAN is used for local configuration options when server connectivity is not possible. This page includes the ability to switch your network Internet Protocol (IP) Address from DHCP assigned to Static. A DHCP assigned address will be the default network IP Address.

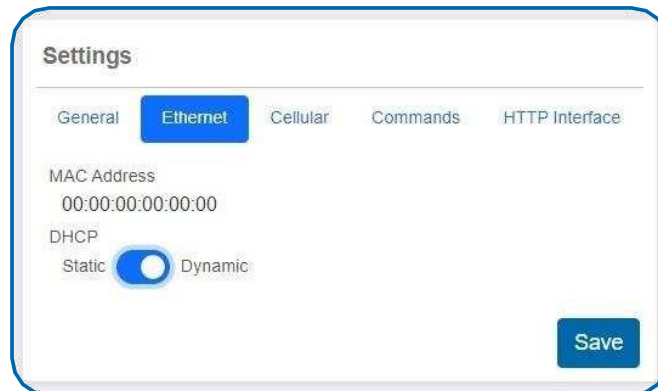
The screenshot shows the 'Settings' application with the 'Ethernet' tab selected. The 'MAC Address' is displayed as '00:00:00:00:00:00'. Under the 'DHCP' section, the 'Static' radio button is selected and highlighted with a blue circle, while the 'Dynamic' radio button is unselected. A 'Save' button is located at the bottom right of the form.

Figure 6

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.

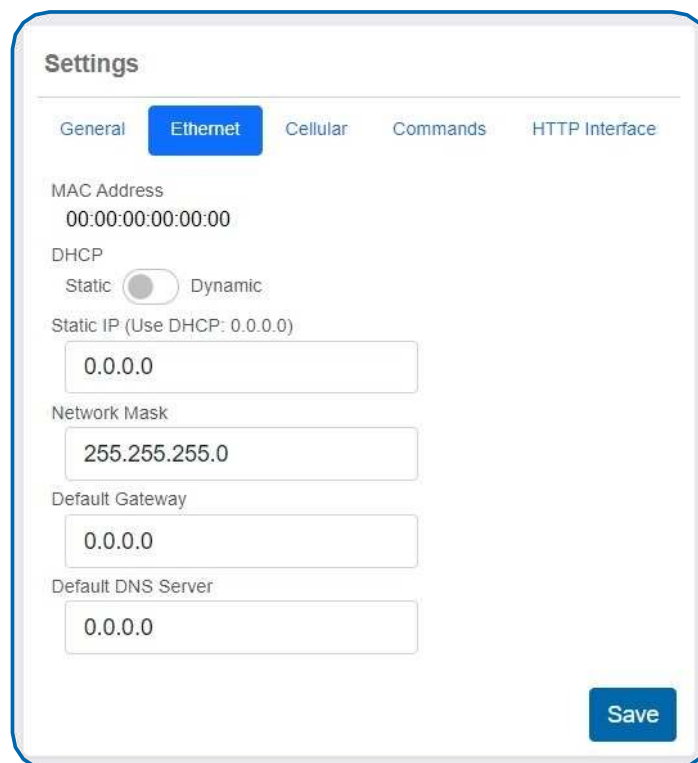
The screenshot shows the 'Settings' application with the 'Ethernet' tab selected. The 'MAC Address' is '00:00:00:00:00:00'. Under the 'DHCP' section, the 'Dynamic' radio button is now selected, and the 'Static' radio button is unselected. Below this, there are four text input fields: 'Static IP (Use DHCP: 0.0.0.0)' with the value '0.0.0.0', 'Network Mask' with '255.255.255.0', 'Default Gateway' with '0.0.0.0', and 'Default DNS Server' with '0.0.0.0'. A 'Save' button is at the bottom right.

Figure 7

**Static IP** - A static IP Address is a numerical sequence assigned to a computer by a network administrator. This is different from a Dynamic IP Address. 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 the gateway utilizes to relay data to the Internet. Typically, your router IP Address.

**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.

## Cellular Settings

- A.** The Global System for Mobile Communications utilizes a 15-digit IMSI (International Mobile Subscriber Identity) number as the primary mode to identify the country, mobile network, and subscriber. It is formatted as MCC-MNC-MSIN. MCC is the Mobile Country Code. MNC is the Mobile Network Code attached to the cellular network. MSIN is a serial number making the IMSI unique to a subscriber.
- B.** The ICCID is the 19-digit unique identification number corresponding to the cellular SIM card. It is possible to change the information contained on a SIM (including the IMSI), but the identity of the SIM remains the same.
- C.** IMEI (International Mobile Equipment Identity) is a number exclusive to your LTE International Gateway to identify the gateway to the cell tower. The Global System for the Mobile Communications network stores the IMEI numbers in their database (EIR - Equipment Identity Register) containing all valid cellular equipment.

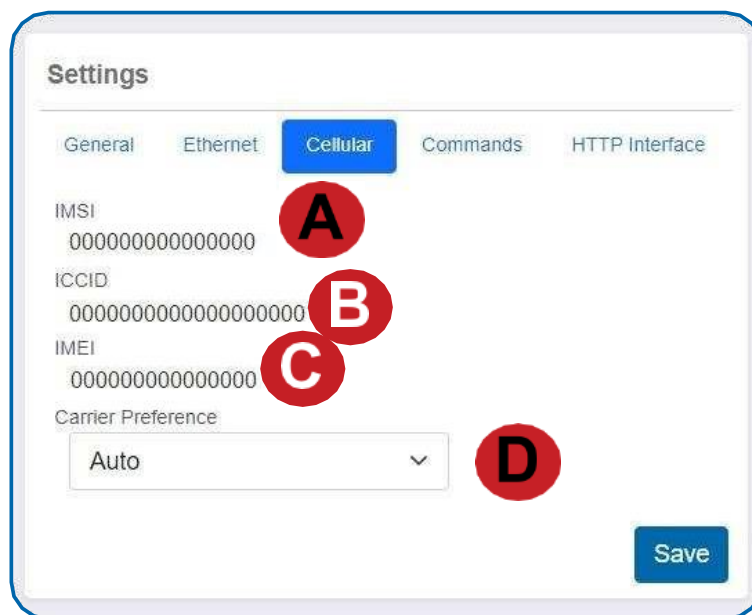


Figure 8

- D.** Carrier Preference permits the selection of Auto (default) or Manual. Auto permits the gateway to use standard gateway SIM identification rules to automatically preconfigure the gateway's cellular service. If the Auto setting is successful or a non-supported carrier SIM is used, selecting Manual in the drop-down menu results in an additional field for the Carrier APN, drop-down menu for the SIM authentication type, and selection boxes for the selection of which of the carrier bands to activate to M Enabled or NB Enabled, as shown in Figure 9.

Carrier Preference

Manual

Carrier APN

SIM Authentication Type

None

Active Bands

	M	Enabled	NB	Enabled
Band 1	<input type="checkbox"/>		<input type="checkbox"/>	
Band 2	<input type="checkbox"/>		<input type="checkbox"/>	
Band 3	<input type="checkbox"/>		<input type="checkbox"/>	
Band 4	<input type="checkbox"/>		<input type="checkbox"/>	
Band 5	<input type="checkbox"/>		<input type="checkbox"/>	
Band 8	<input type="checkbox"/>		<input type="checkbox"/>	
Band 12	<input type="checkbox"/>		<input type="checkbox"/>	
Band 13	<input type="checkbox"/>		<input type="checkbox"/>	
Band 14	<input type="checkbox"/>		N/A	
Band 18	<input type="checkbox"/>		<input type="checkbox"/>	
Band 19	<input type="checkbox"/>		<input type="checkbox"/>	
Band 20	<input type="checkbox"/>		<input type="checkbox"/>	
Band 25	<input type="checkbox"/>		<input type="checkbox"/>	
Band 26	<input type="checkbox"/>		<input type="checkbox"/>	
Band 27	<input type="checkbox"/>		N/A	
Band 28	<input type="checkbox"/>		<input type="checkbox"/>	
Band 31	<input type="checkbox"/>		<input type="checkbox"/>	
Band 66	<input type="checkbox"/>		<input type="checkbox"/>	
Band 71	N/A		<input type="checkbox"/>	
Band 72	<input type="checkbox"/>		<input type="checkbox"/>	
Band 73	<input type="checkbox"/>		<input type="checkbox"/>	
Band 85	<input type="checkbox"/>		<input type="checkbox"/>	

Save

Figure 9

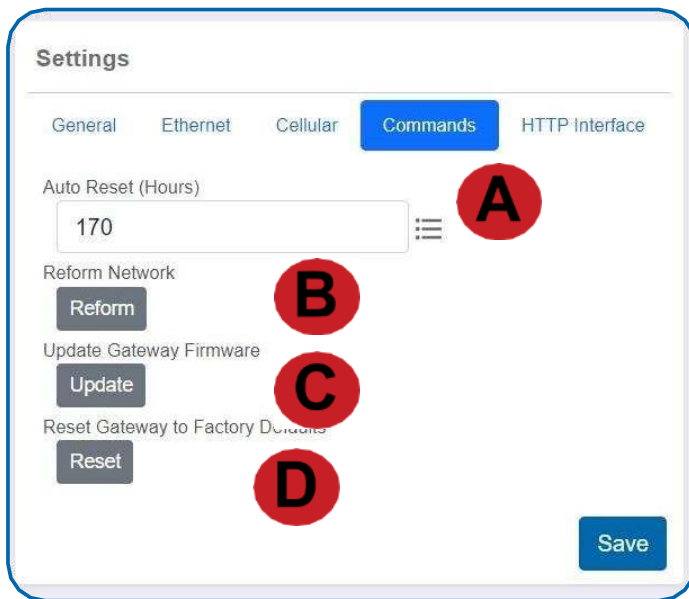
**A.** Carrier APN is provided by the carrier and enables access to the cellular carrier's network and public or private Internet access.

**B.** SIM Authentication Type: A minority of APNs are set up with a username and password used to create authenticated network sessions. Where this is not the case, the default of None may be selected in the drop-down menu. The other two options for authentication type are Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP). These two authentication types specify the security protocol used to send a username and password to establish an authenticated network connection.

Finally, boxes are provided for the active bands enabled for Cat-M1 (M Enabled) and NB-4G Cellular (NB Enabled) transmissions. By selecting these boxes, the user configures the 4G Cellular Gateway to transmit and receive to and from the cellular tower in accordance with the respective protocol(s).

## Commands

Choose the **Commands** tab located just under Settings to access the Commands page.



A. 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.

B. 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.

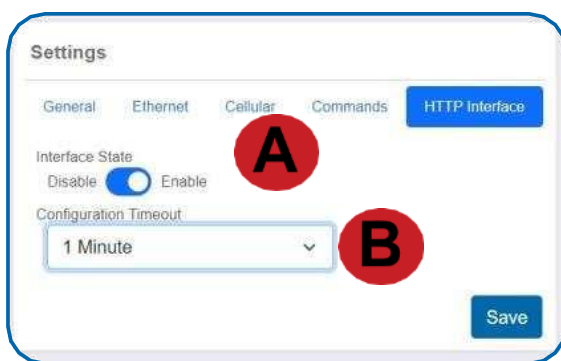
Reforming the network cleans up communication when multiple networks are in range of each other

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.

C. If there are updates available for your gateway firmware, the Update Gateway Firmware button will appear, giving you the option to select it and install the latest firmware.

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

## HTTP Interface



A. The 4G Cellular Gateway has a local HTTP configuration Interface. The HTTP Interface may be enabled so that it is accessible to change settings within its timeout window, discussed below, or to simply display status and settings information. The HTTP Interface may also be **disabled** so that it is inaccessible.

B. The **Configuration Timeout** sets the time, whether nonexistent, when Read Only is selected, 1 minute, 5 minutes, 30 minutes, or infinite, when Always Available is selected,

during which the HTTP Interface may be used to change settings on the 4G Cellular Gateway after startup. After this time, the HTTP Interface is only available to display status and settings information.

The Local HTTP Interface will be enabled as a Read-Only timeout and set to zero (0) minutes. This means that you can pull up the web pages you need on the local interface but will not be able to make any modifications. Changing the timeout to something non-zero on this page will load without warnings and all of the settings are fully configurable.

## VI. USING THE LOCAL INTERFACE

If using Scigiene Premiere is not an option, you can set up your gateway settings through the local interface.

- Connect the gateway Ethernet cord by one of the following methods:
  - AUTO-IP Method: Plug the cable directly into a PC and disable other networking interfaces. After 60 seconds, most PCs will default to randomly generated IP settings.
  - Network Method: Plug the cable into router or switch.
- Plug in the gateway to a power outlet.
- Power on the gateway. While booting, the lights will scroll red and green. At the end of the boot process, all of the lights will be green for two seconds.
- While the lights are green, quickly press and hold the utility button until the lights change to all red. Release the button and the local configuration page will be temporarily enabled and writable.
- If using the Network Method: 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 to your gateway.
- Use your web browser to connect to your gateway using the assigned IP address or AUTO-IP "http://169.254.100.1". You should be redirected to the Gateway Status page. Note - Using https:// will result in connection failure.
- Once the gateway interface has been reached, head over to the Settings tab and select the Ethernet Network option from the left-hand menu. Under the **HTTP Interface Settings**, enable the HTTP Interface and set select an appropriate timeout time, from "1 Minute" to "Always Available" from the **HTTP Configuration Timeout**. Select Save Changes when completed.
- Note that each time a page is refreshed or every time the gateway restarts, the HTTP interface time resets. After it times out, the web interface will be disabled until either the gateway restarts with a non-zero timeout value, or the special restart mode is enabled using the utility button.



### GATEWAY STATUS TAB

#### Ethernet Local Area Network Status

This is a Read-Only section listing the current conditions for your Local Area Network.

**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 numerical identifier for your gateway 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 up into the network address and the host address.

**DNS Address** - A Domain Name System is

the method employed by a URL to translate the alphabetic entry in an address bar into a numerical address associated with a server.

## **Cellular Network Status**

**Link** - Defines whether your Cellular Network is connected.

**IMEI** - (International Mobile Equipment Identity) is a number exclusive to your LTE International Gateway to identify the gateway to the cell tower. The Global System for Mobile Communications network stores the IMEI numbers in their database (EIR - Equipment Identity Register) containing all valid cellular equipment.

**ICCID** - The 19-digit unique identification number corresponding to the cellular SIM card. It is possible to change the information contained on a SIM (including the IMSI), but the identity of the SIM itself remains the same.

**IMSI** - The Global System for Mobile Communications utilizes a 15-digit IMSI (International Mobile Subscriber Identity) number as the primary mode to identify the country, mobile network, and subscriber. It is formatted as MCC-MNC-MSIN. MCC is the Mobile Country Code. MNC is the Mobile Network Code attached to the cellular network. MSIN is a serial number making the IMSI unique to a subscriber.

**Carrier** - The cellular carrier for your network.

**Signal** - This is the signal strength of the cellular network.

## **Interface Status**

The HTTP Interface is the only interface available for the 4G Cellular Gateway. This field defines the status of the default server for the HTTP interface, as hosted on the 4G Cellular Gateway, and whether the default server is ON or OFF.

## **Wireless Network Status**

**Data cache used** - The percentage of your default server cache used by data from your wireless devices.

**Total wireless devices** - The total amount of wireless devices reporting to this gateway.

Figure 13

## GENERAL CONFIGURATIONS

### **Gateway Settings**

**Power Mode** - As discussed above, this setting allows the user to choose Standard, which keeps lights and cellular transmission active when plugged into an outlet, or when on battery power, powers down lights and the cellular connection between communications. The user may also choose Force Low Power, so the gateway always powers down the lights and the cellular connection when not talking to the server, or Force High Power, so the gateway always keeps the lights and cellular transmission active.

### **Default Server Settings**

**Heartbeat Minutes** - Defines the report interval between the 4G Cellular Gateway and the server to which it reports its sensor data to be made available to the user.

**Force Transmit on Aware** - Determines whether the 4G Cellular Gateway is forced to report data as soon as a sensor in the network maintained by the gateway informs the gateway that this sensor has entered an aware state. It also determines whether the gateway can wait until its next scheduled Heartbeat report to convey this information to the server providing access to the sensor data.

**Disable Network on No Server** - Configures the 4G Cellular Gateway to disable the wireless network it maintains with the sensors it reports on, so that those sensors might engage another gateway capable of reporting their data. It can also configure the 4G Cellular Gateway to maintain its wireless network and save sensor reports on its local memory to relay to the server at which the reports are made available once the connection with the server is restored.

### **Auto Reboot Settings**

**Reboot Period** - Defines the number of hours before the Local Interface automatically reboots, up to a maximum of 8760 hours. Setting this to 0 will disable the feature.



The screenshot displays the 'Gateway Configuration' web interface for a device with ID 923812. The interface has a top navigation bar with 'Status' and 'Settings' tabs, and buttons for 'Factory Reset' and 'Reboot'. The 'Settings' tab is active, showing a sidebar with 'General', 'Ethernet Network', 'Cellular Network', and 'Wireless Network' options. The 'Ethernet Network' option is selected, leading to the 'Local Area Network Settings' section. This section contains four input fields: 'IP Address (set to 0.0.0.0 for DHCP)', 'Router IP Address (set to 0.0.0.0 for DHCP)', 'Subnet Mask (set to 0.0.0.0 for DHCP)', and 'DNS server', all currently set to '0.0.0.0'. Below these is the 'HTTP Interface Settings' section, which includes a radio button for 'HTTP Interface' (set to 'Enable') and a dropdown for 'HTTP Configuration Timeout' (set to '1 Minute'). A 'Save Changes' button is at the bottom. The firmware version '2.0.1.1' is noted in the bottom right corner.

Figure 14

## ETHERNET NETWORK SETTINGS (Future capability)

### Local Area Network Settings

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

**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 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.

### HTTP Interface Settings

**HTTP Interface** - The local HTTP Interface may be enabled so that it is either available to configure settings of the 4G Cellular Gateway or available to display status and settings information in a Read-Only state. Alternatively, the local HTTP Interface may be disabled, in which case it becomes inaccessible.

**HTTP Configuration Timeout** - This drop-down menu allows you to set a predefined amount of time of 1 Minute, 5 Minutes, or 30 Minutes during which the local HTTP Interface can be used to configure settings on the 4G Cellular Gateway after startup. After this time, the HTTP Interface cannot change settings on the gateway and only displays status and settings information. The gateway must be submitted to a factory reboot, or reconfigured in Scigiene Premiere, so that the HTTP Interface can change settings again during the timeout window. The timeout window is refreshed each time the Interface page is refreshed or every time the gateway restarts the HTTP interface. The timeout may also be set to Always Available, in which case there is no timeout window on the Interface's ability to change settings, and Read Only, which prevents the HTTP Interface from changing settings immediately.

## CELLULAR NETWORK

The Cellular Network Configuration holds a drop-down menu to select your cell **Carrier Preferences**, concerning the APN and the active bands enabled for Cat-M1/LTE Cat-M/LTE-M and NB-4G Cellular communication with a cellular tower. In most situations, Auto **Configuration** should be selected to allow the preconfigured SIM card shipped with the 4G Cellular Gateway to handle configuration of the APN and active bands.

Choose the Save Changes button to commit this change to the network. Select "Click **heretorunadvancedLTEmoduleconsole...**" to send a command through the Cellular Module Console Viewer.

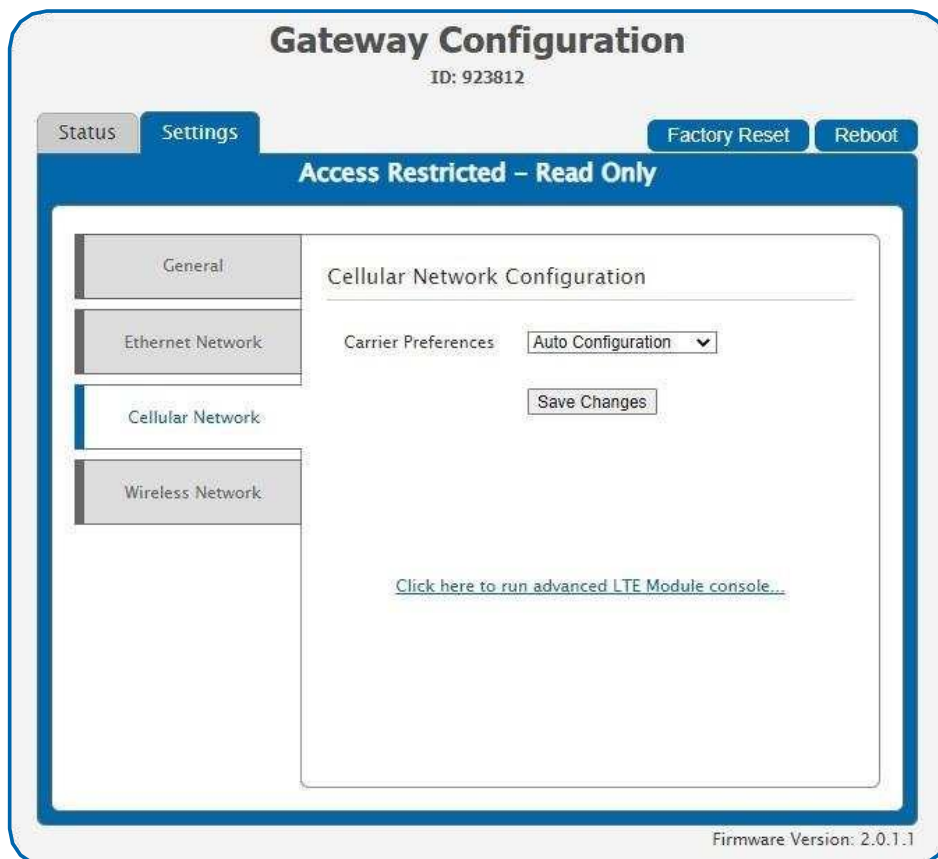


Figure 15

Where required, Manual **Configuration** may also be selected. As shown in Figure 14 below, once **Manual Configuration** is selected, a drop-down menu appears for the SIM APN, defining settings used to set up a gateway connection between the cellular carrier network and the network, usually the Internet, where the server resides that makes sensor data accessible.

**SIM Authentication type** provides a drop-down menu for situations where configuration of the APN includes the setting of a username and password for authenticated network sessions. The security protocol used to send the username and password may be selected as PAP, CHAP, or either PAP or CHAP.

Finally, boxes are provided to enable/disable the active bands for CAT-M1/LTE CAT-M/LTE-M (M Enabled) and NB-4G Cellular 2 (NB Enabled) cellular communication. These bands are determined by carrier and region.

# Gateway Configuration

ID: 923812

Status

Settings

Factory Reset

Reboot

Access Restricted – Read Only

General

Ethernet Network

Cellular Network

Wireless Network

## Cellular Network Configuration

Carrier Preferences

Manual Configuration

SIM APN

SIM Authentication

CHAP

SIM Username

SIM Password

## Active LTE Bands

	M Enabled	NB Enabled
Band 1	<input type="checkbox"/>	<input type="checkbox"/>
Band 2	<input type="checkbox"/>	<input type="checkbox"/>
Band 3	<input type="checkbox"/>	<input type="checkbox"/>
Band 4	<input type="checkbox"/>	<input type="checkbox"/>
Band 5	<input type="checkbox"/>	<input type="checkbox"/>
Band 8	<input type="checkbox"/>	<input type="checkbox"/>
Band 12	<input type="checkbox"/>	<input type="checkbox"/>
Band 13	<input type="checkbox"/>	<input type="checkbox"/>
Band 14	<input type="checkbox"/>	<input type="checkbox"/>
Band 18	<input type="checkbox"/>	<input type="checkbox"/>
Band 19	<input type="checkbox"/>	<input type="checkbox"/>
Band 20	<input type="checkbox"/>	<input type="checkbox"/>
Band 25	<input type="checkbox"/>	<input type="checkbox"/>
Band 26	<input type="checkbox"/>	<input type="checkbox"/>
Band 27	<input type="checkbox"/>	<input type="checkbox"/>
Band 28	<input type="checkbox"/>	<input type="checkbox"/>
Band 31	<input type="checkbox"/>	<input type="checkbox"/>
Band 66	<input type="checkbox"/>	<input type="checkbox"/>
Band 71	<input type="checkbox"/>	<input type="checkbox"/>
Band 72	<input type="checkbox"/>	<input type="checkbox"/>
Band 73	<input type="checkbox"/>	<input type="checkbox"/>
Band 85	<input type="checkbox"/>	<input type="checkbox"/>

Save Changes

[Click here to run advanced LTE Module console...](#)

Firmware Version: 2.0.1.1

Figure 16

## WIRELESS NETWORK

### **Add Device to Network**

This is an alternative way to add devices to communicate with your gateway. Any wireless device added here will continue to display on your Scigiene Premiere account. However, once you have added one or more devices to your gateway's network here, the network should be reformed to inform the gateway.

**Device ID** - This is a unique 6-digit number located on the back label of your device beside the QR code.

**Security Code** - A 6-letter code beginning with "IM" located on the back label sticker of your device.

**Slot Index** - Optional text field to enter the slot where your wireless device will be stored can be between 1 - 256 characters.

### **Remove Device from Network**

This is an alternative way to remove devices from your gateway's network so that they will no longer communicate with your network. However, once you have removed one or more devices from your gateway's network here, the network should be reformed to inform the gateway.

The screenshot displays the 'Gateway Configuration' web interface for a device with ID 923812. The interface has a top navigation bar with 'Status' and 'Settings' tabs, and buttons for 'Factory Reset' and 'Reboot'. Below this is a blue banner indicating 'Access Restricted - Read Only'. A left sidebar contains a menu with 'General', 'Ethernet Network', 'Cellular Network', and 'Wireless Network' (which is highlighted). The main content area is titled 'Add Device to Network' and includes three input fields: 'Device ID', 'Security Code', and 'Slot Index [1-256] (Optional)', each followed by an 'Add Device' button. Below this is a 'Remove Device to Network' section with a 'Device ID' input field and a 'Remove' button. Further down is a 'Reform Network' section with a 'Reform Now' button. The bottom section is 'Create Network Backup', featuring a 'Click to Download' link. The final section is 'Restore Network Backup', which includes a 'Choose File' button and the text 'No file chosen'. The firmware version '2.0.1.1' is noted in the bottom right corner.

Figure 17

## Reform Network

Selecting the Reform Now button will trigger the gateway to remove all of the sensors from the internal whitelist, and then request a new sensor list from the server. This command will force all of the 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.

## Create Network Backup and Restore Network Backup

Backup creates an export of the Network List in XML. Restoring the Network Backup takes the file and overrides the current Network List results back to the previous settings pulled from an uploaded file.

## SUPPORT

If you are unable to solve your issue using our online support, please contact Scigiene.



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)

## WARRANTY INFORMATION

(a) Scigiene warrants that Scigiene-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. 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 Merchandise Authorization (RMA) number 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 RMA number 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 1-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. Please visit [Scigiene.com/policy/returns/](https://www.scigiene.com/policy/returns/) for Scigiene's return policy and instructions.

(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.



## United States FCC

*This equipment has been tested and found to comply with the limits for a Class B digital device, 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.

## 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)*

**Scigiene 4G Cellular gateway models slanting with MNG2-9-CME-CCE also contain module: FCC ID: XMR202007BG95M6**

*The system antenna(s) used with the device must not exceed the following levels:*

- 4 dBi in 700 MHz, i.e., LTE FDD-12 band
- 4 dBi in 850 MHz, i.e., LTE FDD-5 band
- 7 dBi in 1700 MHz, i.e., LTE FDD-4 band
- 7 dBi in 1900 MHz, i.e., LTE FDD-2 band

## 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 Isotropically Radiated Power (E.I.R.P.) is not more than that necessary for successful communication.

The radio transmitters (IC: 9794A-G2SC1, IC: 10224A-2020BG95M6) 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 INFORMATION

*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 Sensors or Scigiene Premiere, please visit us on the web at [www.scigiene.com](http://www.scigiene.com).



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)