www.iotsensorid.com.au

IoT Management Group

4G LTE Cellular Gateway

USER GUIDE

IMPORTANT!

For best results, please wait to power on your LTE Cellular Gateway until after you have registered an account on the sensor portal and added your gateway and sensors to the online system.

Table of Contents

I. ABOUT THE LTE CELLULAR GATEWAY

The LTE Cellular Gateway allows you to control settings for your sensors without needing additional IT infrastructure. All you need is a power source to monitor your environment and equipment using our industry-leading devices. The LTE Cellular Gateway communicates with sensors and the sensor portal to deliver data alerting you to conditions in a surrounding area.

LTE Cellular Gateways operate utilizing the latest 4G LTE CAT-M1/NB1 cellular technology. The LTE Cellular Gateway is a specialized device with an incredible range. This advanced wireless IoT (Internet of Things) gateway accommodates multiple vertical IoT application segments and remote wireless sensor management solutions. Your gateway is equipped with the 24-hour backup battery.* Wireless Sensors will continue to communicate with the sensor portal via cellular transmission in the event of a power outage. The LTE Cellular Gateway is ideal for applications without an existing wired Internet connection or where existing infrastructure is dedicated to other resources.

* Actual time may vary depending on usage.

LTE CELLULAR 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)
- Up to 50,000 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
- 24-hour battery backup in event of power outage

* Actual range may vary depending on environment.

** When paired with a data plan.

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 LTE Cellular Gateway manages communication between your sensors and sensor portal. When running, the gateway will periodically transmit data on a heartbeat. The gateway will store information received from sensors until its next heartbeat.

The LTE Cellular Gateway is a cellular gateway. It uses cellular towers to relay data received from sensors to sensor portal. Sensors communicate with the gateway, then the gateway relays information to the cloud.

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.

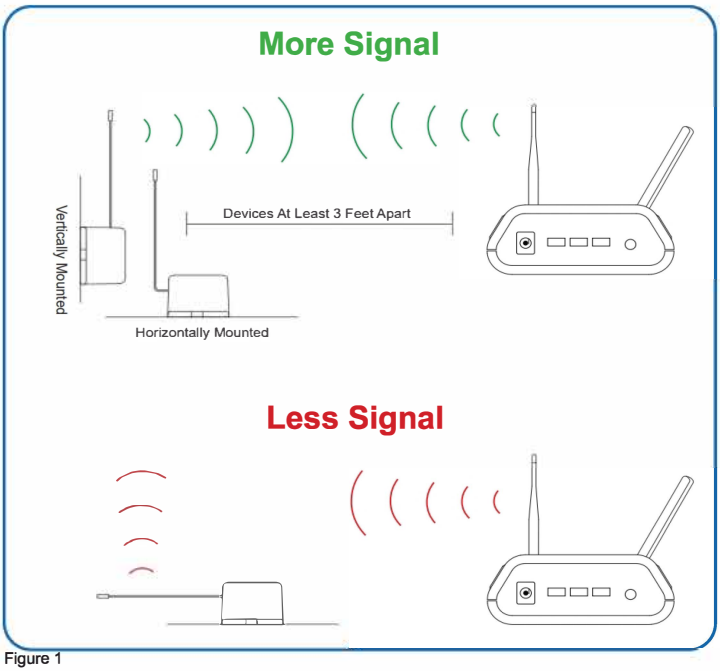


Figure 1

III. GATEWAY SECURITY

The LTE Cellular Gateway has been designed and built to securely manage data from sensors monitoring your environment and equipment. Hacking from botnets are in the headlines, We have 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 our security infrastructure. Security features of the gateway include tamper proof network interfaces, data encryption, and bank-grade security.

Our proprietary sensor protocol uses low transmit power and specialized radio equipment to transmit application data. Wireless devices listening on open communication protocols cannot eavesdrop on sensors. Packet level encryption and verification is key to ensuring traffic isn't altered between sensors and gateways. Paired with 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

The sensor to gateway secure wireless tunnel is generated using ECDH-256 (Elliptic Curve Diffie-Hellman) public key exchange to generate 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, we proudly offer robust bank-grade security at every level.

DATA SECURITY ON THE GATEWAY

The LTE gateway is designed to prevent prying eyes from accessing the data that is stored on the sensors. The LTE Cellular 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 LTE Cellular Gateway and the sensor portal 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. Because all traffic is initiated from the gateway there is no special IP configuration needed for the gateway allowing it to operate with any 4G LTE CAT-M1/NB1 enabled SIM provider.

IV. GATEWAY REGISTRATION

If this is your first time using the sensor portal 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 a sensor portal account, please consult the Sensor Portal User Guide.

REGISTERING THE GATEWAY

You will need to enter the **Device ID** and the **Security Code** from your LTE Cellular 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 you are accessing the online portal through a desktop computer, you may enter the Device ID and Security Code manually.

- 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.

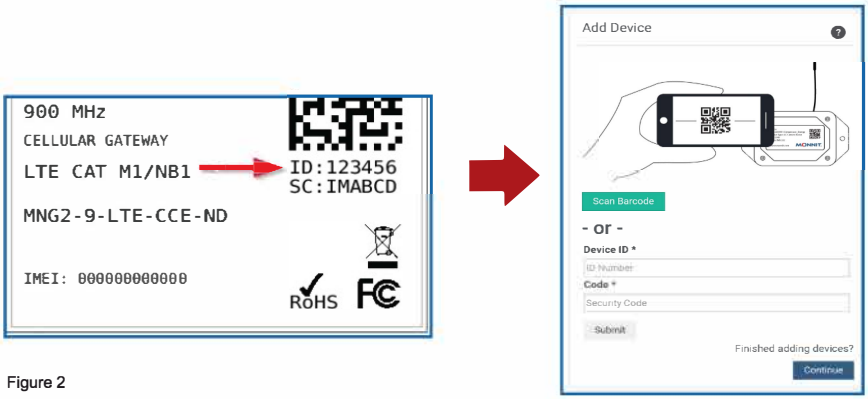


Figure 2

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

V. USING THE LTE CELLULAR GATEWAY

USING THE LTE CELLULAR GATEWAY

1. Connect your antennas to the gateway as seen in the below diagram.

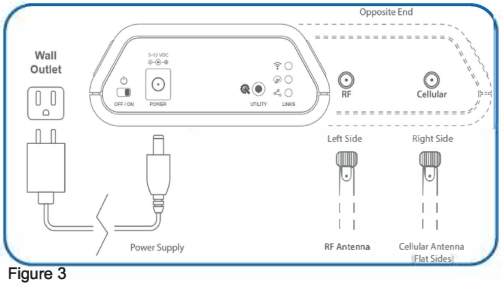


Figure 3

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 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 all becoming green for one second. In case of failure, the light sequence will repeat after ten seconds. Please contact technical support if the lights aren't green after two minutes.

Connection stage: The gateway will attempt to settle all operational connections. As the gateway first connects to the network, all other lights will be dark. A blinking green light indicates the gateway is attempting to make a tower connection. A flashing red light is a signal the cellular connection has encountered a problem.

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

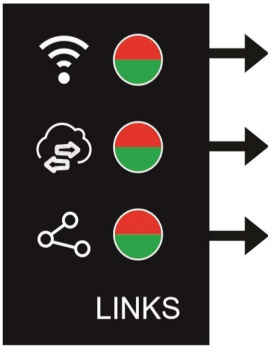


Figure 4

Steady Green: Communication with sensors is OK.
Blinking Green: Active communication with sensors.
Steady Red: Sensor communication problem.

Steady Green: Last communication with the server was OK.
Blinking Green: Active communication with the server
Steady Red: Last communication with the server was unsuccessful.

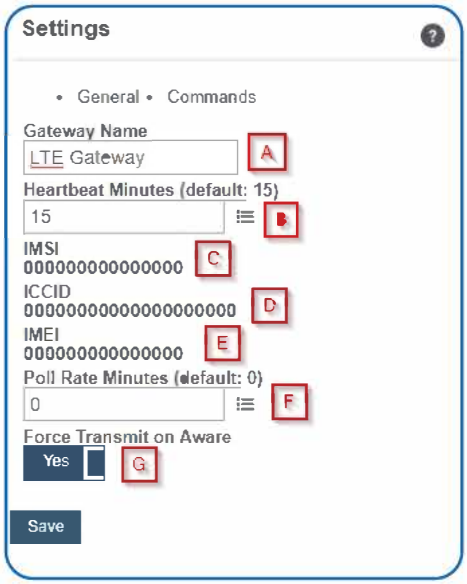
Steady Green: Connected to the cellular network
Triple Blinking Green: Cellular Network Offline
Double Blinking Green: Scanning for Tower
Single Blinking Green: Activating Data Session
Blinking Green / Red: Low cellular signal
Blinking Red: Cellular connection error

If your gateway is running off battery power or the device has been switched to a low power mode, all lights are off. The sensor data light will blink green when data is received by the gateway. The internet server light will blink every five seconds the status of the last connection. If the light is green, the communication was good. If the light is red, the communication failed.

LTE CELLULAR GATEWAY SETTINGS

The LTE 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 LTE Cellular Gateway from the list of gateways registered to your account. Select the "**Settings**" tab to edit the gateway:



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 checks in with the server. The default is fifteen minutes. So every fifteen minutes your gateway will report to the server.

C. The Global System for Mobile Communications utilizes a fifteen 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.

D. The **ICCID** is the nineteen-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.

E. IMEI (International Mobile Equipment Identity) is a number exclusive to your LTE Cellular 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.

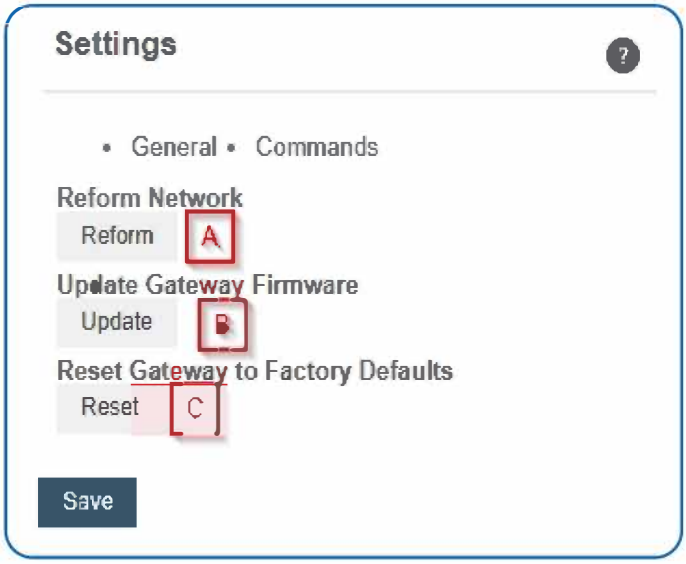
F. The **Poll Rate Minute** setting only applies if you are using Control or Local Alert. Here's how it works: to conserve cellular data, your gateway has a set heartbeat (meaning it only exchanges data with the server once every fifteen minutes by default). If you are using Control or Local Alert, you may want to control equipment or receive local alerts more frequently. If you were to increase your gateway heartbeat, you would increase your data usage substantially.

Setting a poll rate allows your gateway to check for priority incoming messages more frequently—while using a fraction of the data of a regular message exchange. Your gateway asks the server if there are any priority incoming messages, and if there are, they are exchanged immediately. If not, no messages are exchanged until your gateway has its next regular heartbeat.

G. Force Transmit on Aware means that if the sensors reach an aware state outside of the heartbeat interval, the gateway will immediately relay that data to the server instead of waiting the extra time it would take to reach the next heartbeat minute.

Commands

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



A. 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.

B. 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.

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

(Legal information goes here.)