



Remote Monitoring for Business

**IMPORTANT!** Before purchasing, you need to verify that your cellular provider is compatible with our gateway. Please click the link below to view the checklist you need to share with your provider.

[Provider Requirements](#)



## ALTA XL<sup>®</sup> IoT Gateway USER GUIDE

### **IMPORTANT!**

For best results, please wait to power on your ALTA XL<sup>®</sup> IoT Gateway until after you have created an iMonnit account and added the gateway and sensors to your new IoT network.

## Table of Contents

<b>I. ABOUT THE ALTA XL® IoT GATEWAY</b>	<b>1</b>
<b>II. HOW YOUR GATEWAY WORKS</b>	<b>2</b>
<b>III. GATEWAY SECURITY</b>	<b>2</b>
<b>IV. GATEWAY REGISTRATION</b>	<b>3</b>
<b>V. USING THE ALTA XL IoT GATEWAY</b>	<b>3</b>
USING THE COMMERCIAL ALTA XL IoT GATEWAY	3
SET UP THE INDUSTRIAL ALTA XL IoT GATEWAY	4
UNDERSTANDING THE COMMERCIAL ALTA XL IoT GATEWAY LIGHTS	5
STANDARD POWER MODE OPERATIONS	6
BATTERY POWER MODE OPERATIONS	6
UTILITY BUTTON ACTIONS	6
<b>VI. ALTA XL IoT GATEWAY SETTINGS IN iMONNIT</b>	<b>7</b>
GENERAL SETTINGS	7
ETHERNET SETTINGS	8
CELLULAR SETTINGS	8
MANUAL SIM SETTINGS	9
COMMANDS	10
HTTP INTERFACE	10
<b>VII. USING THE LOCAL INTERFACE</b>	<b>10</b>
STATUS VIEW	11
ETHERNET LOCAL AREA NETWORK STATUS	11
CELLULAR NETWORK STATUS	11
GENERAL CONFIGURATIONS	12
ETHERNET NETWORK	13
CELLULAR NETWORK	13
MANUAL SIM SETTINGS	14
WIRELESS NETWORK	15
<b>CELLULAR PROVIDER INFORMATION REQUEST</b>	<b>16</b>
<b>TROUBLESHOOTING</b>	<b>17</b>
<b>SUPPORT</b>	<b>20</b>
<b>WARRANTY INFORMATION</b>	<b>20</b>
<b>CERTIFICATIONS</b>	<b>21</b>
<b>SAFETY INFORMATION</b>	<b>23</b>
<b>COVERAGE MAPS</b>	<b>23</b>

## I. ABOUT THE GATEWAY

The ALTA XL® IoT Gateway features a powerful wireless transceiver with up to 1 Watt transmission strength, an amplified receiver, and 4G LTE CAT-M1/NB2 cellular technology to backhaul ALTA® Wireless Sensor data. The ALTA XL® IoT Gateway can send and receive data communications with ALTA Sensors at 2,000+ feet through 18+ walls in commercial building environments.

You only need a power source and the iMonnit® Cloud Platform to monitor virtually any environment and equipment using Monnit's industry-leading wireless IoT devices. The ALTA XL® IoT Gateway communicates with ALTA Sensors and iMonnit to deliver data and send alerts about various machine, equipment, or area conditions.

The ALTA XL® IoT Gateway is available in two versions: Commercial and Industrial. It's equipped with a 60-hour backup battery and will continue to communicate with iMonnit via its advanced cellular engine transmission in the event of a power outage.

Additionally, the ALTA XL® IoT Gateway comes with an RJ-45 Ethernet jack (commercial version only) for local device configuration. However, it's ideal for applications without a wired Internet connection or with infrastructure dedicated to other resources.

The ALTA XL® IoT Gateway also includes a GNSS location chipset supporting GPS, GLONASS, BeiDou, Galileo, and QZSS satellites. With the proper gateway subscription enabled, the IoT gateway's location data can be collected, viewed, and distributed to iMonnit and additional software via an application programming interface (API).

### ALTA XL® IoT GATEWAY FEATURES

- 4G LTE CAT-M1/NB2 cellular technology
- Wireless range of 2,000+ feet through 18+ 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
- Up to 60-hour battery backup in the event of a power outage
- External on/off and magnetic utility switches (industrial version only)
- RJ-45 10/100BASE-TX Ethernet jack for configuration and server connectivity (commercial version only)
- Location data subscription supported (GPS/GLONASS/BeiDou/Galileo/QZSS)

<sup>1</sup> Actual range may vary depending on the environment.

<sup>2</sup> Total messages in memory varies with sensor type. (32,000 is for Temperature Sensors. Additional information is available at [Monnit.com/Support/](https://monnit.com/Support/)).

### 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

### IMPORTANT!

The antenna must be connected at all times if the gateway is powered. Failure to do this will cause the device to consume more than that rated power. Extended operation may potentially cause premature product failure.



## II. HOW YOUR GATEWAY WORKS

The ALTA XL® IoT Gateway manages communication between ALTA Sensors and iMonnit. When running, the gateway will periodically transmit data on a user-configured preset Heartbeat Interval (in minutes). The gateway will receive data from all sensors assigned to the network (within range) and store the data it receives from the sensors until its next Heartbeat.

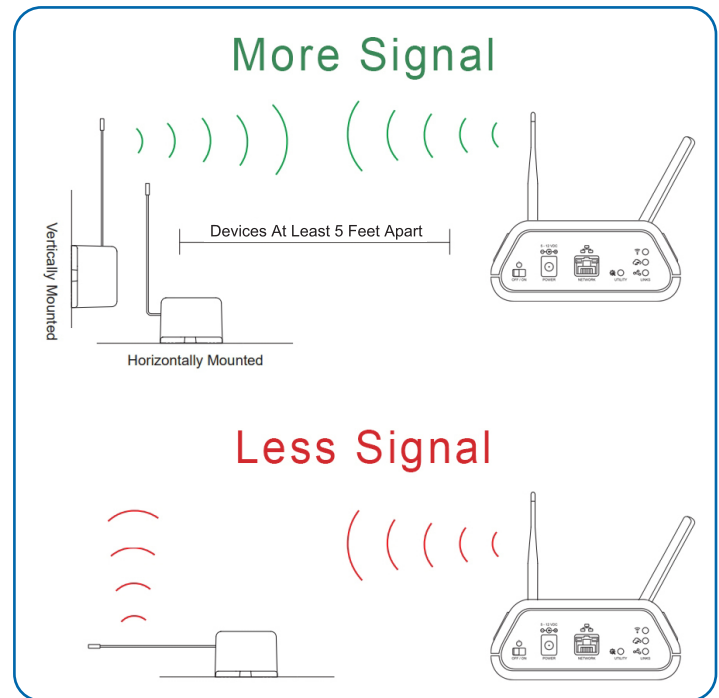
The ALTA XL® IoT Gateway is a cellular (LTE-M or CAT-M1) gateway. It uses its connection to relay data received from ALTA Sensors to iMonnit Software. Sensors communicate with the gateway, then the gateway relays information to iMonnit.

For your wireless sensors to work optimally, orient all antennas for your sensors and gateways in 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.

## III. GATEWAY SECURITY

The ALTA XL® IoT Gateway is designed and built to manage data from the sensors monitoring your environment and equipment securely. The same methods used by financial institutions to transmit data are also used in Monnit security infrastructure. The gateway's security features include tamper-proof network interfaces, data encryption, and bank-grade security.

Monnit'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 power consumption protocol.



## SENSOR COMMUNICATION SECURITY

Wireless devices listening on open communication protocols cannot eavesdrop on ALTA Sensors. Monnit's sensor-to-gateway data communication implements Encrypt-RF® encryption technology. 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, Monnit offers robust bank-grade security at every level.

For more information, reference the security section with this link:



## DATA SECURITY ON THE GATEWAY

The ALTA XL® IoT Gateway prevents prying eyes from accessing the data stored on the sensors. The 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 ALTA XL® IoT Gateway and iMonnit is secured by packet-level encryption with Encrypt-RF. 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

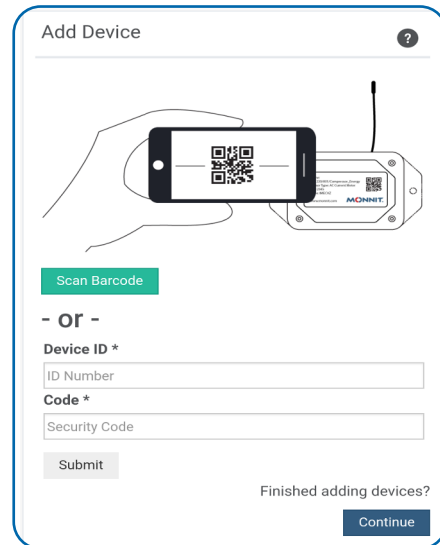
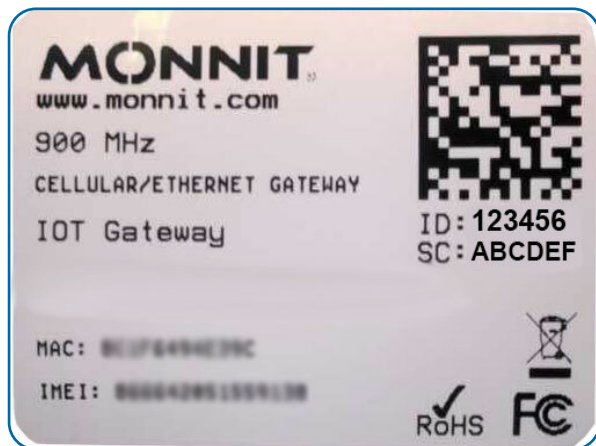
If this is your first time using the iMonnit online portal, you'll need to create a new account. If you have already created an account, start by logging in. For instructions on how to register for an iMonnit account, please consult this video.

### REGISTERING THE ALTA XL® IoT GATEWAY

Enter the **Device ID** and the **Security Code (SC)** from the ALTA XL IoT 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 iMonnit through a desktop computer, you may enter the **Device ID** and **SC** manually.

- 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.

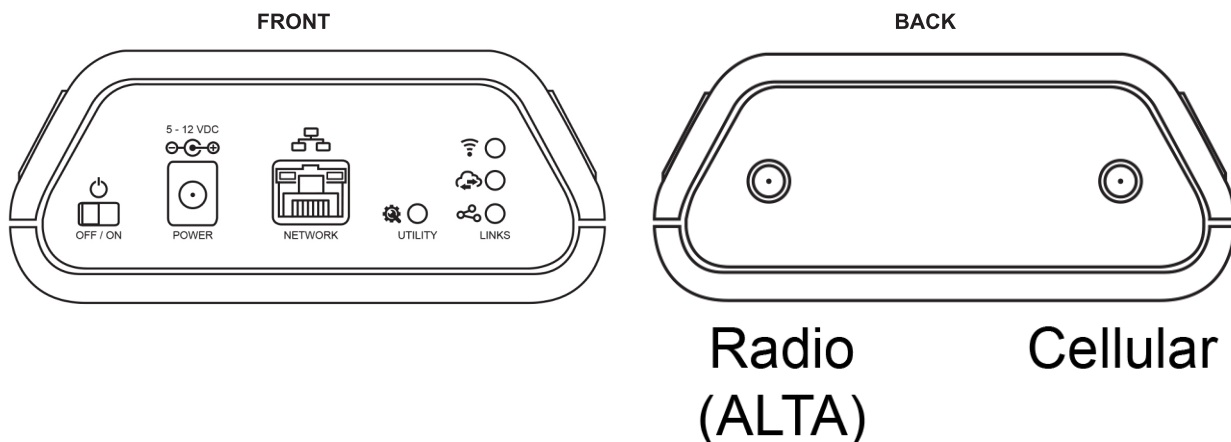


**IMPORTANT:** Add the gateway and all sensors to iMonnit so that on boot, the gateway can download and whitelist the sensors from the account.

## V. USING THE ALTA XL® IoT GATEWAY

### USING THE COMMERCIAL ALTA XL® IoT GATEWAY

1. Attach the cellular and ALTA antennas to the back of the gateway.

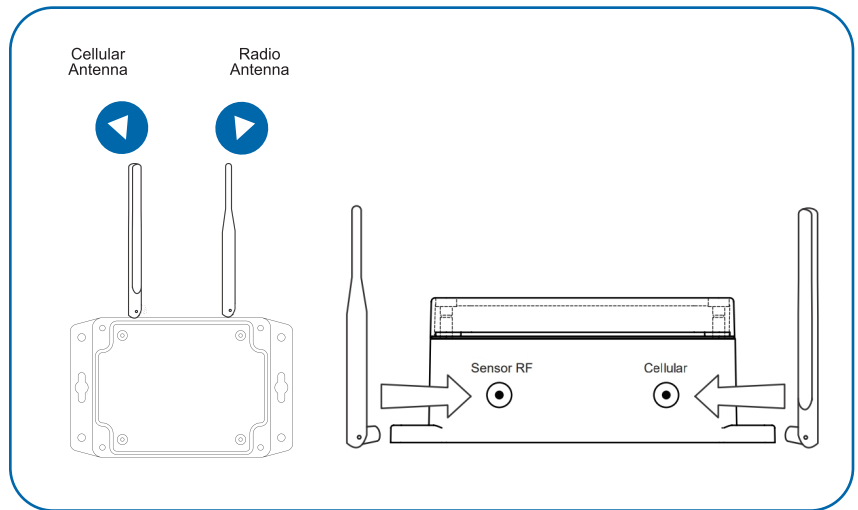


2. Plug the power supply cord into an outlet.
3. Slide the power switch on.
4. After the three LEDs switch to green, your gateway is ready to use.



## SET UP THE INDUSTRIAL ALTA XL® IoT GATEWAY

1. Connect your antennas to the gateway as seen in the diagram. The Cellular Antenna is flat on two sides and the ALTA Radio Antenna is round.
2. Plug the power supply cord into an outlet.



## USING THE INDUSTRIAL ALTA XL® IoT GATEWAY ON/OFF AND UTILITY SWITCHES

The ALTA Industrial ALTA XL® IoT Gateway has a magnetic On/Off power switch and utility switch. To operate either button or reed switch, use the magnet that shipped with the gateway. To use, simply place the provided magnet to the touch points on either side of the gateway (highlighted in red below).



Left side: Magnetic power on/off button



Users will receive one of the two magnets.



Right side: Magnetic utility button

## INDUSTRIAL ALTA XL® IoT GATEWAYS WITH DATA PLANS

When purchasing a gateway with a data plan (e.g -2Y, -2YATT, -2YVZW, etc...), The gateway is professionally sealed against the environment to meet IP-65. The gateway is then finalized with a warranty label. This label restricts access to the internal circuitry and any attempts to remove or cut this label will void the product warranty.








## UNDERSTANDING THE COMMERCIAL ALTA XL® IoT 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.

Sensor Data		Steady Green: Communication with sensors is OK Blinking Green: Active communication with sensors Steady Red: Sensor communication problem
Internet Server		Steady Green: Last communication with Monnit's server was OK Blinking Green: Active communication with Monnit's server Steady Red: Last communication with Monnit's server was unsuccessful
Cellular Service	 LINKS	Steady Green: Internet connection ready Single Blink Green: Cellular connection idle Double Blink Green: Scanning for tower Triple Blink Green: Requesting data session and IP Address Solid Green with Single Red Blink: Low signal report Solid Red with One Second Flashing Red/Green: SIM Fault Solid Red with Single Green Blink: Limited or no Internet Flashing Red for One Second: Cellular module startup fault Flashing Red for Three Seconds: Cellular fault (Tower rejection) Flashing Green for One Second: Cellular FOTA download in progress Flashing Green for Three Seconds: Cellular FOTA upgrading

**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.



## Standard or Forced-High Power Mode Operations

While the gateway is powered normally or configured to Forced-high power mode, the gateway will remain fully active and ready to communicate with the server. All LED indicators will be kept active (as described above), The Ethernet and cellular interfaces will stay connected, and GPS location services will remain active.

GPS locations services are permitted to acquire satellite data for up to nine minutes. If a suitable location calculation is not achieved during that time, the gateway will report the lack of a location-fix and the gateway will wait for the next Location Heartbeat to re-acquire a location fix.

The gateway will attempt to communicate with the server for up to one minute for every interface enabled (default is two minutes). If the gateway is unable to connect with the server using either the Ethernet or cellular interface, the gateway will begin to retry connectivity based on the following sequence:

Attempt	Back-off Time Between Attempts	Cumulative Time Attempting Communication
0	N/A	0 minutes
1	0 minute	2 minutes
2	0 minute	4 minutes
3	1 minute	7 minutes
4	2 minute	11 minutes
5	5 minutes	18 minutes
6	10 minutes	30 minutes
7	15 minutes	47 minutes
8+	random 20–40 minutes	... 22–42 minutes added on every failure

## On Battery or Forced-Low Power Mode Operations

If the gateway is running off of battery power or the device has been switched to a Forced-low power mode, all lights are typically off. The sensor data light will blink green when data is received by the gateway. The Internet server light will blink every five seconds, indicating the status of the last connection. If the light is green, the communication was good. If the light is red, the communication failed. In this mode, the Ethernet connectivity is powered down and the HTTP interface is not available.

Gateway Heartbeats, Polls, and GPS location services are limited to a minimum of **15 minutes** during low power events. However, if a wireless device signals that an urgent communication is required to be delivered to the server, the gateway will power up Ethernet, cellular, and GPS services temporarily during a server connection. If the gateway is unable to connect with the server using either the Ethernet or cellular interface, the gateway will begin to retry connectivity based on the following sequence:

Attempt	Back-off Time Between Attempts	Cumulative Time Attempting Communication
0	N/A	0 minutes
1	5 minute	7 minutes
2	5 minute	14 minutes
3	5 minutes	21 minutes
4	5 minutes	28 minutes
5+	random 20–40 minutes	... 22–42 minutes added on every failure

**Utility Button Actions:** The utility button can be used during the operational stage to perform a configuration reset or a full-factory reset. The configuration reset will erase all of your unique settings and return the gateway to factory default settings, while saving any data collected by the sensors prior to the reset. The full-factory reset will not only restore default settings, but will also erase any data on the gateway.

To perform a configuration reset, the utility button is pressed for 5 to 10 seconds and released during that time. After pressing the utility button for more than five seconds, all of the LEDs turn solid red. Releasing the button during this LED display will result in the configuration reset.

If the utility button is held for more than 10 seconds, all of the LEDs will begin to blink red. Releasing the utility button when all of the LEDs are blinking red will result in a full factory reset of the gateway, restoration of default settings, and the loss of all data in memory.





## VI. ALTA XL IoT GATEWAY SETTINGS IN iMONNIT

Access gateway settings by selecting **Gateways** in the main navigation panel. Choose the ALTA XL IoT 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

Gateway Name  
ALTA IoT Gateway - XXXXXX

Heartbeat Minutes (default: 15)  
15

Poll Rate Minutes (default: 0)  
0

Connection Preference  
Ethernet Preferred

On Aware Messages  
Wait for Heartbeat ☒ Trigger Heartbeat

On Server Loss  
Log Sensor Data ☐ Disable Wireless

Gateway Power Mode  
Standard

Primary Server  
sensorsgateway.com:3000

Location Heartbeat Minutes (default: 0)  
0

Save

**A. Gateway Name** assigns your gateway a unique title. By default, the gateway name will be the type followed by the Device ID.

**B. Heartbeat Minutes** configures the interval that the gateway periodically delivers data to the server. The default is 15 minutes, meaning the gateway will report to the Primary Server every 15 minutes.

**C. Poll Rate Minutes** configures the interval that the gateway periodically checks in with the server. If the server has urgent commands or notification for wireless sensors, the Primary Server will signal the gateway for a full data dialog (Heartbeat). The default is 0 minutes, meaning the gateway poll feature is disabled.

**D. Connection Preferences** enables the selection of how the server sends messages to the Primary Server. Options are **Ethernet Preferred** (default), **Ethernet Only**, and **Cellular Only**. **Ethernet Preferred** is also "Ethernet with Cellular Backup." When either **Ethernet Preferred** or **Cellular Only** are selected, the location (GPS/GNSS) data generator capability are enabled. **Ethernet Only** will disable the location data generator.

**E. 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**, messages are stored until the gateway is scheduled to communicate before connecting with the Primary Server.

**F. 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.

**G. Gateway Power Mode** enables the selection between **Standard** power (default), **Force Low Power**, and **Force High Power**, from a drop-down menu. **Standard** means that the 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 the gateway will always power down the lights and the cellular connection when not talking to the server. **Force High Power** means the gateway will keep the lights and cellular module active, regardless of whether or not the gateway is plugged in.

**H. Primary Server** shows the configured URL:PORT of the server. If the Gateway is "UNLOCKED," this configuration changes to a modifiable text-box.

**I. Location Heartbeat Minutes** is only visible if the gateway has been "LOCATION UNLOCKED" and is used to configure the periodic delivery of location (GPS/GNSS) data to the Primary Server. Location data functionality is only available when the cellular technologies are enabled (See Connection Preferences "D").



## ETHERNET SETTINGS (Commercial Version Only)

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.

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.

**NOTE:** Please consult your Network Administrators to obtain the correct "Static" setting for your network.

Settings

General **Ethernet** Cellular Commands HTTP Interface

MAC Address  
00:00:00:00:00:00

DHCP  
Static ☐ Dynamic ☒

Static IP (Use DHCP: 0.0.0.0)

Network Mask

Default Gateway

Default DNS Server

Save

Settings

General **Ethernet** Cellular Commands HTTP Interface

MAC Address  
00:00:00:00:00:00

DHCP  
Static ☒ Dynamic ☐

Save

**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.

**Default Gateway** - This is the forwarding host the gateway uses to relay data to the Internet, typically your router IP Address.

**Default DNS Server** - DNS Servers take alphanumeric data (like a URL address) and returns the IP Address for the server containing the information you need.

## 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 the subscriber.

**B.** The **ICCID** is the 19-digit unique identification number corresponding to the cellular SIM card.

**C.** **IMEI** (International Mobile Equipment Identity) is a number exclusive to your 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.

**D.** **Carrier Preference** permits the selection of **Auto** (default) or **Manual**. **Auto** permits the gateway to use standard gateway SIM identification rules to automatically preconfigures the gateway's cellular service. **Manual** is useful if that gateway does not reliably and in a timely manner connect to a tower, or a non-supported carrier SIM is used.

Settings

General Ethernet **Cellular** Commands HTTP Interface

IMSI  
000000000000000 **A**

ICCID  
000000000000000000 **B**

IMEI  
000000000000000 **C**

Carrier Preference  
 **D**

Save



## Manual Settings and Options (expanded)

The **Manual** setting permits additional settings to become available (i.e. Carrier APN, SIM Authentication Type, Carrier Active Bands).

### Using Cellular Provider Information

**Cellular Access Point Name (APN)** - Enables access to the cellular network and public or private Internet access. These APNs are unique to the cellular network or sub-network designated for the SIM. The following two options are supported:

- Unspecified APN - If the field is left blank, the APN is requested from the tower on connection
- Specified APN - if the field is not left blank, the cellular connection is pre-configured with this APN prior to requesting a tower connection and Internet access

**SIM Authentication Type** - To create authenticated connections, APNs may have a username/password setting and use a specific security protocol to send a username and password. The following options are supported:

- **"None"** - No username or password required and no username and password are available
- **"PAP" or "CHAP"** - Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP) is used to send the username and password and the following fields become visible:

SIM Username	<input type="text"/>
SIM Password	<input type="password"/>

**Cellular Bands** - Different networks and locations will have different cellular bands available: CAT-M1 (M-Enabled) and NB-IoT (NB-Enabled) connections:

- ☐ When a checkbox is unmarked, the band will not be used
- ☒ When a checkbox is marked, the band will be used

### Confirm Connectivity

After saving the configurations, the gateway will reboot and attempt these settings. You can see the successful cellular settings:

If the bottom gateway indicator is green and stable, the cellular connection is active.



View "status.htm" and verify the cellular status is connected.

If the gateway is not connecting after saving and applying the information from the cellular provider, then additional, advanced troubleshooting steps need to be taken.

**Settings**

General Ethernet **Cellular** Commands HTTP Interface

IMSIXXXXXXXXXXXXX  
ICCIDXXXXXXXXXXXXX  
IMEIXXXXXXXXXXXXX

Carrier PreferenceManual

Carrier APN

SIM Authentication TypeNone

	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"/>

Active Bands

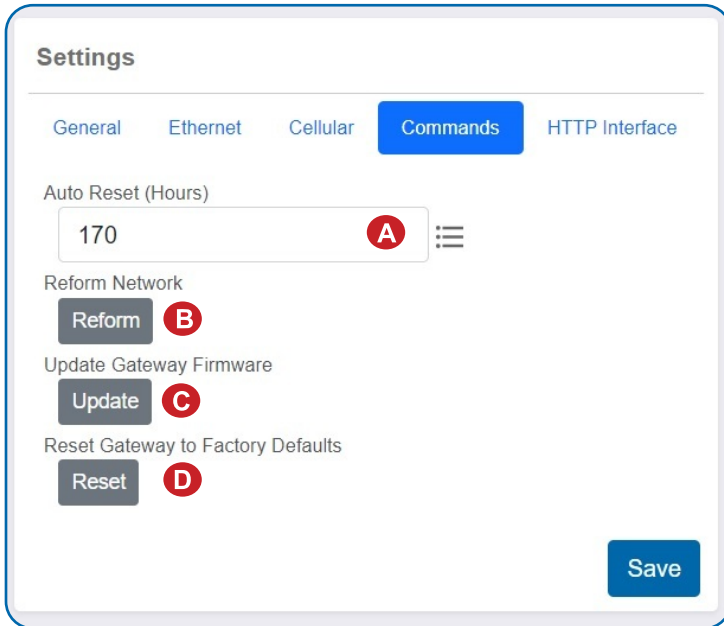
#### Note:

- If either NB or M technologies are not used, disable the technology by not checking any bands
- If no bands are enabled, then the page will prompt you to specify at least one band
- If many bands and technologies are selected, the gateway will take a long time to scan for a tower



## 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.

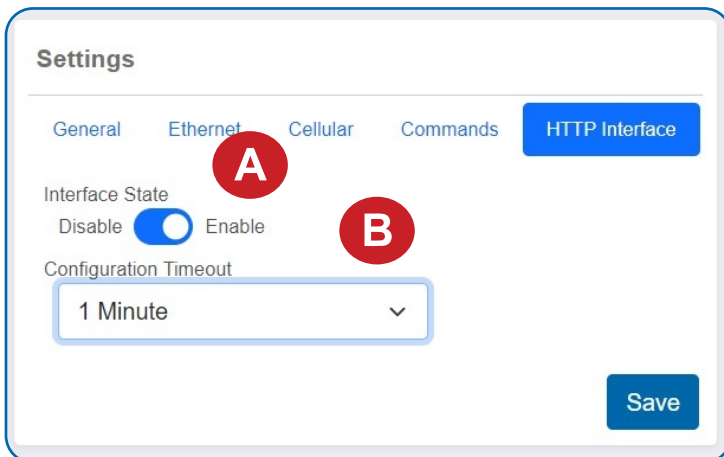
**B.** Selecting the **Reform Network** command will trigger the gateway to remove all sensors from the internal whitelist, and then request a new sensor list from the server. This command will force all sensors to reinitialize their connection with the gateway.

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 (Commercial Ethernet Version Only)



**A.** The 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 amount of time the HTTP Interface may be used to change settings on the gateway after startup or a utility button press. Options are "Read Only" (default), "1 minute," "5 minutes," "30 minutes," or "Always Available." After this time, the HTTP Interface is only available to display status and settings information.

## VII. USING THE LOCAL INTERFACE (COMMERCIAL ETHERNET VERSION ONLY)

If using iMonnit 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 a 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 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.





## STATUS VIEW

### 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 access 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 address 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 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. Values range from 0–31. Values less than 4 means low signal.

### Interface Status

The HTTP Interface shows the status of the default server for the HTTP interface, as hosted on the gateway, and whether the default server is ON or OFF.

Location (GPS/GNSS) interface shows the current status of the GPS/GNSS interface.

### 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 number of wireless devices reporting to this gateway.

**Wireless devices list** - Table lists or slot. The total number of wireless devices reporting to this gateway.

## Gateway Configuration

ID: 000000

StatusSettingsFactory ResetReboot

Ethernet LAN

Link:

Connected

Gateway MAC Address:

XX:XX:XX:XX:XX:XX

Gateway IP Address:

000.000.000.000

Router IP Address:

000.000.000.0

Network Mask:

000.000.000.0

DNS Address:

00.00.00.00

Cellular Network

Link:

Connected

IMEI:

0000000000000000

ICCID:

00000000000000000000

IMSI:

0000000000000000

Carrier:

XXX

Signal:

XX

Services

	Status
Default Server	On
Location (GPS/GNSS)	Locked

Wireless Network

Data cache used:

0%

Total wireless devices:

0

Slot

Device ID

Firmware Version: 2.0.1.3



## 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.

**GNSS/GPS Heartbeat Minutes** is only visible if the gateway has been "LOCATION UNLOCKED" and is used to configure the periodic delivery of location (GPS/GNSS) data to the Default Server. Location data functionality is only available when the cellular technologies are enabled (See Connection Preferences).

### Default Server Settings

**Heartbeat Minutes** - Defines the report interval between the gateway and the server that receives its sensor data.

**Poll Rate Minutes** - Configures the interval that the gateway periodically checks in with the server. If the server has urgent commands or notifications for wireless sensors, the Primary Server will signal the gateway for a full data dialog (Heartbeat). The default is 0 minutes, meaning the gateway poll feature is disabled.

**On Aware Messages** - Determines whether the gateway will "Trigger Heartbeat" or "Wait for Heartbeat" when a sensor in the network maintained by the gateway informs the gateway that this sensor has entered an Aware State. This 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.

**On Server Loss** - Configures the gateway to either "Disable Wireless Network" or maintain the network and "Log Sensor Data" while the server is unavailable. By default, the gateway is configured to maintain its wireless network and save sensor reports on its local memory until the connection with the server is restored. In networks with more than one gateway, disabling the network allows sensors to jump to connected gateways and deliver data to the server in a more timely manner.

**Connection Preferences** enables the selection of how the server sends messages to the Primary Server. Options are **Ethernet Preferred** (default), **Ethernet Only**, and **Cellular Only**. **Ethernet Preferred** is also "Ethernet with Cellular Backup." When either **Ethernet Preferred** or **Cellular Only** are selected, the location (GPS/GNSS) data generator capability are enabled. **Ethernet Only** will disable the location data generator.

**Default Server Name/IP** and **Server Port** are the configured URL:PORT of the server and only visible when the Gateway is "UNLOCKED."

### 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 'Settings' page of a gateway configuration interface. The top navigation bar includes 'Status' and 'Settings' tabs, along with 'Factory Reset' and 'Reboot' buttons. The 'Settings' tab is selected, revealing a 'General' sidebar with three network-related options: 'Ethernet Network', 'Cellular Network', and 'Wireless Network'. The main configuration area is organized into three distinct sections. The 'Gateway Settings' section contains 'Power Mode' (set to 'Standard') and 'GNSS/GPS Heartbeat (Minutes)' (set to '0.00'). The 'Server Settings' section includes 'Heartbeat (Minutes)' (15.00), 'Poll Rate (Minutes)' (0.00), 'On Aware Messages' (Trigger Heartbeat), 'On Server Loss' (Log Sensor Data), 'Connection Preference' (Ethernet Preferred), 'Server Name/IP' (staging.imonnit.com), and 'Server Port' (3000). The 'Auto Reboot Settings' section features 'Reboot Period (Hrs)' (168). A 'Save Changes' button is positioned at the bottom right of the settings area. The footer of the interface indicates the 'Firmware Version: 2.0.1.5'.





## ETHERNET NETWORK

### Local Area Network Settings

From the **Ethernet Network** 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 alphanumeric 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 gateway or available to display status and settings information in a Read-Only state. Alternatively, the local HTTP Interface may be disabled, so 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 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 iMonnit, 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," so 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-IoT communication with a cellular tower. In most situations, **Auto Configuration** should be selected to allow the pre-configured SIM card shipped with the gateway to handle configuration of the APN and active bands.



## Manual Settings and Options (expanded)

The **Manual** setting permits additional settings to become available (i.e. Carrier APN, SIM Authentication Type, Carrier Active Bands).

### Using Cellular Provider Information

**Cellular Access Point Name (APN)** - Enables access to the cellular network and public or private Internet access. These APNs are unique to the cellular network or sub-network designated for the SIM. The following two options are supported:

- Unspecified APN - If the field is left blank, the APN is requested from the tower on connection
- Specified APN - if the field is not left blank, the cellular connection is pre-configured with this APN prior to requesting a tower connection and Internet access

**SIM Authentication Type** - To create authenticated connections, APNs may have a username/password setting and use a specific security protocol to send a username and password. The following options are supported:

- **"None"** - No username or password required and no username and password are available
- **"PAP" or "CHAP"** - Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP) is used to send the username and password and following fields become visible:

SIM Username	<input type="text"/>
SIM Password	<input type="password"/>

**Cellular Bands** - Different networks and locations will have different cellular bands available: CAT-M1 (M-Enabled) and NB-IoT (NB-Enabled) connections:

- ☐ When a checkbox is unmarked, the band will not be used
- ☒ When a checkbox is marked, the band will be used

### Confirm Connectivity

After saving the configurations, the gateway will reboot and attempt these settings. You can see the successful cellular settings:

If the bottom gateway indicator is green and stable, the cellular connection is active.



View "status.htm" and verify the cellular status is connected.

If the gateway is not connecting after saving and applying the information from the cellular provider, then additional, advanced troubleshooting steps need to be taken.

	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"/>

#### Note:

- If either NB or M technologies are not used, disable the technology by not checking any bands
- If no bands are enabled, then the page will prompt you to specify at least one band
- If many bands and technologies are selected, the gateway will take a long time to scan for a tower



## 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 iMonnit 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 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.

### 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.

## Gateway Configuration

ID: 923812

Status

Settings

Factory Reset

Reboot

Access Restricted – Read Only

General

Ethernet Network

Cellular Network

Wireless Network

Add Device to Network

Device ID:

Security Code:

Slot Index [1-256]:   
(Optional)

Add Device

Remove Device to Network

Device ID: 

Remove

Reform Network

Reform Now

Create Network Backup

[Click to Download](#)

Restore Network Backup

Choose File

No file chosen

Firmware Version: 2.0.1.1



# IMPORTANT

## CELLULAR PROVIDER INFORMATION REQUEST

To customize any of the cellular settings in **Manual Mode**, the following questions must be answered by your cellular provider:

- Does the cellular provider support LTE-M (CAT-M1) or NB-IoT (CAT-NB2)?
  - If yes, do you use specific SIMs with these technologies?
- What LTE-M cellular bands should I use at my location?
  - None, if not used or specify?
- What NB-IoT (NB2) Cellular Bands should I use at my location?
  - None, if not used or specify?
- What APN should be used with this SIM/Network?
  - Does the network support unspecified or network-provided APNs?
- Does this SIM support Authentication?
  - If so,
    - What is the type: PAP or CHAP?
    - What is the username?
    - What is the password?

More detailed information can be found [here](#).



## ADVANCED CELLULAR TROUBLESHOOTING

### Troubleshooting Setup

To set up the IoT Gateway for Advanced Cellular Troubleshooting:

- The SIM card must be placed in the SIM card holder inside the gateway
- The Ethernet interface must be connected
- The Connection Preferences must be either "Ethernet Preferred" or "Cellular Only"
- The HTTP Interface Settings must be "Enable" and "Always Available"

### HTTP Interface Settings

---

HTTP Interface:

☒ Enable  
☐ Disable

HTTP Configuration Timeout

Always Available ▼

View of "lan.htm"

On "lte.htm," the following link can be selected to access the LTE Module Console Viewer "lcon.htm."

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

The LTE Module Console Viewer is the page where advanced cellular troubleshooting steps are executed. The page permits commands to be sent directly to the cellular module and for responses to be displayed.

Advanced LTE Console Mode – Reboot to Exit

Reboot

Cellular Module Console Viewer – (all other gateway functions disabled)

Command:

Send

View of "lcon.htm"



## STEPS FOR TROUBLESHOOTING

The following table outlines the commands and expected responses for each step of troubleshooting. If the result does not match the expected, record the result and share with Monnit Technical Support (support@monnit.com). This information is also helpful to identify the required settings to add automatic cellular provider support to future gateway firmware. Record the command and results you get and share with Monnit Technical Support (support@monnit.com).

STEP	COMMAND	EXPECTED RESULT																								
1	+CPIN?	+CPIN: READY Result: The SIM is correctly installed and inserted.																								
2	+GSN	XXXXXXXXXXXXXXXXXX Result: The IMEI of the Module is reported.																								
3	+CIMI	XXXXXXXXXXXXXXXXXX Result: The IMSI of the SIM is reported.																								
4	+QCCID	+QCCID: XXXXXXXXXXXXXXXXXXXX Result: The ICCID of the SIM is reported.																								
5	+QPRTPARA=3	OK Result: The Module will learn the BAND and APN settings from the SIM card.																								
6	+CFUN=1,1	OK Result: Reboot the Module and apply the settings learned from +QPRTPARA command. Note: The next command should run between 5 and 15 seconds after this one.																								
7	E0;+COPS=2;+CEREG=2	OK Result: Halt Module, remove command echoes, and enable tower identification.																								
8	+QCFG="band"	+QCFG: "band",0x0,0x80a,0x80a Result: This shows that Bands 2, 4, and 12 are recognized by the SIM by default. Note: This is an AT&T Example. Other bands can be decoded from the data below. <table><tr><td>B1 0x1</td><td>B2 0x2</td><td>B3 0x4</td><td>B4 0x8</td></tr><tr><td>B5 0x10</td><td>B6 0x80</td><td>B12 0x800</td><td>B13 0x1000</td></tr><tr><td>B14 0x2000</td><td>B18 0x20000</td><td>B19 0x40000</td><td>B20 0x80000</td></tr><tr><td>B25 0x1000000</td><td>B26 0x2000000</td><td>B27 0x4000000</td><td>B28 0x8000000</td></tr><tr><td>B31 0x40000000</td><td>B66 0x2000000000000000</td><td>B71 0x4000000000000000</td><td>B72 0x8000000000000000</td></tr><tr><td>B73 0x100000000000000000</td><td>B85 0x1000000000000000000</td><td>All Bands (M) 0x4001820000000000F0E389F</td><td>All Bands (NB) 0x4001C2000000004E0E189F</td></tr></table> If the results need to change, the command format is as follows: +QCFG="band",0x0,<M BAND MASK>,<NB BAND MASK> Example for setting Band 5 and 13: +QCFG="band",0x0,0x1010,0x1010	B1 0x1	B2 0x2	B3 0x4	B4 0x8	B5 0x10	B6 0x80	B12 0x800	B13 0x1000	B14 0x2000	B18 0x20000	B19 0x40000	B20 0x80000	B25 0x1000000	B26 0x2000000	B27 0x4000000	B28 0x8000000	B31 0x40000000	B66 0x2000000000000000	B71 0x4000000000000000	B72 0x8000000000000000	B73 0x100000000000000000	B85 0x1000000000000000000	All Bands (M) 0x4001820000000000F0E389F	All Bands (NB) 0x4001C2000000004E0E189F
B1 0x1	B2 0x2	B3 0x4	B4 0x8																							
B5 0x10	B6 0x80	B12 0x800	B13 0x1000																							
B14 0x2000	B18 0x20000	B19 0x40000	B20 0x80000																							
B25 0x1000000	B26 0x2000000	B27 0x4000000	B28 0x8000000																							
B31 0x40000000	B66 0x2000000000000000	B71 0x4000000000000000	B72 0x8000000000000000																							
B73 0x100000000000000000	B85 0x1000000000000000000	All Bands (M) 0x4001820000000000F0E389F	All Bands (NB) 0x4001C2000000004E0E189F																							
9	+QCFG="iotopmode",0 or +QCFG="iotopmode",1 or +QCFG="iotopmode",2	OK Result: Set Technology to: 0 = M1 only (auto-default) , 1 = NB only, 2 = Both M1/NB2. Note: Choose which command and send one only.																								





10	+QICSGP=...	<p><b>OK</b></p> <p>Result: Set the APN, Username, and Password, and Authentication Type  +QICSGP=1,&lt;context_types&gt;,[<b>"APN"</b>,"username","password",&lt;authentication&gt;]]]  &lt;context_type&gt; is 1 for "IP" and 3 for "IPV4V6"  &lt;authentication&gt; is 0 None, 1 PAP, and 2 CHAP</p> <p>Empty APN, no Authentication example: <b>+QICSGP=1,3,""</b>  set APN, no authentication example: <b>+QICSGP=1,3,"my.apn.com"</b>  Full Example with CHAP: <b>+QICSGP=1,3,"carrier.apn","myuser","mypass",2</b></p>
11	+CFUN=1;+COPS=0	<p><b>OK</b></p> <p>Result: The cellular module now is active.</p>
12	+CEREG?	<p><b>+CEREG: 2,0</b> -- 0 is Off, run step 11  <b>+CEREG: 2,2</b> -- 2 is Scanning for Tower  <b>+CEREG: 2,1,"990D","6E20B0F",8</b> -- 1 is "home" network, tower information and technology  <b>+CEREG: 2,5,"990D","6E20B0F",8</b> -- 5 is "roaming" network, tower information and technology  <b>+CEREG: 2,3</b> -- 3 is registration denied  <b>+CEREG: 2,4</b> -- 4 is unknown state</p> <p>Result: Check for Tower Connection. Keep running this command until Result is 1 or 5.  Note: Success on this step means that steps 8-10 were input correctly.</p>
13	+COPS?	<p><b>+COPS: 0,0,"AT&amp;T",8</b></p> <p>Result: Reports the carrier the gateway is attached to.</p>
14	+CSQ	<p><b>+CSQ: 28,99</b></p> <p>Result: The first number reports the signal strength (&gt;4 is acceptable signal).</p>
15	+CGATT?	<p><b>+CGATT: 1</b></p> <p>Result: Data session active if value is 1. Failed to Open a data session if 0.</p>
16	+CGCONTRDP	<p><b>+CGCONTRDP: 1,5,"m2m005230.attz",10.139.237.252,,100.122.11.10,100.121.11.10</b></p> <p>Result: Show the current APN and IP settings in use.</p>
17	+QIOPEN=...	<p><b>OK</b>  <b>+QIOPEN: 1,0</b></p> <p>Send: <b>+QIOPEN=1,1,"UDP","sensorgateway.com",3000</b> (Test DNS and server) or  <b>+QIOPEN=1,1,"UDP","68.169.16.253",3000</b> (Test server only)  Result: The UDP socket opened successfully.</p>
18	+QISENDEX=...	<p><b>SEND OK</b>  <b>+QIURC: "recv",1</b> (If the network is fast enough, this message is received, indicating there was a response from the server. This message may not be received.)</p> <p>Send : <b>+QISENDEX=1,"4757503D393237333930"</b>  Result: Data sent to the server.</p>
19	+QIRD=1,2	<p><b>+QIRD: 2</b>  <b>CB or OK</b> (Data from Server)  <b>OK</b></p> <p>Result: Two bytes were received from the server successfully.</p>
20	+QICLOSE=1	<p><b>OK</b></p> <p>Result: The socket is closed.</p>



## SUPPORT

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

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

## WARRANTY INFORMATION

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

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

Products returned under this Warranty must be unmodified and in original packaging. Monnit reserves the right to refuse warranty repairs or replacements for any Products that are damaged or not in original form. For Products outside the 1-year warranty period, repair services are available at Monnit at standard labor rates for a period of one year from the Customer's original date of receipt.

**(b)** As a condition to Monnit's obligations under the immediately preceding paragraphs, the Customer shall return Products to be examined and replaced to Monnit's facilities, in shipping cartons which clearly display a valid RMA number provided by Monnit. Customer acknowledges that replacement Products may be repaired, refurbished, or tested and found to be complying. Please visit [Monnit.com/policy/returns/](https://monnit.com/policy/returns/) for Monnit's return policy and instructions.

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

### Limitation of Warranty and Remedies

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

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



## CERTIFICATIONS

### United States FCC

#### All ALTA XL® IoT Gateways Contain FCC ID: ZTL-G2XL1 & FCC ID: XMR202007BG95M6

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 one the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

- (1) This device may not cause harmful interference, and
- (2) This device must accept any interference received, including interference that may cause undesired operation.

**Warning:** Changes or modifications not expressly approved by Monnit 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. Additionally, a separation distance of 22 cm or more should be maintained between this device and persons during device operation.

#### Approved Antennas For ALTA XL® Wireless Gateways Containing FCC ID: ZTL-G2SC1

ALTA XL® devices have been designed to operate with an approved antenna listed below, and having a maximum gain of 14 dBi with the noted required cable loss. Antennas having a gain greater than 14 dBi are strictly prohibited for use with this device. The required antenna impedance is 50 ohms.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (EIRP) is not more than that required for successful communication.

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

Part Number	Manufacturer	Description	Required Cable Loss
XQZ-900E-2	Xianzi	3 dBi Dipole Omni	0 dB
HG905RD-RSP	Hyperlink	5 dBi Dipole Omni	0.44 dB
HG908U-PRO	Hyperlink	8dBi Fiberglass Omni	3.48 dB
HG8909P	Hyperlink	9dBi Flat Panel	3.54 dB
HG914YE-NF	Hyperlink	14dBi Yagi	10.74 dB

#### Approved Antennas For ALTA XL® Wireless Gateway Containing FCC ID: XMR202007BG95M6

The cellular 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



**WARNING:** ISM and LTE antennas are considered integral to the ALTA XL® IoT Gateway and should remain fixed within 3 meters of the device during operation.



## 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-G2XL1, 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.

### French

Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pour l'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillage radioélectrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la Puissance Isotrope Rayonnée Équivalente (P.I.R.É) ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.

Le présent émetteurs radio (IC: 9794A-G2XL1, IC: 10224A-2020BG95M6) a été approuvé par Industrie Canada pour fonctionner avec les types d'antenne figurant sur la page précédente et ayant un gain admissible maximal et l'impédance requise pour chaque type d'antenne. Les types d'antenne non inclus dans cette liste, ou dont le gain est supérieur au gain maximal indiqué, sont strictement interdits pour l'exploitation de l'émetteur.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.



**WARNING:** To satisfy IC 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. Additionally, a separation distance of 32.1 cm or more should be maintained between this device and persons during device operation.

---



## 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 the 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. 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.

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

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

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

### Additional Information and Support

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

### Equipment Errata: Power Supply Advisory

When using the gateway in remote area or powering the gateway with an inverter, there is a potential for unbalanced or noisy power (not true sinusoidal AC power). The gateway may experienced random reboots and Ethernet link instability in these situations. Monnit recommends using the AC/DC power supply issued with the device in those situation. Additionally, Power line filters or higher-end power inverters may all be required for stable operation.

## Coverage Maps:

[AT&T](#) [Verizon](#) [Telenor](#) [Hologram](#) [Sasktel](#)

This map shows an approximation of wireless data coverage in the United States, Puerto Rico, and U.S. Virgin Islands.



**Monnit Corporation**

3400 South West Temple • Salt Lake City, UT 84115 • 801-561-5555  
[www.monnit.com](http://www.monnit.com)



Change Log

Revision	Author	Date (yyyy/mm/dd)	Change
1		2023/1/19	Original release.
2			
3			