



Remote Monitoring for Business



ALTA XL[®] Ethernet Gateway USER GUIDE

IMPORTANT!

For best results, please wait to power on your ALTA XL[®] Ethernet Gateway until after you've registered an account on iMonnit.

Table of Contents

I. ABOUT THE ALTA XL ETHERNET GATEWAY	1
ALTA XL ETHERNET GATEWAY FEATURES	1
EXAMPLE APPLICATIONS	1
II. HOW YOUR GATEWAY WORKS	2
III. GATEWAY SECURITY	3
SENSOR COMMUNICATION SECURITY	3
DATA SECURITY ON THE GATEWAY	3
SERVER COMMUNICATION SECURITY	3
IV. GATEWAY REGISTRATION	4
REGISTERING THE GATEWAY	4
V. USING THE GATEWAY	5
UNDERSTANDING THE GATEWAY LIGHTS	5
GATEWAY SETTINGS	6
VI. INSTALLING IMONNIT EXPRESS SOFTWARE	11
INSTALLING IMONNIT EXPRESS SOFTWARE	11
INSTALLING MONNIT MINE SOFTWARE	11
VII. USING THE LOCAL INTERFACE	12
STATUS TAB	12
SETTINGS TAB	13
TROUBLESHOOTING	20
SUPPORT	21
WARRANTY INFORMATION	21
CERTIFICATIONS	23
SAFETY RECOMMENDATIONS	26

I. ABOUT THE ALTA XL® ETHERNET GATEWAY

The ALTA XL® Ethernet Gateway features a powerful wireless transceiver with up to 1 Watt of transmission power and an amplified receiver. The ALTA XL® Ethernet Gateway can send and receive data communications with ALTA® Wireless Sensors 2,000+ feet through 18+ walls in commercial building environments.

The gateway allows ALTA Sensors to communicate with iMonnit® IoT Monitoring and Notification System without needing a PC. Simply provide power and plug the gateway into an open Ethernet port with an Internet connection. It will automatically connect with our online servers, providing the perfect solution for Internet-enabled commercial locations.

The ALTA XL® Ethernet Gateway is an advanced gateway that enables fast, reliable IoT data solutions. It's specifically designed to respond to the increasing market need for global technology that accommodates various vertical IoT application segments and remote wireless sensor management solutions.

ALTA XL® ETHERNET GATEWAY FEATURES

- Wireless range of 2,000+ feet through 18+ walls*
- Frequency-Hopping Spread Spectrum (FHSS)
- Best-in-class interference immunity
- Encrypt-RF® Security (Diffie-Hellman Key Exchange + AES-128 CBC for sensor data messages)
- 30,000 sensor message memory**
- 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

* Actual range may vary depending on the environment

** Total messages in memory varies with sensor type (30K total messages for temperature)

EXAMPLE APPLICATIONS

- Remote Location Monitoring
- Facility Management
- 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

Your ALTA XL® Ethernet Gateway manages communication between your sensors and iMonnit. When running, the gateway will periodically transmit data on a Heartbeat. The gateway will store information received from sensors until its next Heartbeat.

The ALTA XL Ethernet Gateway uses an Ethernet connection to relay data received from sensors to iMonnit. Sensors must also be at least three feet away from the gateway to function correctly.

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

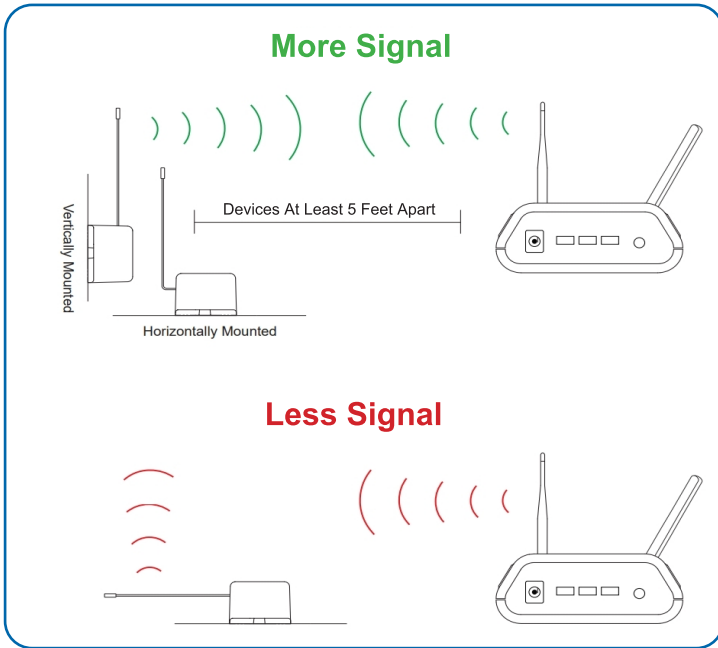


Figure 1

III. GATEWAY SECURITY

The ALTA XL® Ethernet 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 the Monnit security infrastructure. The gateway's security features 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. Paired with a best-in-class range and power consumption protocol, all data is transmitted securely from your devices.

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® Ethernet 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 on 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.

For more information on Monnit gateway security, reference this link:



SERVER COMMUNICATION SECURITY

Communication between your ALTA XL® Ethernet Gateway and iMonnit 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 VPNs. The gateway can still operate within a VPN, if it is present.

IV. GATEWAY REGISTRATION

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

REGISTERING THE GATEWAY

You will need to enter the **Device ID** and the **Security Code (SC)** from your 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 manually enter the **Device ID** and **SC**. 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 is all letters (no numbers). It can also be found on the barcode label of your gateway.

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

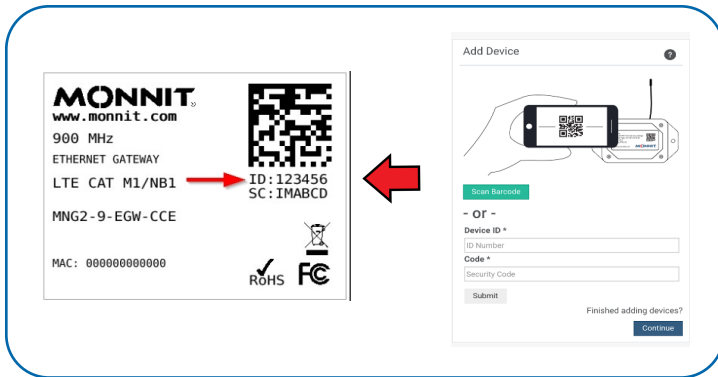


Figure 2

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

V. USING THE GATEWAY

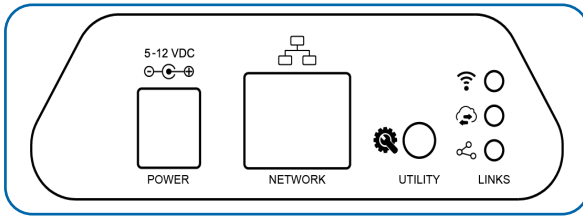


Figure 3

See Figure 3 above.

Power: Power cord connection location

Network: Ethernet connection location

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

1. Connect your antennas to the gateway.
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 analyzes electronics and programming. The LEDs flash red and green before turning green for one second and entering a waterfall pattern. In case of failure, the light sequence repeats after 10 seconds. The gateway continues trying to boot until it succeeds. Please contact technical support if the lights aren't green after two minutes.

Connection Stage: When the LEDs turn solid green for 1.5 seconds, the power-on step is complete. After the Network Uplink Connectivity LED displays a solid green LED, the gateway attempts to connect to its default server and other configured surfaces. The gateway attempts to settle all active connections. When the gateway first connects to the network, no other lights illuminate.

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

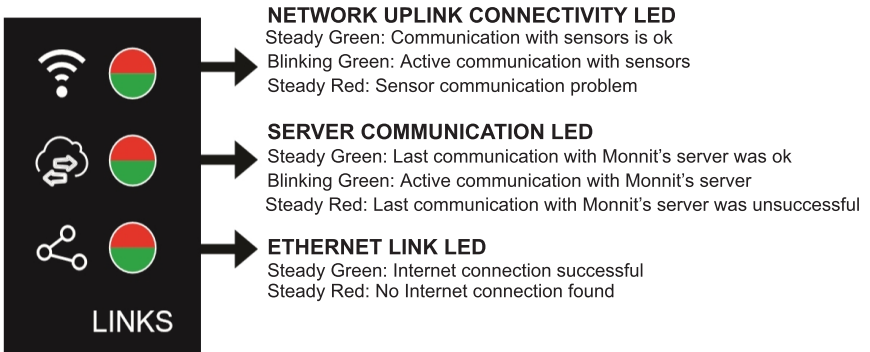


Figure 4

GATEWAY SETTINGS

General

The gateway receives data from all sensors assigned to the network and within its range. It then returns this data to the server in a series of Heartbeats.

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

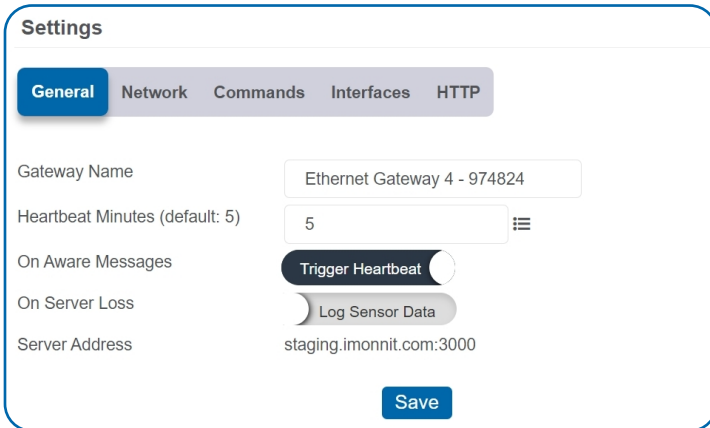


Figure 5

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

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

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

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

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

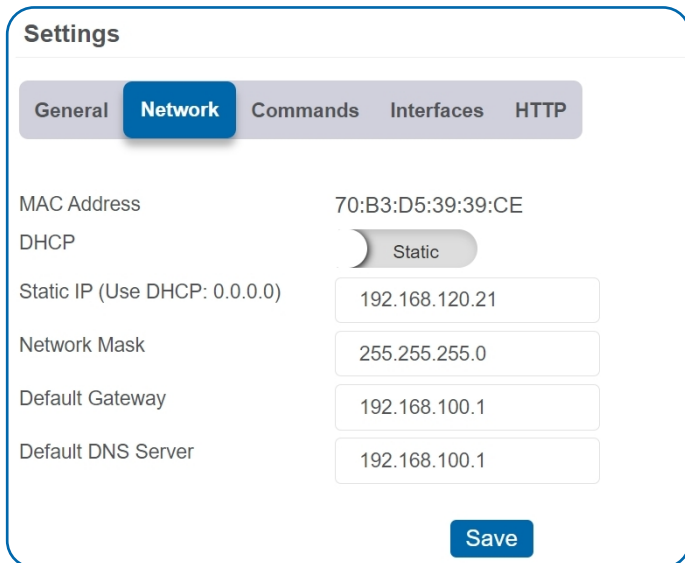
Toggling this to Disable Wireless Network will force the sensors communicating with this gateway to find a new gateway in order to deliver sensor messages to the server immediately.

Network

Choose the Local Area **Network** (LAN) tab under the Settings title to open up the LAN configuration page. The LAN includes the ability to switch your network Internet Protocol (IP) address from Dynamic Host Configuration Protocol (DHCP) to Static. DHCP will be the default network IP address.

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

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



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

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

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

Figure 6

Static IP – A Static IP address is a numerical sequence assigned to a computer by a network administrator. This is different from a Dynamic IP address in that a Static IP doesn't periodically change. It remains constant.

Network Mask – Also known as Subnet Mask, this number hides the network half of an IP address. The most common Network Mask number is 255.255.255.0.

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

Default DNS Server – Domain Name System (DNS) Servers take alphanumeric data (like a URL address) and return the IP address for the server containing the information you're looking for.

Commands

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

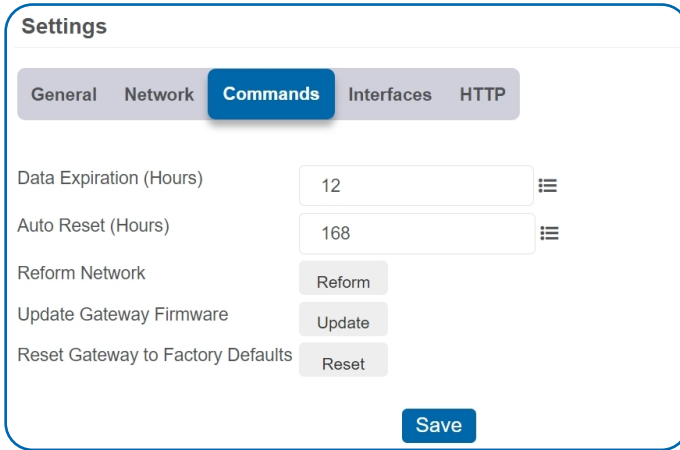


Figure 7

Data Expiration (Hours) – Manage data expiration time in the gateway. After this time has elapsed, the data pulled for the Modbus protocol and Simple Network Management Protocol (SNMP) will be zero-ed out.

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

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

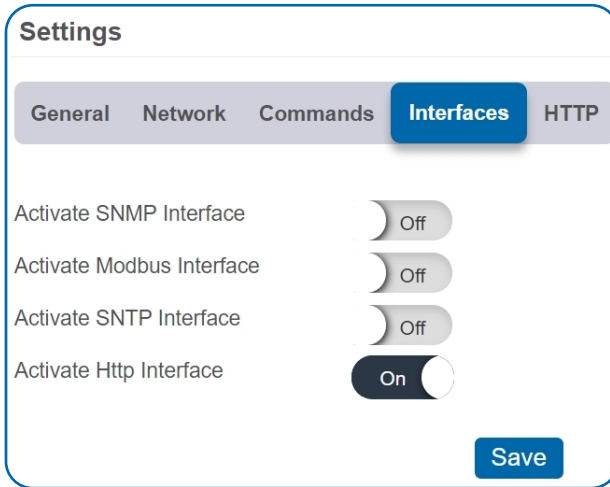
Reforming the network cleans up communication when multiple networks are in range of each other so they're all in sync. This is especially useful if you must move sensors to a new network, and would like to clear these sensors from the gateway's internal list. Reforming the network will place a new list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

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

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

Interface Activation

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



Settings

General Network Commands **Interfaces** HTTP

Activate SNMP Interface Off

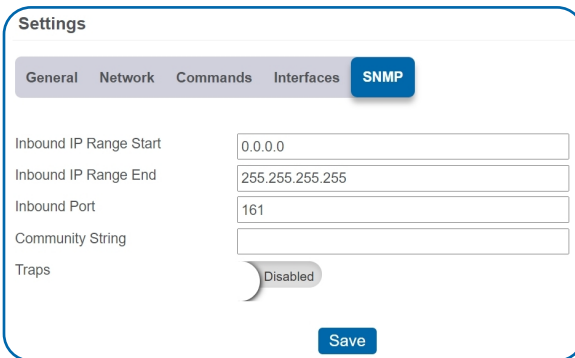
Activate Modbus Interface Off

Activate Sntp Interface Off

Activate Http Interface On

Save

Figure 8



Settings

General Network Commands Interfaces **SNMP**

Inbound IP Range Start

Inbound IP Range End

Inbound Port

Community String

Traps Disabled

Save

Figure 9

SNMP Interface – SNMP is an Internet application protocol that manages and monitors network device functionality. We use SNMP version 1. The settings can be configured both on iMonnit and the local interface. See Figure 9.

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

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

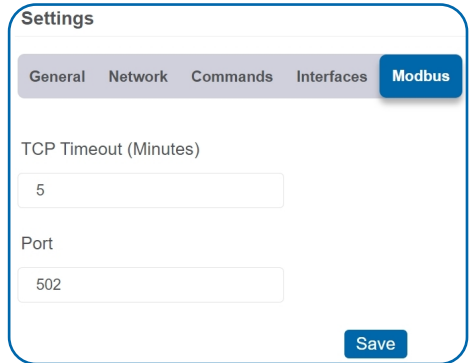
SNMP Community String – This is used as a configurable password for clients within the accepted IP Range. Communication will not be allowed if the Community String does not match. The default will be set to public.

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

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

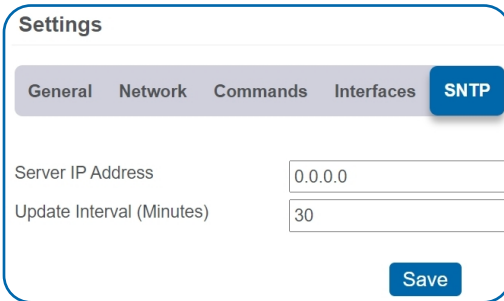
Trap Port – The server port where the trap alert state is sent when active.

Modbus Interface – Modbus Transmission Control Protocol (TCP) is the Modbus remote terminal unit (RTU) protocol with a TCP interface that runs on Ethernet. Monnit provides the Modbus TCP interface for you to pull gateway and sensor data. You can use Modbus without an active server interface. The data will not be sent to a server, but you can continue to poll for new data as it is received by the gateway. See Figure 10.



The screenshot shows the 'Settings' page with the 'Modbus' tab selected. The 'General' tab is also visible. The 'TCP Timeout (Minutes)' field is set to 5, and the 'Port' field is set to 502. A 'Save' button is located at the bottom right.

Figure 10



The screenshot shows the 'Settings' page with the 'SNTP' tab selected. The 'General' tab is also visible. The 'Server IP Address' field is set to 0.0.0.0, and the 'Update Interval (Minutes)' field is set to 30. A 'Save' button is located at the bottom right.

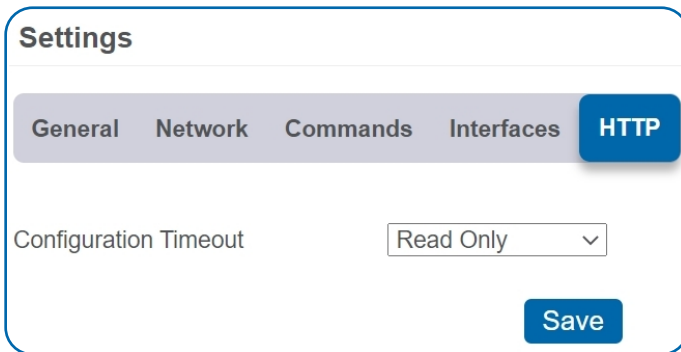
Figure 11

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

If the Monnit Server is active, it will be utilized for time synchronization in ordinary operation. So SNTP will be used as a backup. If you disable the default server interface, you must configure the SNTP Interface. See Figure 11.

HTTP Interface – The Hypertext Transfer Protocol (HTTP) Interface allows you to set how long the local interface is active before being automatically disabled. You may configure the local HTTP interface to remain Read Only, or to be disabled after one minute, five minutes, 30 minutes, or always active.

See Figure 12.



The screenshot shows the 'Settings' page with the 'HTTP' tab selected. The 'General' tab is also visible. The 'Configuration Timeout' field is set to 'Read Only'. A 'Save' button is located at the bottom right.

Figure 12

VI. INSTALLING IMONNIT EXPRESS AND MINE

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

INSTALLING IMONNIT EXPRESS SOFTWARE

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

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

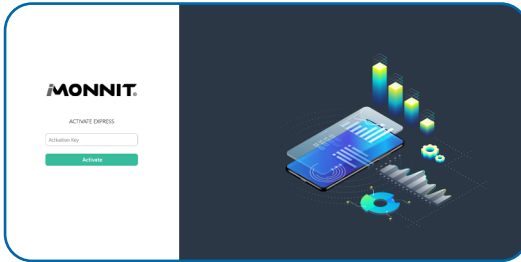


Figure 13

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

- Go to imonnit.com/sethost
- Enter the Gateway ID and Security Code included on the label directly under the QR code on the bottom of your gateway.
- Select the button for **Gateway Server Settings**.
- You must have an IP address to your server running iMonnit Express. Choose your port and whether this is a dynamic or static DHCP. Then press the **Submit** button.
- Enter the key code.

INSTALLING MONNIT MINE SOFTWARE

Monnit MINE is an open software platform that integrates Monnit Sensors and Gateways with your own software system. Monnit Gateways can be unlocked, allowing them to be directed to a custom host or IP address. Monnit MINE works as a translation application between Monnit Sensor networks and existing or custom software applications.

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

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

VII. USING THE LOCAL INTERFACE

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

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

Note

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

STATUS TAB

Ethernet LAN (Local Area Network Status)

This is a read-only section listing the current conditions for your LAN. See Figure 14.

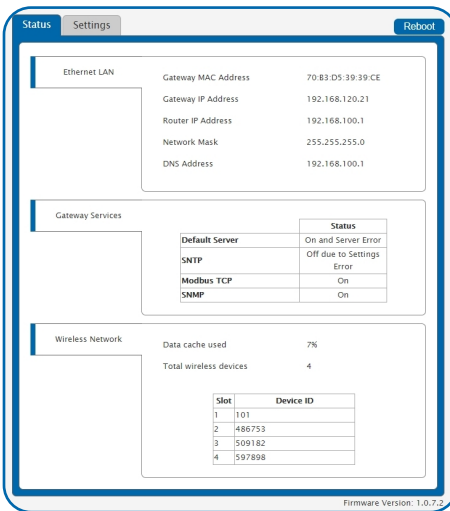


Figure 14

Gateway MAC Address – This is the media access control (MAC) address of your gateway to exclusively identify the device to a Network Interface Controller.

Gateway IP Address – This is a network address for your gateway when it's connected to the Internet.

Router IP Address – This is a network address for your router when it's connected to the Internet.

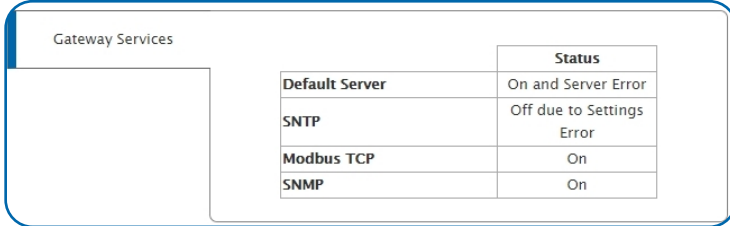
Network Mask – Also known as a Subnet Mask, this masks the IP address by dividing it into the network address and the host address.

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

Gateway Services

See Figure 15.

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



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

Figure 15

Wireless Network Status

See Figure 14.

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

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

SETTINGS TAB

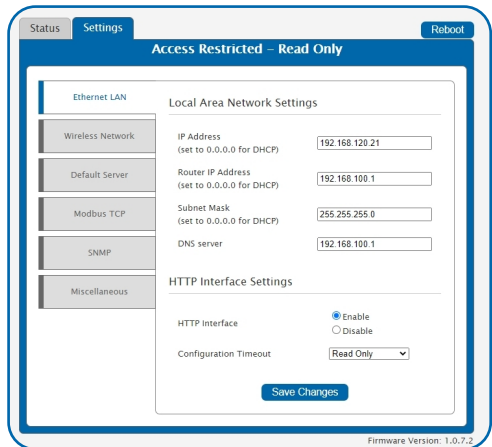
Ethernet LAN

See Figure 16.

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

Local Area Network Settings

In this section, you can edit LAN settings discussed on page 12.



Access Restricted – Read Only

Ethernet LAN

Local Area Network Settings

IP Address (set to 0.0.0.0 for DHCP) 192.168.120.21

Router IP Address (set to 0.0.0.0 for DHCP) 192.168.100.1

Subnet Mask (set to 0.0.0.0 for DHCP) 255.255.255.0

DNS server 192.168.100.1

HTTP Interface Settings

HTTP Interface Enable Disable

Configuration Timeout Read Only

Save Changes

Firmware Version: 1.0.7.2

Figure 16

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

Configuration Timeout: This allows you to set a time limit of one minute, five minutes, and 30 minutes for how long the local interface is active. Read Only keeps the interface active, but you can't make any changes. You can only change the settings out of Read

Only through the HTTP Interface on iMonnit; see page 10. Always Available makes the interface always open and editable.

Wireless Network

See Figure 17.

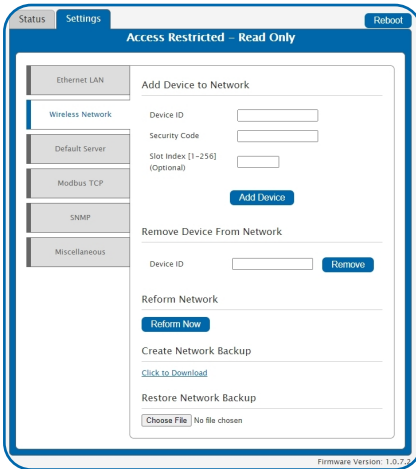


Figure 17

Add Device to Network

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

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

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

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

Remove Device from Network

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

Reform Network

Select the Reform Now button to remove all devices from the Wireless Device List.

Create Network Backup

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

Restore Network Backup

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

Default Server

See Figure 18.

Default Server Settings

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

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

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

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

The **On Server Loss** field sets what happens when the gateway loses communication with the server. The default setting Log Sensor Data commands the gateway to continue communicating with your sensors and store readings until it can re-establish a connection to the server. Toggling this to Disable Wireless Network will force the sensors to find a new gateway to deliver sensor messages to the server immediately.

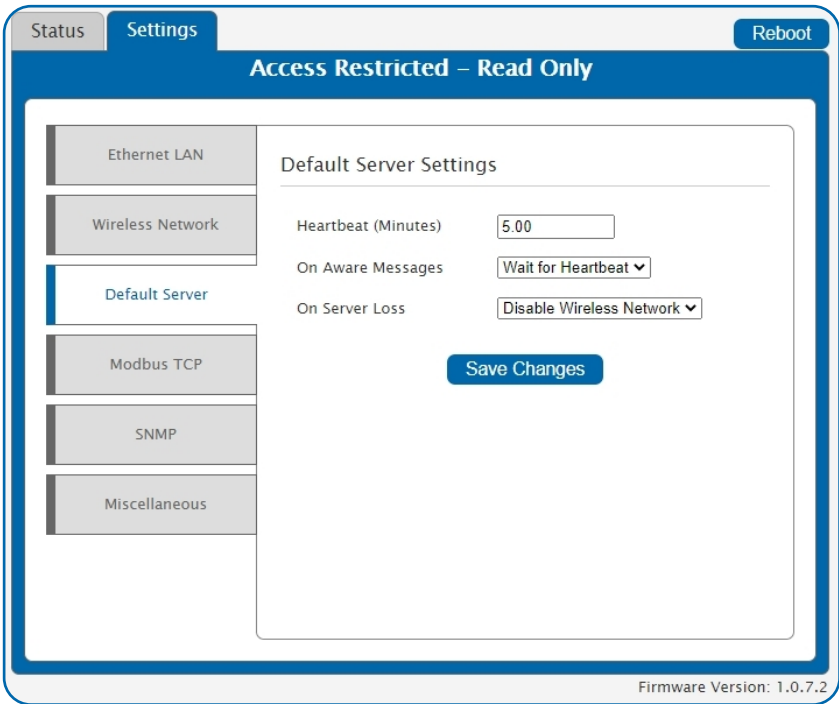


Figure 18

Modbus TCP (Transmission Control Protocol)

See Figure 19.

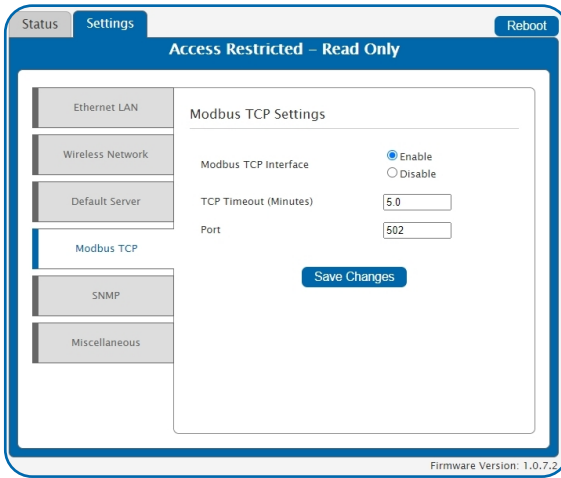


Figure 19

Modbus TCP Settings

Modbus TCP interface runs on an Ethernet connection. The TCP makes sure all data is received. Modbus TCP is a non-streaming data interface standard. This means data must be requested in order for it to be received. Additionally, only the current data points are available for reading. Historical sensor information is not available. See Figure 19.

The Modbus TCP Interface will store all data values in 16-bit registers. The registers and their associated data fields are mapped below. To access the sensor holding registers for a particular device, the assigned slot number for the device needs to be known. When reviewing added devices through the default server, the order in which devices are presented may not necessarily correspond to the order in which the devices are stored in the gateway network list as the default server will sort the devices based on their ID. To be certain which device is in a particular slot, go to the gateway local web interface status.htm page and note the device's assigned slot.

After the slot number(s) for the desired devices to read from are known, the following formula may be applied to determine the correct starting register to read from to retrieve the recorded data from the device:

DATA ADDRESS:

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

REGISTER ADDRESS:

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

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

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

SENSOR HOLDING REGISTERS (Slot 1)			
Field	Description	Register	Data Address
Sensor ID_High	The first 16 bits of a 32-bit serial ID number	40101	100
Sensor ID_Low	The last 16 bits of a 32-bit serial ID number	40102	101
Device Type	The unique type identifier for the sensor profile	40103	102
Data Age	The number of seconds that have elapsed since the last data was retrieved	40104	103
Is Device Active	0 indicates no data for this slot	40105	104
Is Aware	Becomes aware when a sensor threshold has been breached	40106	105
Voltage	Battery voltage	40107	106
RSSI	Signal Strength Indicator...0-100%	40108	107
Data 1	Sensor Data Field 1	40109	108
Data 2	Sensor Data Field 2	40110	109
Data 3	Sensor Data Field 3	40111	110
Data 4	Sensor Data Field 4	40112	111
Data 5	Sensor Data Field 5	40113	112
Data 6	Sensor Data Field 6	40114	113
Data 7	Sensor Data Field 7	40115	114
Data 8	Sensor Data Field 8	40116	115

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

SNMP

See Figure 20.

The screenshot shows the 'Simple Network Management Protocol v1 Settings' page. The 'SNMP Interface' is enabled. The 'Inbound IP Address Range' is set to 0.0.0.0 to 255.255.255.255. The 'Inbound Port' is 161. The 'Community String' is public. The 'Traps' are disabled. The 'MIB-II System Configuration Strings' section has four input fields for Contact String, Name String, Location String, and Description String.

Figure 20

The SNMP version 1 settings for a gateway can be adjusted on the offline local interface. You can continue to use SNMP without the server interface active. The data will not be sent to a server, but you can continue to poll for the data as it is received by the gateway. See Figures 20 through 22.

- **Inbound IP Range Start and End** – This is the IP address for the SNMP client. If you communicate with one device, the starting and ending IP addresses will be the same. Exchanging information with multiple machines will require a set of different starting and ending IP addresses.
- **Inbound Port** – This is the number for where specifically in the server data from the gateway is received.
- **SNMP Community String** – This is used as a configurable password for clients within the accepted IP Range. Communication will not be allowed if the Community String does not match. The default will be set to public.

Trap Settings

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

MIB-II System Configuration Strings

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

SNMP Client Configuration

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

Data Interpretation

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

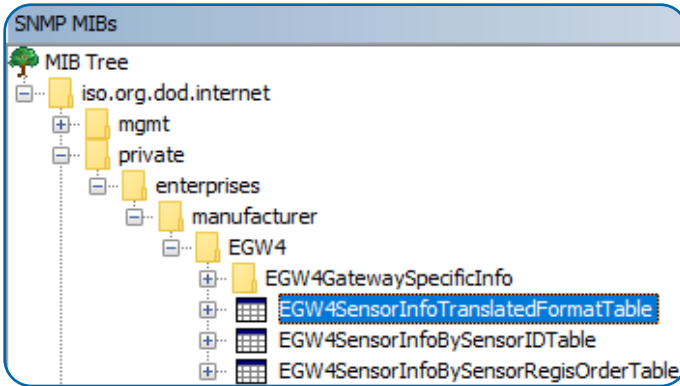


Figure 21

Data presented in the EGW4 Sensor Info Translated Format Table will be converted into usable information. The other tables listed here will display raw data. The SNMP Data Interpretation document can be requested by contacting Monnit directly. It will explain how the raw data can be converted into usable information.

Miscellaneous System

See Figure 22.

SNTP Settings

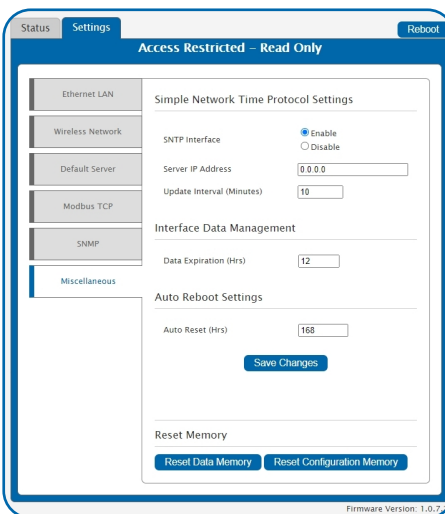


Figure 22

SNTP synchronizes computer clocks on a network when the Monnit Interface is unavailable.

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

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

Interface Data Management

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

Auto Reboot Settings

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

Reset Memory

Reset Data Memory button: Press this to wipe stored sensor readings from the gateway. All the changes you made to your settings remain intact.

Reset Configuration Memory button: Press this to reboot all your settings back to the factory defaults.

TROUBLESHOOTING

LED Indicators

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

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

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

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

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

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

Will Not Connect to iMonnit

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

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

Detailed instructions for each step can be found [here](#).

SUPPORT

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

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

WARRANTY INFORMATION

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

Customer may return all Products for repair or replacement due to defects in original materials and workmanship if Monnit is notified within one year of customer's receipt of the Product. Monnit reserves the right to repair or replace Products at its own and complete discretion. Customer must obtain from Monnit a 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, customer shall return Products to be examined and replaced to Monnit's facilities, in shipping cartons which clearly display a valid RMA number provided by Monnit. Customer acknowledges that replacement Products may be repaired, refurbished, or tested and found to be complying. Customer shall bear the risk of loss for such return shipment and shall bear all shipping costs. Monnit shall deliver replacements for Products determined by Monnit to be properly returned.

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

Limitation of Warranty and Remedies.

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

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

CERTIFICATIONS

United States FCC

All ALTA XL® Gateways Contain FCC ID: ZTL-G2XL1

This equipment has been tested and found to comply with the limits for a Class B digital devices, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help

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

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

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 transmitter IC: 9794A-G2XL1 has 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 té 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.

RF Exposure



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 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 (US: 22cm or IC: 32.1cm). 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 equipments introduced on the market. All the relevant information's is available on the European Community website: <http://ec.europa.eu/enterprise/sectors/rtte/documents/>

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

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.

Additional Information and Support

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



Monnit Corporation

3400 South West Temple • Salt Lake City, UT 84115 • 801-561-5555
www.monnit.com

Change Log

Date	Change	Reason	Modified By
1/19/23	Change Log Created	Original Release	Marketing