



Monnit Ethernet Gateway 4 User Guide

IMPORTANT!

For best results, please wait to power on your Ethernet Gateway 4 until after you have registered an account on iMonnit and added your gateway and sensors to the online system.

Table of Contents

I. ABOUT THE ETHERNET GATEWAY 4	1
ALTA ETHERNET GATEWAY 4 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
SNTP SECURITY	3
SNMP SECURITY	3
IV. GATEWAY REGISTRATION	4
REGISTERING THE ETHERNET GATEWAY 4	4
V. USING THE ETHERNET GATEWAY 4	5
USING THE ETHERNET GATEWAY 4	5
UNDERSTANDING THE ETHERNET GATEWAY 4 LIGHTS	5
ETHERNET GATEWAY 4 SETTINGS	6
VI. INSTALLING MONNIT EXPRESS AND MINE	11
INSTALLING MONNIT EXPRESS	11
INSTALLING MONNIT MINE	11
VII. USING THE LOCAL INTERFACE	12
GATEWAY STATUS TAB	12
GATEWAY OPTIONS TAB	13
DATA INTERFACES TAB	15
SUPPORT	20
WARRANTY INFORMATION	20
CERTIFICATIONS	22



I. ABOUT THE ETHERNET GATEWAY 4

Monnit's ALTA Ethernet Gateway 4 allows your Monnit Wireless Sensors to communicate with the iMonnit® Online Wireless Sensor Monitoring and Notification System without the need for a PC. Simply provide power and plug the gateway into an open Ethernet network port with an Internet connection. It will then automatically connect with our online servers, providing the perfect solution for commercial locations where there is an active Internet connection.

The Ethernet Gateway 4 allows your Monnit Wireless Sensors to communicate with the iMonnit system via Ethernet transmission. ALTA Ethernet Gateways are advanced wireless IoT gateways that enable fast time-to-market solutions. Monnit's Ethernet Gateway 4 is specifically designed to respond to the increasing market need for global technology that accommodates a variety of vertical IoT application segments and remote wireless sensor management solutions.

ALTA ETHERNET GATEWAY 4 FEATURES

- Wireless range of 1,200+ feet through 12+ walls *
- Frequency Hopping Spread Spectrum (FHSS) **
- Improved interference immunity
- Encrypt-RF® Security (Diffie-Hellman Key Exchange + AES-128 CBC for sensor data messages)
- 15,000 sensor message memory
- Over the air updates (future proof)
- True plug & play, no hassles for Internet configuration set-up
- No PC required for operation
- Local status LEDs with transmission and online status indicators
- AC power supply

* Actual range may vary depending on environment.

** When paired with a Monnit data plan.

EXAMPLE APPLICATIONS

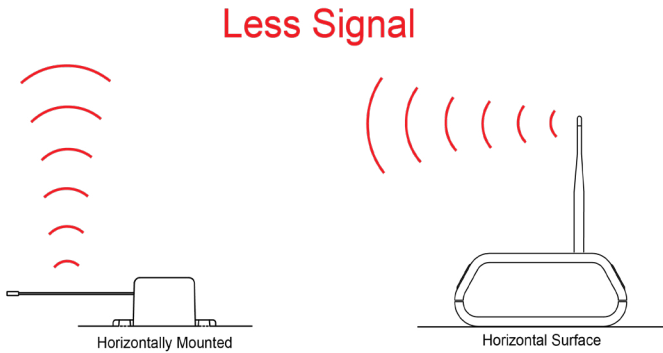
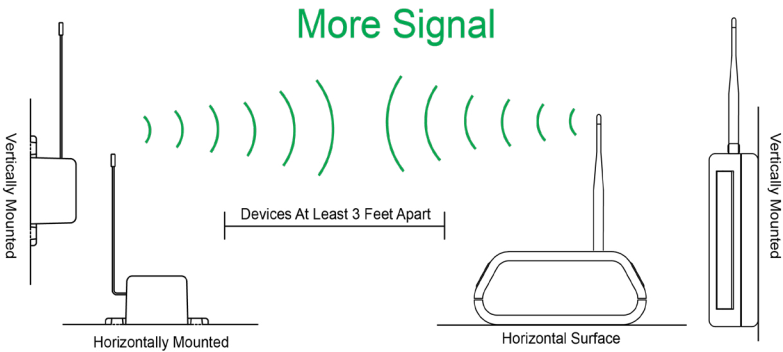
- Remote Location Monitoring
- Shipping and Transportation
- Agricultural Monitoring
- Vacant Property Management
- Vacation Home Property Management
- Construction Site Monitoring
- Data Center Monitoring

II. HOW YOUR GATEWAY WORKS

Your ALTA Ethernet Gateway 4 manages communication between your sensors, iMonnit, and network peers through the SNMP v1 and Modbus TCP protocols. When running, the gateway will periodically transmit data on a heartbeat to the iMonnit servers. The gateway will store information received from sensors until its next heartbeat.

The ALTA Ethernet Gateway 4 uses an Ethernet connection to relay data received from sensors to iMonnit. Sensors communicate with the gateway, then the gateway relays information to the cloud.

For your wireless sensors to work optimally, orient all antennas for your sensor(s) and gateway(s) the same direction (typically vertical).



III. GATEWAY SECURITY

The ALTA Ethernet Gateway 4 has been designed and built to securely manage data from sensors monitoring your environment and equipment. Hacking from botnets are in the headlines, Monnit Corporation has taken strong measures to ensure your data security is handled with the utmost care and attention to detail. The same methods utilized by financial institutions to transmit data are also used in Monnit security infrastructure. Security features of the gateway include purpose built operating system, data encryption, and bank-grade security.

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

SENSOR COMMUNICATION SECURITY

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

DATA SECURITY ON THE GATEWAY

The ALTA Ethernet Gateway 4 is designed to prevent prying eyes from accessing the data that is stored on the sensors and on iMonnit. The ALTA Ethernet Gateway 4 does not run on an off the shelf multi-function OS (operating system). Instead it runs a purpose specific real-time embedded state machine that cannot be hacked to run malicious processes. When fully secured after initial configuration steps, the gateway provides no active interface that can be used to gain access. The fortified gateway prevents snooping of sensor traffic, keeping your sensitive data from malicious parties and secures the gateway from becoming a relay for malicious programs.

SERVER COMMUNICATION SECURITY

Communication between your ALTA Ethernet Gateway 4 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 VPN's. The gateway can still operate within a VPN if it is present.

SNTP SECURITY

The gateway can be set up to retrieve time from an SNTP server. 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.

SNMP SECURITY

SNMP stands for Simple Network Management Protocol) is an Internet application protocol that manages and monitors network device functionality. Monnit uses SNMP version 1. These settings can both be configured both on iMonnit and the local interface.

IV. GATEWAY REGISTRATION

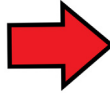
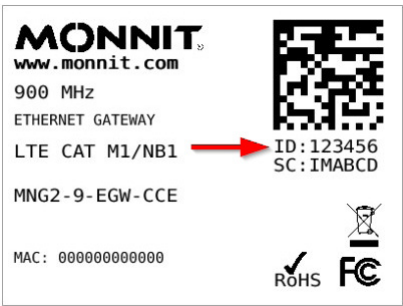
If this is your first time using the iMonnit online portal, you will need to create a new account. If you have already created an account, start by logging in. For instructions on how to register for an iMonnit account, please consult the iMonnit User Guide viewable at monnit.com/support/documentation.

REGISTERING THE ETHERNET GATEWAY 4

To register your gateway on iMonnit, you will need to enter the **Device ID** and the **Security Code** from your Ethernet Gateway 4 in the corresponding text boxes. Use the camera on your smartphone to scan the QR code on your Gateway. If you do not have a camera on your phone, or you are accessing the online portal through a desktop computer, you may enter the Device ID and Security Code manually.

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

When completed, select the "Submit" button.



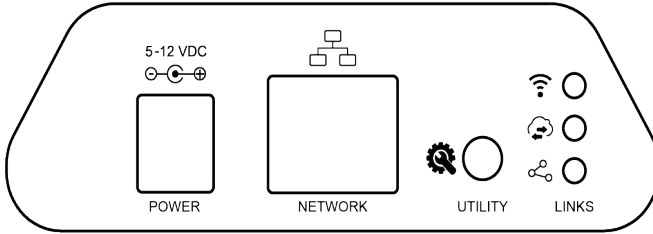
The screenshot shows the 'Add Device' interface. At the top, it says 'Add Device' with a help icon. Below is an illustration of a hand holding a smartphone scanning a QR code on a gateway device. A green 'Scan Barcode' button is visible. Below that, it says '- Or -' and shows two input fields: 'Device ID *' (with 'ID Number' as a hint) and 'Code *' (with 'Security Code' as a hint). A 'Submit' button is at the bottom left. At the bottom right, it says 'Finished adding devices?' and a blue 'Continue' button.

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

V. USING THE ETHERNET GATEWAY 4

USING THE ETHERNET GATEWAY 4

The back of your gateway will look like the diagram below:



From left to right, we see:

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

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

Utility Button: A short, five second, press of this button will enable the local interface. Pressing the utility button for fifteen seconds will reset the gateway.

1. Connect your antenna to the gateway.
2. Plug the power supply cord and the network cable into an outlet.
3. After the three LED lights switch to green, your gateway is ready to use.

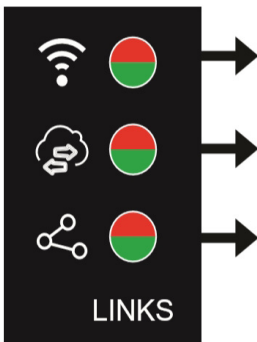
UNDERSTANDING THE ETHERNET GATEWAY 4 LIGHTS

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 and entering a “waterfall” pattern. In case of failure, the light sequence will repeat after ten seconds. The gateway will continue trying to boot until it succeeds. Please contact technical support if the lights aren’t green after two minutes.

Connection stage: When the LEDs turn solid green for 1.5 seconds, the power-on stage will be complete. After the Network Uplink Connectivity Indicator displays a solid green LED, the gateway will attempt to begin making connections to it’s default server and other configured surfaces. The gateway will attempt to settle all operational connections. As the gateway first connects to the network, all other lights will be dark.

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



Steady Green: Communication with sensors is normal.
Blinking Green: Active communication with sensors.
Steady Red: Gateway hardware may be faulty

Steady Green: Communication with the default server is okay.
Blinking Green: Active communication with the default server
Steady Red: Last communication with the data interface was unsuccessful. This could signal an issue with the default server.

Steady Green: Network connection successful.
Steady Red: No Network connection has been made.

ETHERNET GATEWAY 4 SETTINGS ON IMONNIT

The Ethernet Gateway 4 will receive data from all sensors assigned to the network and within range, then return this data to the iMonnit server in a series of heartbeats.

You can access gateway settings by selecting “Gateways” in the main navigation panel. Choose the Ethernet Gateway 4 from the list of gateways registered to your account. Select the “**Settings**” tab to edit the gateway:

Settings

General Commands
Local Area Network Interface Activation

Gateway Name
EGW2

Heartbeat Minutes (default: 5)
5

Force Transmit on Aware
Yes

Server Address
[REDACTED]

Save

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

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

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

Commands

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

The screenshot shows a web interface for 'Settings'. At the top, there are four tabs: 'General', 'Commands' (which is selected), 'Local Area Network', and 'Interface Activation'. Below the tabs, there are two input fields: 'Will Call Expiration (Hours)' with the value '12' and 'Auto Reset (Hours)' with the value '168'. Each input field has a menu icon to its right. Below these are three sections of buttons: 'Reform Network' with a 'Reform' button, 'Update Gateway Firmware' with an 'Update' button, and 'Reset Gateway to Factory Defaults' with a 'Reset' button. At the bottom of the settings area is a large 'Save' button.

A. Will Call Expiration is the number of hours that messages are kept in the internal memory for the Modbus TCP and SNMP interfaces before it is cleared out.

B. This is the time in hours that the gateway will continuously operate before an automatic reset takes place. An auto reset takes about ten seconds.

C. 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.

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

Local Area Network

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

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

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

The screenshot shows a web interface for network settings. At the top, there's a 'Settings' title. Below it are four tabs: 'General', 'Commands', 'Local Area Network' (which is selected), and 'Interface Activation'. Under the 'Local Area Network' tab, there are several fields: 'MAC Address' with the value '00:00:00:00:00:00', a 'DHCP' section with a radio button selected for 'Static', and four text input fields for 'Static IP (Use DHCP: 0.0.0.0)', 'Network Mask', 'Default Gateway', and 'Default DNS Server', all containing the value '0.0.0.0'. At the bottom of the form is a dark blue 'Save' button.

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

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

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

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

Interface Activation

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

Settings

General Commands
Local Area Network Interface Activation
SNMP Interface

Activate SNMP Interface
 On

Activate Modbus Interface
 Off

Activate Sntp Interface
 Off

Activate Http Interface
 Off

Settings

General Commands
Local Area Network Interface Activation
SNMP Interface

Inbound IP Range Start

Inbound IP Range End

Inbound Port

SNMP Community String

Trap Settings

Traps
 Enabled

Trap IP Address

Trap Port

Trap on Authentication Failure
 Enabled

Trap on New Sensor Data
 Disabled

Trap on Sensor Alarms
 Disabled

SNMP Interface – SNMP stands for Simple Network Management Protocol) is an Internet application protocol that manages and monitors network device functionality. Monnit uses SNMP version 1. These settings can both be configured both on iMonnit and the local interface.

Inbound IP Range Start and End - This is the IP address for the SNMP client. If you have one device to communicate with, the start and end IP addresses will be the same. Exchanging information with multiple machines will require a set of different start and end IP addresses.

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

SNMP Community String – This is used to support SNMPv1 protocol by giving access to a router's or other device's statistics. The default will be set to "public."

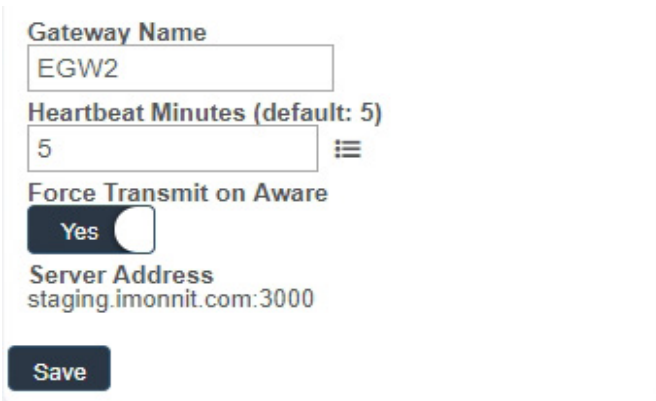
Trap Settings

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

Trap IP Address - The IP Address for the SNMP Server where the trap will be sent.

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

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



The screenshot shows a settings form for the Modbus Interface. It includes a text input for 'Gateway Name' with the value 'EGW2', a numeric input for 'Heartbeat Minutes (default: 5)' with the value '5', a toggle switch for 'Force Transmit on Aware' currently set to 'Yes', and a text input for 'Server Address' with the value 'staging.imonnit.com:3000'. A 'Save' button is located at the bottom.

Settings

- General
- Commands
- Local Area Network
- SNTP Interface
- Interface Activation

Server IP Address

Update Interval (Minutes)

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

If the 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.

HTTP Interface – The HTTP Interface allows you to set how long you wish the local interface to be active before being automatically disabled. For increased Security, your choices are to have the local HTTP interface disabled after 1 minute, 5 minutes, 30 minutes, or always active. See the next section for more on the local interface.



The screenshot shows a settings form for the HTTP Interface. It includes a dropdown menu for 'Auto Disable (Minutes)' with the selected value 'Default (5 min)'. A 'Save' button is located at the bottom.

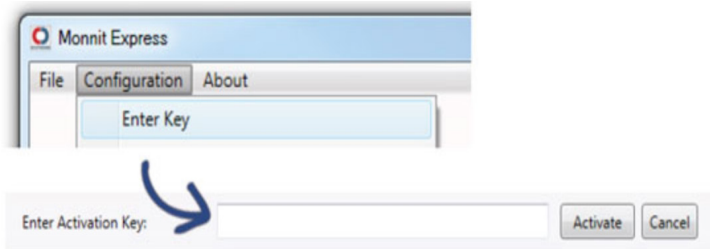
VI. INSTALLING MONNIT EXPRESS AND MINE

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

INSTALLING MONNIT EXPRESS SOFTWARE

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

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.”



2. Next, you will need to add your Ethernet 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. 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 provides the ability to integrate Monnit wireless sensors and gateways with your own software system. Monnit wireless gateways can be unlocked, allowing them to be directed to a custom host or IP address, where an installation of Monnit MINE works as a translation application between Monnit wireless sensors networks and existing or custom software applications.

When you purchase the Monnit MINE software, you will receive an activation code.

Next, you will need to add your Ethernet 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. 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 interface.

- Connect the gateway to a router or network switch using an Ethernet cord.
- Plug in the gateway to a power outlet.
- Power on the gateway. While booting, the lights will scroll green.
- Press and hold the utility button. At the end of the boot process, all lights will be green for two seconds then shift to red. Release the button and the local configuration page will be temporarily enabled.
- 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 your gateway.
- Use your web browser to connect to your gateway using the assigned IP address. You should be redirected to the Gateway Status page.
- Once the gateway interface has been reached, head over to the General Options tab and select the Miscellaneous System Configuration page. Enable the HTTP interface and set it to be available for one hour (3600 seconds). 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. After configuration set this to a small integer.

GATEWAY STATUS TAB

Ethernet Local Area Network Status

The screenshot shows the 'Gateway Status' tab of the 'Wireless Ethernet Gateway Configuration' page. It is divided into three main sections:

- Ethernet Local Area Network Status:** Displays Gateway MAC Address (FF:FF:FF:FF:FF:FF), Gateway IP Address (192.168.100.178), Router IP Address (192.168.100.1), Network Mask (255.255.128.0), and DNS Address (75.75.75.75).
- Data Interface Statuses:** Shows Gateway data cache used (0%) and a table of interface statuses.
- Wireless Sensor Network Status:** Shows the number of Gateway devices (1) and a table of device slots.

Interface	Status
Default Server	On
SNTP	Off
Modbus TCP	Off
SNMP	Disabled

Slot	Device ID
1	12346

Firmware Version: 1.0.2.7 Gateway ID: 935772

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

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

Gateway IP Address - This is a numerical identifier for your gateway when it is connected to the Internet.

Router IP Address - This is a numerical identifier for your router when it is connected to the Internet.

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

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

Data Interface Statuses

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

Status Table - These status fields indicate the current operation status for each data interface. The Default Server field can contain "Off", "Off due to Settings Error", "On and Server Error", or "On". The SNTP field can contain "Off", "Off due to Settings Error", "On and Synced", or "On". The Modbus TCP field can contain "Off", "Off due to Settings Error", or "On". The SNMP field can contain "Off", "Off due to Settings Error", "On and Traps Ready", or "On".

Wireless Sensor Network Status

This section list the number of gateways communicating with the server. 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.

GATEWAY OPTIONS TAB

Ethernet Local Area Network Configuration

From the Local Area Network Configuration tab, you can modify 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.

The screenshot displays the 'Wireless Ethernet Gateway Configuration' web interface. The 'General Options' tab is selected, and the 'Ethernet Local Area Network Configuration' sub-tab is active. The interface includes a sidebar with navigation options: 'Ethernet Local Area Network Configuration' (selected), 'Wireless Sensor Network Configuration', 'System Time Configuration', and 'Miscellaneous System Configuration'. The main configuration area contains the following fields:

Field	Value
IP Address (set to 0.0.0.0 for DHCP)	0.0.0.0
Router IP Address (set to 0.0.0.0 for DHCP)	0.0.0.0
Subnet Mask (set to 0.0.0.0 for DHCP)	0.0.0.0
DNS server	0.0.0.0

A 'Save Changes' button is located at the bottom right of the configuration area. At the bottom of the page, the firmware version is listed as '1.0.2.7' and the gateway ID as '935772'.

Wireless Sensor Network Configuration

The screenshot shows the 'Wireless Ethernet Gateway Configuration' web interface. The 'General Options' tab is selected. On the left, there is a navigation menu with four items: 'Ethernet Local Area Network Configuration', 'Wireless Sensor Network Configuration' (which is highlighted), 'System Time Configuration', and 'Miscellaneous System Configuration'. The main content area is titled 'Add Device to Gateway'. It contains three input fields: 'Slot Index [1-256]: (Optional)', 'Device ID:', and 'Security Code:'. Below these fields is an 'Add Device' button. Underneath is an 'Erase Device List' section with a 'Reform Wireless Network' button. At the bottom, there is a table titled 'Current Wireless Network Device List' with two columns: 'Slot' and 'Device ID'. The table contains one entry: Slot 1 with Device ID 12346. At the very bottom of the page, it shows 'Firmware Version: 1.0.2.7' and 'Gateway ID: 935772'.

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.

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

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

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

System Time Configuration

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

The screenshot shows the 'Wireless Ethernet Gateway Configuration' web interface. The 'General Options' tab is selected. On the left, there is a navigation menu with four items: 'Ethernet Local Area Network Configuration', 'Wireless Sensor Network Configuration', 'System Time Configuration' (which is highlighted), and 'Miscellaneous System Configuration'. The main content area is titled 'Simple Network Time Protocol Configuration'. It contains several settings: 'SNTP:' with radio buttons for 'Enable' (selected) and 'Disable'; 'SNTP IP Address:' with a text input field containing '0.0.0.0'; 'SNTP Resample Period (Sec): (65535 is the maximum)' with a text input field containing '1600'; 'Epoch between Default Server and SNTP:' with a text input field containing '9534364800'. Below this is the 'Gateway System Time Configuration' section, which includes: 'System Reset Period (Hrs): (0 is disabled, 8760 is the maximum)' with a text input field containing '168'; 'System Time Source:' with radio buttons for 'Default Server' (selected) and 'SNTP'; 'Secondary Time Source Follower Period (Sec): (65535 is the maximum)' with a text input field containing '7200'. At the bottom of this section is a 'Save Changes' button. At the very bottom of the page, it shows 'Firmware Version: 1.0.2.7' and 'Gateway ID: 935772'.

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

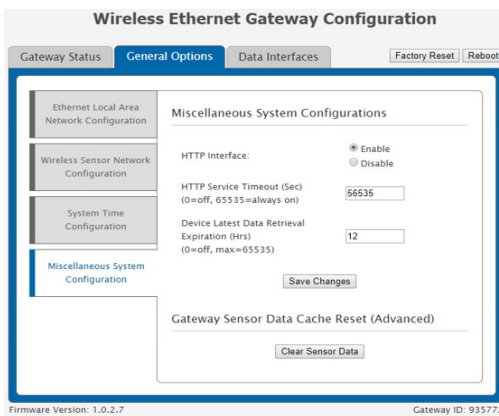
SNTP Resample Period: The time in seconds when the gateway will check the server for the correct time.

Epoch between Default Server and SNTP: This is the difference in seconds between the standard NTP Epoch (start date 01/01/1900) and Monnit's Epoch (start date 01/01/2012).

System Reset Period: The time in hours it takes for the system to reset.

Secondary Time Source Failover Period: The time in seconds that the gateway will continue to attempt to poll the Primary System Time Source unsuccessfully for an updated time before switching over and using time from the secondary time source. This time period should be longer than the SNTP Resample Period if SNTP is being used.

Miscellaneous System Configuration



HTTP Service Timeout: This is a security setting for allowing this web interface to be active. The default is 5 minutes. Setting the field to 0 will turn it off.

Device Latest Data Retrieval: An expiration period for data before it is considered to be "old" meaning data interfaces will not report this sensor data.

Clear Sensor Data button: Pressing this button will purge all old device messages from the gateway to start from a clean slate. You will lose all messages for all data interfaces.

DATA INTERFACES TAB

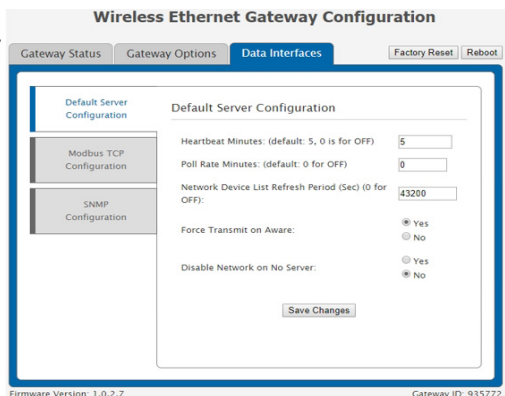
Default Server Configuration

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

Many of the settings here are the same as they are in iMonnit.

The **Network Device List Refresh Period** setting controls the amount of time before the gateway requests the network device list from the default server.

The **Disable Network on No Server** setting controls whether the wireless device network is disabled after the gateway determines it cannot reach the default server.



Modbus Transmission Control Protocol Configuration

The screenshot displays the 'Wireless Ethernet Gateway Configuration' web interface. At the top, there are navigation tabs: 'Gateway Status', 'Gateway Options', and 'Data Interfaces' (which is selected). To the right of the tabs are 'Factory Reset' and 'Reboot' buttons. On the left side, there is a sidebar with three configuration sections: 'Default Server Configuration', 'Modbus TCP Configuration' (which is highlighted with a blue bar), and 'SNMP Configuration'. The main content area is titled 'Modbus Transmission Control Protocol Configuration'. It contains the following settings:

- Modbus TCP:** A radio button interface with 'Enable' and 'Disable' options. The 'Disable' option is selected.
- TCP Timeout Minutes: (default: 5):** A text input field containing the value '5'.
- Port:** A text input field containing the value '502'.

At the bottom of the configuration area is a 'Save Changes' button. At the very bottom of the page, the text 'Firmware Version: 1.0.2.7' is on the left and 'Gateway ID: 935772' is on the right.

Modbus TCP interface runs on an Ethernet connection. TCP makes sure all data is received. Modbus TCP is a non-streaming data interface standard. This means data must be requested in order for it to be received. 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 `wsn.htm` page or status page and note which slot the desired device is assigned to.

After the slot number(s) for the desired devices to read from are known, the following formula may be applied to determine the correct starting register to read from to retrieve the recorded data from the device: $\text{starting register} = 101 + 16(\text{slot no.} - 1)$. Each reading will report the most recent message received from that device by the gateway, so the polling frequency should be greater than the device heartbeat frequency to avoid missing device updates.

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			
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
Sensor ID_High	The first 16 bits of a 32-bit serial ID number	40117	116
Sensor ID_Low	The last 16 bits of a 32-bit serial ID number	40118	117
Device Type	The unique type identifier for the sensor profile	40119	118
Data Age	The number of seconds that have elapsed since the last data was retrieved	40120	119
Is Device Active	0 indicates no data for this slot	40121	120
Is Aware	Becomes aware when a sensor threshold has been breached	40122	121
Voltage	Battery voltage	40123	122
RSSI	Signal Strength Indicator...0-100%	40124	123
Data 1	Sensor Data Field 1	40125	124

SNMP Configuration

The screenshot displays the 'Wireless Ethernet Gateway Configuration' web interface. The 'Data Interfaces' tab is selected, and the 'SNMP Configuration' page is active. The interface includes a navigation menu on the left with options for 'Default Server Configuration', 'Modbus TCP Configuration', and 'SNMP Configuration'. The main content area is titled 'Simple Network Management Protocol v1 Configuration' and contains the following settings:

- SNMP:** Enable, Disable
- Inbound IP Address Range:** (Set the same values for a single address. Start/End are inclusive.)
 - Starting Address:
 - Ending Address:
- Inbound Port:**
- Community String:**

Trap Settings

- Traps:** Enable, Disable
- Trap URL:**
- Trap Port:**
- Trap on Authentication Failure:** Enable, Disable
- Trap on New Sensor Data:** Enable, Disable
- Trap on Sensor Alarms:** Enable, Disable

MIB-II System Configuration Strings

- Contact String:**
- Name String:**
- Location String:**
- Description String:**

A 'Save Changes' button is located at the bottom of the configuration area. The footer of the page shows 'Firmware Version: 1.0.2.7' and 'Gateway ID: 935772'.

SNMP (Simple Network Management Protocol) settings for a gateway can be adjusted on the offline local interface. You can continue to use SNMP without the server interface active. The data will not be sent to a server, but you can continue to poll for the data as it is received by the gateway.

- **Inbound IP Range Start and End** - This is the IP address for the SNMP client. If you have one device to communicate with, the start and end IP addresses will be the same. Exchanging information with multiple machines will require a set of different start and end IP addresses.

- **Inbound Port** – This is the number for where specifically in the server data from the gateway is received.
- **SNMP Community String** – This is used to support SNMPv1 protocol by giving access to a router's or other device's statistics. The default will be set to "public."

Trap Settings

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

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

MIB-II System Configuration Strings

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

SUPPORT

For technical support and troubleshooting tips, please visit our support knowledge base online at monnit.com/support. 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 Number (RMA) 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 Return Material Authorization Number (RMA) 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 one 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

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

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

Warning: *Changes or modifications not expressly approved by 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.

Monnit and ALTA Wireless Sensors, Wireless Sensor Adapters and Ethernet Gateways:

This equipment complies with the radiation exposure limits prescribed for an uncontrolled environment for fixed and mobile use conditions. This equipment should be installed and operated with a minimum distance of 23 cm between the radiator and the body of the user or nearby persons.

All ALTA Wireless Sensors and Gateways Contain FCC ID: ZTL-G2SC1.

Approved Antennas

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

- *Xianzi XQZ-900E (5 dBi Dipole Omnidirectional)*
- *HyperLink HG908U-PRO (8 dBi Fiberglass Omnidirectional)*
- *HyperLink HG8909P (9 dBd Flat Panel Antenna)*
- *HyperLink HG914YE-NF (14 dBd Yagi)*
- *Specialized Manufacturing MC-ANT-20/4.0C (1 dBi 4" whip)*

Canada (IC)

English

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

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

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

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-RFSC1, IC: 9794A-G2SC1, IC: 4160a-CNN0301, IC: 5131A-CE910DUAL, IC: 5131A-HE910NA, IC: 5131A-GE910 et IC: 8595A2AGQN-4NNN) 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.

European Union - Directive 1999/5/EC

ALTA Wireless Ethernet Gateway model MNG2-9-EGW-CCE has been evaluated against the essential requirements of the 1999/5/EC Directive.

Hereby, Monnit Corp., declares that Monnit ethernet gateway model MNG2-9-EGW-CCE is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

In order to satisfy the essential requirements of 1999/5/EC Directive, the Monnit ethernet gateway is compliant with the following standards:

Article 3.1(a): Electrical safety	EN 60950-1:2006 + A11:2009 + A1:2010 + A12:2011 + AC:2011
Article 3.1(a): Exposure to electromagnetic fields	EN 62311:2008
Article 3.1(b): EMC	EN 301 489-1 V1.9.2 EN 301 489-7 V1.3.1
Article 3.2: Radio spectrum use	EN 301 511 V9.0.2

The conformity assessment procedure referred to in Article 10 and detailed in Annex IV of Directive 1999/5/EC has been followed with the involvement of the following Testing Body.

*Testing Body:
NEMKO CANADA INC
303 River Road
Ottawa, ON, Canada*

*Manufacturer:
Monnit Corp.
3400 South West Temple
Salt Lake City, UT 84115*

There is no restriction for the commercialization of Monnit and ALTA 868MHz and 433MHz wireless products in all the countries of the European Union.

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, aircrafts, etc.*
- *Where there is risk of explosion such as gasoline stations, oil refineries, etc.*

It is responsibility of the user to enforce the country regulation and the specific environment regulation.

Do not disassemble the product; any mark of tampering will compromise the warranty validity. We recommend following the instructions of this user guide for correct setup and use of the product.

Please handle the product with care, avoiding any dropping and contact with the internal circuit board as electrostatic discharges may damage the product itself. The same precautions should be taken if manually inserting a SIM card, checking carefully the instruction for its use. Do not insert or remove the SIM when the product is in power saving mode.

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

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/rte/documents/>

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 at monnit.com/support.



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